Universidad Nacional Autónoma de México

Facultad de Ingeniería

"ANÁLISIS Y DISEÑO DE UNA RED LAN EMPLEANDO FAST ETHERNET E IPv6 PARA LA DELEGACIÓN XOCHIMILCO"

T E S I S

Que para obtener el título de:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

Gustavo Rodrigo Sánchez Vélez

Director de Tesis: M.I. Marcial Contreras Barrera

CD. UNIVERSITARIA MEXICO, D.F. NOVIEMBRE 2003

A

Agradecimientos

Gracias a ti **DIOS** por dejarme vivir, por darme fuerzas cuando más lo necesito, por darme valor para hablar de ti, por darme cuenta de las cosas, por poner en mi camino rocas y personas, y moldear la persona quien soy, y sobretodo por cuidarme en cada momento de la vida.

Gracias **Abuelita** por permitirme verte y sentirte junto de mí, por tu cuidado de mis primeros años de vida, por el sacrificio y por todo tu amor. TE EXTRAÑO MUCHO.

Gracias a mi Abuelita **Lupe** por todo su amor, apoyo y mantenerme en su pensamiento.

Gracias **Mamá** y **Papá** por estar junto a mí, por tanto y tanto amor, por ver que nunca me faltara nada, por los regaños, consejos, pláticas hasta altas horas de la noche, por las tardes de películas, por mi niñez.

A ti **Mamá** por tanto sacrificio, entrega, apoyo, por todo tu amor y todas las palabras de aliento, gracias por tus consejos y tu ternura, por tu ayuda, por tus desvelos, GRACIAS.

A ti **Papá** por el sacrificio, por tus consejos, por los regaños y la presión de terminar este trabajo, por la enseñanza de tantas cosas.

Gracias **Daniel** por existir, por tu inocencia, por tu carácter, por la forma de ver las cosas, por tus juegos, por tu valor, por tu desinhibición ante la vida, por tu cariño y sobre todo por creer tanto en mí. TQM.

Gracias **Sandra** por todas tus preocupaciones, por tu cariño, por perdonar mis engaños de juegos de nuestra niñez, y por tu confianza. TQM.

A ti **Edith**, por compartir tantas y tantas cosas, por pasar por alto mis olvidos, por nuestros sueños, por estar junto a mí, por todo tu amor y ser parte de mi vida:

S... t...,
s... m...,
s... j...

A todos mis primos y mis tíos **Tere, Anita** y **Emilio** por su cariño y por estar tan cerca de mí y de mi familia. Gracias tía Tere por tu carisma y por preocuparte por nosotros. Gracias tía Anita por preocuparte tanto de mí. Gracias tío Emilio por estar junto a mí.

Gracias a mis amigos, **David, Jorge** y **Vero**, por enseñarme todas las bases para poder continuar con la carrera, por brindarme su corazón y

haberme escuchado cuando más lo necesitaba. David, sin ti no hubiera podido pasar del primer semestre a no ser por toda tu paciencia y el tiempo para enseñarme, de verdad, muchas gracias.

Gracias **Marcial** por creer en mi desde un principio, por abrir parte de tus sentimientos y ser exigente para todo. Gracias **Paty** por ayudarme en todo y por tu amistad.

A mis amigas, **Iliana, Claudia** y **Elizabeth**, gracias por compartir las diferentes etapas de mi vida y aguantar mi carácter y mis olvidos. Además de escucharme y ayudarme en todo momento y a cualquier hora.

Gracias Señora **Leticia Guerrero** por ayudarme en mi salud, mi persona, mi familia y mi casa. Gracias por escucharme y hacerme sentir paz y bienestar.

Pool, gracias por enseñarme parte del negocio de la computación y sobretodo por tu amistad.

Martín gracias por tus pláticas, consejos y tu amistad incondicional además de las horas invertidas para el proyecto del robot.

Gracias **Adriana** por defenderme, por creer en mí y darme la oportunidad de trabajar.

Gracias **Lucero** por creer en mí y por compartir tus conocimientos además de tu ayuda para elaborar este proyecto.

Gracias Daisy por ser una parte importante de mi vida y discúlpame por no haberte regresado a casa.

A ti **RODRIGO** por aguantar y sobreponerte de todas las cosas que te han sucedido, por tu carácter, por ser enérgico, por nunca rendirte y experimentar con las cosas para aprender. Gracias por tu sentido del humor, tus ocurrencias y caras.

Y por supuesto a la Facultad por la formación y sus conocimientos impartidos, y a la **UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO** por ser la máxima casa de estudios y por todo lo que representa.

"POR MI RAZA HABLARÁ EL ESPÍRITU"

PAGINACIÓN DISCONTINUA

ÍNDICE

PRÓLOGO

El objetivo de este trabajo de tesis es diseñar y reestructurar la red LAN actual de la delegación Xochimilco, utilizando la nueva versión del protocolo IP (IPv6), partiendo de un estudio previo de las condiciones del lugar, necesidades, recursos disponibles y estructura de la red actual así como incrementar el ancho de banda del enlace dedicado a Internet (DS0) y ser tomado en cuenta como una opción real de implementación.

El problema consiste en ampliar el ancho de banda en la red de la delegación Xochimilco ya que ésta cuenta con un enlace dedicado (DS0= 64kbps) que sirve como enlace para la conexión a Internet.

Cabe señalar que este trabajo presenta una solución integral, puesto que se tienen problemas causados por diferentes deficiencias: cableado, equipo de comunicaciones, computadoras y sus aplicaciones y enlaces dedicados.

En la actualidad en la delegación Xochimilco se cuenta con 215 equipos de cómputo de los cuales sólo 120 se encuentran conectados en al red, con una velocidad de transmisión de 10 Mbps. Por tanto, la topología de red utilizada es híbrida por lo que en algunas zonas se crea un cuello de botella, asimismo el ancho de banda del enlace a Internet es muy pequeño.

Considerando que actualmente 120 de los 215 equipos están conectados a la red también aumentará el número de direcciones IP, que a corto plazo serán escasas en todo el mundo, por lo que aparece la exigencia de emigrar a una nueva versión del protocolo IP (IPv6) atrayendo todos sus beneficios.

La solución de este problema le será útil a la gran cantidad de personas que laboran y están en contacto con la delegación, por contar con una mayor velocidad en la transmisión de datos.

Con la nueva versión del protocolo IP obtendremos mayor seguridad, autenticación, integridad y confidencialidad en los datos, se incrementará el tamaño de direcciones de 32 a 128 bits, entre otros aspectos.

El conjunto de un mayor ancho de banda, la migración a la nueva versión del protocolo IP (cambio de sistema operativo en las computadoras), y de manera opcional el cambio de cableado, traerá como beneficio la transmisión de una mayor cantidad de información, tener un mayor número de usuarios conectados a la red, además de contar con mejor recepción en las transferencias de archivos grandes (bases de datos).

Para la solución del problema se han optado tres pasos:

- Investigación
- Análisis
- Costo-beneficio

En esta tesis se incluyen los tres caminos que están estrechamente ligados, es decir, no se puede utilizar solo un método sin dejar de depender de los restantes. Por ejemplo no podemos referirnos a un costo-beneficio sin realizar antes un análisis previo tanto de la red actual del lugar mencionado o hacer a un lado la investigación de la mejor tecnología para los recursos y necesidades con los que se vaya a partir o se cuenten.

Por tanto a continuación se describe el camino a seguir para el desarrollo de este proyecto de tesis y así obtener la solución al problema en cuestión. Se describe en tres rubios:

Primero: Estudio previo.

Se realizará un estudio sobre la problemática que existe en la red actual. Se cuestionará al jefe del Departamento de Sistemas o departamento afín, con el objetivo de tener conocimiento de la causa de los problemas que se presentan con la red en ese momento. Asimismo se investigarán los recursos con los que se cuenta (si el personal de la delegación nos permite) obteniendo una idea aproximada, lo que debe obtenerse como un límite y no debe rebasarse haciendo un fuerte énfasis como tal.

También se cuestionará cuales son las necesidades separando la primordial, el aumento del ancho de banda dentro de la red local e Internet.

Segundo: Investigación y diseño.

Partiendo del estado anterior podemos investigar la mejor opción en cuanto al ancho de banda, tecnología, equipo, etcétera.

En esta investigación tendremos que tomar en cuenta principalmente el costo y la calidad de cada uno de los aspectos anteriores así como rendimiento y tipo de servicio al contratarlos.

Teniendo todos los datos arriba descritos, se diseñará la nueva red seleccionando cada uno de los elementos que la conformarán.

Tercero: Documentación propuesta.

Ya diseñada la nueva red se presentará al jefe del Departamento de Sistemas un documento que contiene la propuesta de la nueva red, indicando detalladamente cada componente de ésta, contendrá la cotización de cada ámbito o elemento de la propuesta.

Igualmente se explicará en este documento el beneficio que tendrá la nueva red a los usuarios para un mayor desempeño de sus funciones, que se traducirá en un mejor servicio para el personal que tenga algún tipo de contacto con la delegación.

CAPÍTULO 1
Antecedentes

1.1. Introducción

La delegación Xochimilco tiene como encargado de todo el equipo de cómputo y telecomunicaciones a la Subdirección de Informática. Este departamento tiene como actividades: la evaluación de equipo y proyectos, nuevas tecnologías, personal, instalación de equipo, soporte técnico, instalación de cableado, revisión de contratos de arrendamiento, desarrollo de página Web, entre otras actividades. El personal de esta subdirección se informa de toda tecnología por medio de suscripciones a revistas, foros, conferencias, etc.

De esta forma, se aplicarían cambios importantes en la red, tales como incremento en la velocidad de acceso a la red local como de Internet, las ventajas de IPv6 (que se mencionarán en el capítulo 6), que conlleva a la simplificación del trabajo de los usuarios y atender más actividades de su rango, aumentando la productividad de la delegación.

Conviene destacar que este trabajo es sólo una propuesta que será analizada por las autoridades correspondientes pues tiene un costo dividido y puede ser considerado como alto, dependiendo del presupuesto contemplado para este año para el departamento Subdirección de Informática.

Se presentarán costos reales de hardware y software para cubrir las diferentes necesidades para la implementación tanto de un adecuado cableado como IPv6.

También se pondrá a consideración, algunas opciones extras que mejorarían el performance de la red interna para una posible expansión de nodos en esta dependencia sin dejar de visualizar todos sus beneficios.

1.2. Objetivos

1. Incrementar la velocidad de transmisión de datos dentro de la red local y enlaces privados.
2. Mejorar tiempos de respuesta.
3. Diseño y reestructuración de la red local.
4. Cambio de infraestructura: equipo de comunicaciones.
5. Aumentar el rango de direcciones con IPv6.

1.3. Antecedentes

1.3.1. Enlace a Internet y comunicación con D.D.F. (Centro Histórico)

La administración de la delegación Xochimilco cuenta con un enlace dedicado por medio de microondas al Departamento del Distrito Federal (ubicado en el Centro Histórico) para la transmisión de datos: bases de datos; que se comparte para Internet, todo con una velocidad de 64 Kbps.

La empresa que provee el servicio Internet es Telmex. Tienen un contrato por 2 años con facturación mensual, tiene un costo mensual de $950.00 más IVA, como es un enlace para casi 150

personas la velocidad el acceso es muy limitado considerando con los cuellos de botella que ocasionan los concentradores.

En la figura 1.1 se muestra de forma esquemática la conexión de los enlaces mencionados, incluyendo de forma general, las conexiones a la red local.

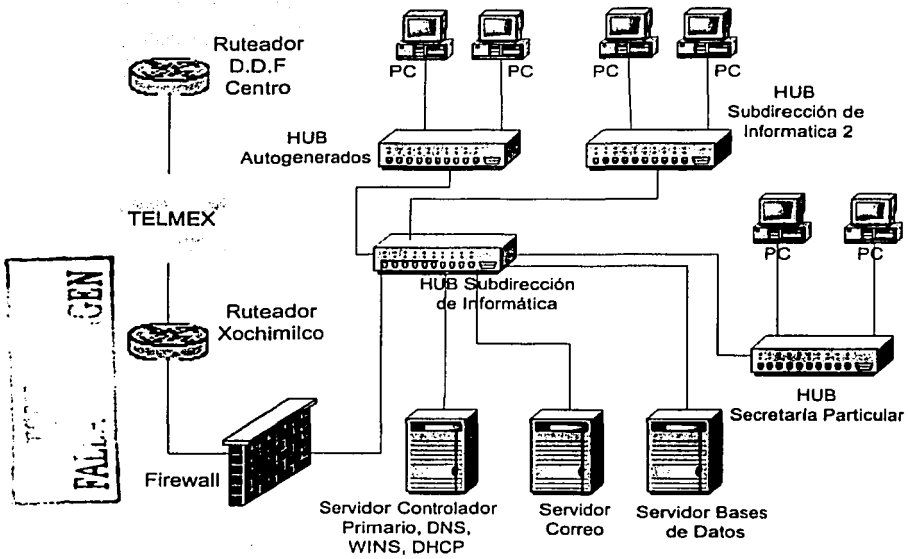


Fig. 1.1. Esquema general de red local

La administración de la red se lleva a cabo por varios servidores. Por un servidor DELL de modelo reciente que contiene el control del dominio y obviamente, de los recursos de la red, es decir, es un PDC (Primary Domain Control). Este servidor se encuentra bajo la plataforma Windows 2000 server. La arquitectura de red es de forma centralizada pues contiene el servicio de DNS, WINS sólo en este servidor, por lo que si tuviera alguna falla ningún otro servidor tomaría todos estos servicios. Se cuenta con servicio de DHCP para que los clientes obtengan una dirección IP (direcciones dinámicas) y no de forma manual (direcciones "fijas").

Existe un servidor de correo con el software de Microsoft Exchange versión 5.5, el cual se encuentra en un servidor DELL del mismo que el anterior con sistema operativo Windows NT versión 4.

Un Firewall se encarga de la seguridad con dispositivo, plataforma que no es posible mencionar al igual que dichos servidores, precisamente por políticas de seguridad sobre todo por tratarse de información federal.

Todos los servidores, ruteadores, computadoras se conectan a un concentrador principal se encuentran en un rack de aluminio en una habitación previamente destinado con aire acondicionado.

No tienen servicio de monitoreo, el único sistema de monitoreo es el que se encuentra de las herramientas de Administración del servidor en Windows 2000 server llamado Event Viewer, el cual sólo menciona las fallas en los servicios, equipo y software de cada servidor.

1.3.2. Red local

La red local esta basada con el estándar 802.3, es decir, una red Ethernet. La delegación Xochimilco, actualmente cuenta con 200 computadoras, de las cuales 120 se encuentran en red, distribuidas en diferentes departamentos:

- Autogenerados
- CESAC
- Contraloría interna
- Desarrollo social
- Recursos financieros
- Recursos materiales
- Secretaría particular
- Servicios generales
- Subdirección jurídica
- Subdirección Plan Lago
- Subdirección de informática
- Subdirección de obras

Cada departamento tiene uno o más concentradores dependiendo del lugar físico donde se encuentren. Todas las computadoras forman una topología en bus lógicamente y físicamente se implementa como una estrella, es decir, todos los dispositivos se concentran por un medio físico a un hub que a su vez se conectan a un concentrador principal (en cascada), por lo que el rendimiento de la red es deficiente a causa de los cuellos de botella. Recordando las funciones de un hub: sólo envía los mensajes, paquetes o información a todos los puertos pues no tiene una tabla donde guarde las relaciones entre puertos y las conexiones de las computadoras. Por tal motivo el concentrador manda un mismo paquete a todos sus puertos por lo que se genera mayor tráfico que con otros dispositivos que si contienen tablas de ruteo en la memoria. Al contrario de un switch, este dedica el ancho de banda general por cada uno de sus puertos, pues tiene conductos conmutados y no compartidos.

Las aplicaciones que emplean son orientadas a conexión con el servidor pues necesitan datos de bases de datos que se encuentren en alguno de los servidores, además de un cliente de correo electrónico, aplicaciones como procesador de textos, hojas de calculo, transferencia de archivos de equipo a equipo.

El cable con el que están comunicados todos los dispositivos es cable UTP categoría 3 y categoría 5. Por lo que su máxima velocidad de transmisión es de 10 Mbps y 100 Mbps respectivamente, según el lugar donde estén ubicadas las computadoras, puesto que no hay un estándar de cableado para toda la delegación a causa del poco mantenimiento a dicho cableado.

Cabe mencionar, no existe "Memoria Técnica" de la red, por lo que no se tiene conocimiento de ubicación de todo el cableado, que tipo, marca, nuevas instalaciones, modificaciones, estándar, etc.

En muchos de los casos se puede ver que el aislante que cubre a los cuatro pares se encuentra fuera del plug RJ-45, es decir, no se encuentran bien hechos los patch cords, por lo que también puede ser causa de la ausencia de comunicación o que se este pueda tener un falso contacto con alguno de los pines del plug.

En la tabla 1.2 se muestran las áreas, marcas, modelos, número de puertos y velocidad máxima a la que pueden transmitir todos los concentradores de la delegación, así como la cantidad de puertos ya empleados para computadoras, o bien para las conexiones con otros concentradores:

	Área	Marca	Modelo	No. de ptos.	Velocidad	No. puertos empleados
1	Autogenerador	3COM	OFFICE-CONNECT	12	100	8
2	CESAC-Ventanilla 2	3COM	OFFICE-CONNECT	8	10/100	5
3	CESAC-Ventanilla 1	3COM	OFFICE-CONNECT	24	10/100	10
4	Contraloría Interna	3COM	OFFICE-CONNECT	8	10/100	8
5	Desarrollo Social	CENTRECOM	OFFICE-CONNECT	8	10/100	6
6	Recursos Financieros	3COM	OFFICE-CONNECT	8	10/100	8
7	Recursos Materiales	3COM	OFFICE-CONNECT	8	10/100	3
8	Secretaria Particular	3COM	AT-FH708E	24	10/100	19
9	Servicios Generales	3COM	SUPER-STACK	24	10/100	5
10	Subdelegación Jurídica	3COM	OFFICE-CONNECT	12	100	10
11	Subdelegación Plan Lago	CENTRECOM	OFFICE-CONNECT	24	10/100	8
12	Subdirección de Informática	3COM	3C250A-TX1	24	10/100	24
13	Subdirección de Informática	3COM	OFFICE-CONNECT	24	10/100	9
14	Subdirección de Obras 1	3COM	OFFICE-CONNECT	24	10/100	13
15	Subdirección de Obras 2	3COM	OFFICE-CONNECT	8	10/100	5
16	Subdirección de Obras 3	3COM	OFFICE-CONNECT	24	10/100	10
17	Subdirección de Obras 4	3COM	OFFICE-CONNECT	8	10/100	5

Tabla. 1.2. Esquema general de red local

También existe la posibilidad que el cableado provoque interrupciones en las comunicaciones causado por probables segmentos trozados, o bien, los cables pueden sufrir desgarres o rasguños puesto que no se encuentran dentro de ningún tipo de canaleta o conducto para protegerlos de golpes o jalones intencionales causados por cambio de lugar de muebles, tropiezos, etcétera. En algunos tramos, el cableado se encuentra por debajo de alfombra, por lo que puede ocasionar las personas no lo vean y recarguen sobre el cable cualquier tipo de mueble y dañarlo.

En muy limitadas ocasiones se encuentran cables muy cercanos a balastras, por lo que puede ocasionar, también, pérdidas de información a causa de los campos magnéticos que ocasionan estos aparatos eléctricos.

Las computadoras son de la marca DELL modelo GX1. Este modelo de computadoras esta diferido en el tiempo, tienen Windows 98 o Windows 95 como sistema operativo. Es muy común que los clientes dejen de imprimir en una impresora que se encuentren en la red, sobre todo cuando se trata de Windows 95. Por lo que los usuarios tienen que reiniciar la computadora para establecer de nuevo la conexión con el servidor de impresión. La memoria que contienen es limitada al igual que el espacio en disco duro. Las nuevas aplicaciones que en un futuro se instalen saturarán estos equipos lo que lleva a la necesidad de cambiarlos.

1.4. Alcances

El alcance que se pretende es el cambio de todos los concentradores por switches evitando que ocurran las "caídas" en los servicios de conexión y los tiempos largos de respuesta, considerando todas las conexiones existentes, es decir, las 120 computadoras que se encuentran a algún concentrador.

El cambio de todo el cableado por uno nuevo es también un alcance que se visualiza porque es uno de los factores importantes ante dicha problemática, considerando la unión de las computadoras faltantes a la red (80 equipos) y la próxima expansión de las instalaciones.

En este rubro, también se aplica la velocidad en la transmisión de datos por parte del enlace privado al Centro Histórico y el enlace con salida a Internet, por lo que se notaría en el performance de la red y por supuesto, de las aplicaciones que corren en las computadoras, no dejando sin considerar el cambio del equipo de cómputo y por consiguiente del sistema operativo.

De esta forma se sugiere un cambio integral y así descartar cualquier factor que provoque dicha problemática.

CAPÍTULO 2
Conceptos generales

2.1. Topologías de redes

La topología de una red es una distribución que tendrá la red en cualquier institución. A manera general una topología puede dividirse en las dos siguientes: física y lógica.

La topología física es la forma física o la búsqueda de la vía más económica y eficaz, con el objeto de conectar los nodos de una red.

La topología lógica es el método que se emplea para la comunicación entre nodos, es decir, la ruta de flujo de datos, de esta manera evitar tiempos de espera en la transmisión de datos, permitir un mejor control de la red y permitir un aumento eficiente de dispositivos en una red.

Las topologías que existen en una de red son las siguientes:
- Horizontal o de bus
- Anillo
- Estrella y,
- Malla

2.1.1. Horizontal o de bus

Esta topología es un caso particular de la topología de árbol, pues sólo tiene un tronco y sin ramas. Esta topología se caracteriza por tener los nodos conectados linealmente por un medio común de comunicación. En los extremos del bus existen dispositivos llamados "terminadores".

La transmisión se lleva a cabo simplemente insertando el mensaje en el canal de comunicación recorriendo ambas direcciones de éste. El mensaje es enviado con una dirección destino, por lo que los nodos que no tengan esta dirección no tomarán el mensaje pero si tendrán que revisarlo. Cuando un nodo reconoce el mensaje como suyo simplemente lo retirará del canal. Si no llega a su destino, después de un determinado tiempo (previamente configurado), los terminadores lo eliminarán para evitar una congestión en la red.

Esta topología emplea el protocolo de CSMA/CD para tener control de acceso al medio, es decir, conocer cual es el estado del canal. Un sólo nodo podrá transmitir sí el medio esta libre de cualquier tipo de señal. Si dos equipos transmitieran al mismo se detecta una colisión y se detendría la transmisión de ambos dispositivos por lo que esperarán hasta que se vuelva a desocupar el canal.

Los problemas que presenta esta topología son la revisión de todos los paquetes por todos los dispositivos de la red, y el problema que causa la transmisión simultánea incluyendo la transmisión contínua de un equipo por un periodo determinado. Asimismo, la falla total o parcial de la red como consecuencia de algún tipo de problema con el cableado.

El estándar empleado para esta topología es Ethernet/IEEE 802.3. En la figura 2.1 se muestra la estructura básica de una red con topología de bus.

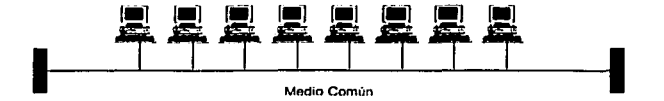


Fig. 2.1. Topología en bus

2.1.2. Anillo

Esta topología consiste en un arreglo secuencial de dispositivos unidos entre sí por medio de enlaces punto a punto, en un anillo cerrado. La transmisión es en un solo sentido en toda el anillo.

Cuando se transmite un mensaje el nodo emisor toma el Token (pasajes de patrones de bits) y lo envía con la dirección origen y dirección destino. Cada nodo revisa la dirección destino del paquete para comprobar si le corresponde, cuando llega al nodo destino lo copia y lo envía al nodo origen con una bandera de recibido. Este lo recibe, libera y envía el Token al siguiente nodo. Si tiene algo que enviar, hace el mismo procedimiento, si no, envía el Token al siguiente nodo.

La topología en anillo presenta los mismos problemas que la topología de bus. Si algún nodo falla, toda la red estaría incomunicada. Afortunadamente existen soluciones como centrales de cableado que detectan el nodo que esta fallando y automáticamente crean un puente para aislar este nodo manteniendo el anillo cerrado.

Estos centros de cableado también se emplean para añadir o eliminar nodos a la red, de esta forma, sólo se conectan o desconectan de los conectores de dichos centros sin pérdida de conexión o cortes en la comunicación. En años anteriores casi toda la red tenía que ser desmontada para agregar o remover un nodo.

El estándar empleado para esta topología es Token Ring/IEEE 802.5. En la figura 2.2 se muestra la figura que representa una topología en anillo.

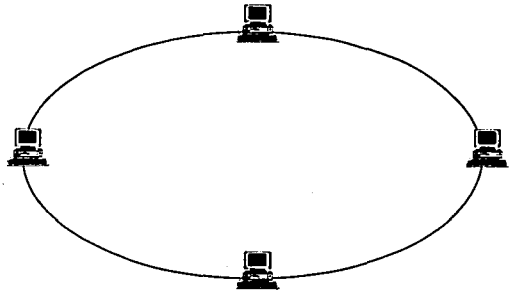


Fig. 2.2. Topología en anillo

2.1.3. Estrella

Es la topología mas empleada en las empresas para la instalacion de redes. La topología en estrella se caracteriza por un nodo central que administra el flujo de datos para y desde todos los nodos. A este nodo central se conectan todos los dispositivos por medio de hubs o switches de red. Para aumentar el numero de equipos sólo se conecta el nuevo dispositivo al concentrador mas cercano sin interrumpir la actividad de la red.

Las redes con topología en bus son implementadas físicamente en estrella, es decir, una topología en estrella es logicamente una red con topología bus. Como explicación de lo anterior se ejemplifica cuando un mensaje de cualquier nodo es recibido por todos los equipos restantes, esta transmisión sólo la puede realizar un solo equipo a la vez. De esta manera las técnicas de acceso al medio son empleadas para la topología en bus.

La desventaja que tiene esta topología es la vulnerabilidad que tendría la red a causa de algun tipo de falla en el nodo central, por lo que se debería tener un especial cuidado en la seguridad de este dispositivo.

La ventaja que presenta es la asignación de prioridades de transmisión y recepción para algunos nodos, esta caracteristica puede ser de gran utilidad para usuarios importantes dentro de la empresa. Así mismo la capacidad de remover dispositivos o cableado defectuoso sin la detención de la red.

En la figura 2.3 ejemplifica la red con topología en estrella.

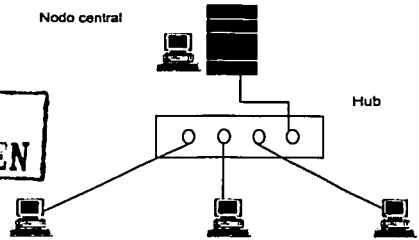


Fig. 2.3. Topología en estrella

2.1.4. Malla

Esta topología consiste en que todos o la mayoría de los nodos están conectados físicamente entre sí. Aunque esto permite el máximo en confiabilidad en cuanto a la transmisión-recepción de datos a consecuencia del ruteo de mensajes y la reducción de cuellos de botella, por lo que el costo de implementación es bastante considerable debido a lo siguiente: n dispositivos dentro de una red, cada equipo requerirá n-1 puertos de entrada-salida de datos.

En realidad esta topología no se emplea porque las distancias entre los diapositivos deben ser pequeñas, además haber considerado dichos costos, lo que lo convierte en innecesario.

La figura 2.4 muestra una red con topología en malla.

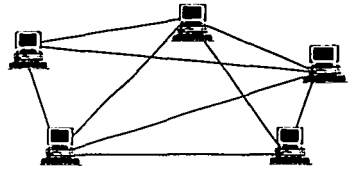


Fig. 2.4. Topología en malla

2.2. Clasificación de las redes de computadoras

La clasificación de las redes no la organización de cómo estará estructurada la red. Se tiene que tomar en cuenta puntos básicos como tipo de equipos que tendrá, tipo de datos que se utilizaran, alcance y posible expansión.

2.2.1. Redes de área local (LAN)

Desde los años 60 apareció el concepto de tiempo compartido, que consiste en colocar en una habitación, una terminal tonta (conjunto de monitor-teclado que sólo enviaban peticiones y recibían respuestas mostradas por medio del monitor) conectada telefónicamente a una distancia geográfica pequeña a un mainframe pagando por el tiempo que duraba la conexión.

Este método tenía una desventaja, la lentitud de la transmisión, pero este problema se solucionó en los años 70 con la aparición de los miniordenadores, sistemas de menores prestaciones que los mainframes pero de menor costo. Los miniordenadores podían instalarse en el lugar en el que se encontraban las terminales. De esta forma, cada departamento podía tener su propio miniordenador para prestar el servicio a múltiples usuarios dando origen al Proceso Distribuido.

Hasta finales de los 70 la compañía Datapoint Corporation lanzó al mercado el ARCNET (Attached Resource Computer Network) con microordenadores con mayor capacidad de procesar diferentes aplicaciones y la disminución del costo hizo que muchas compañías adquirieran esta red como parte de su trabajo.

En la actualidad se puede considerar equipos, tecnologías, software, protocolos, etcétera, para el mantenimiento, integridad de datos, restricción de acceso, compartimiento de información y recursos entre tantas aplicaciones de una red. Todo esto con un menor costo comparable a décadas pasadas, incluyendo el beneficio que trae a las empresas especialmente en su productividad.

Como su nombre lo indica, una red LAN, es un conjunto de equipos conectados entre sí por un medio común de comunicaciones con la finalidad de compartir sus recursos en un área relativamente pequeña. Generalmente una red LAN no suele exceder de un edificio o zona de edificios de una empresa.

2.2.2. Redes de área metropolitana (MAN)

Como su nombre lo indica una red MAN es una red que abarca un área geográfica entre una red LAN y una red WAN, generalmente entre edificios dentro de una ciudad entera. La red MAN esta bajo la norma 802.6 de IEEE.

La introducción de las redes MAN fue el resultado del interés que se tuvo en combinar las características de las redes de área amplia y las redes de área local, es decir, altas velocidades en la transmisión de datos en un área medianamente amplia con un costo relativamente bajo.

Esta red debe ser administrada de forma central, es decir, una instalación, operación y mantenimiento por una solo equipo de trabajo. Esto referente al backbone. Cada compañía de la organización tendrá que encargarse de la administración, operación, seguridad de su propia red, sin la pérdida de comunicación con el departamento corporativo.

El primer mercado para una MAN son los clientes que tienen la necesidad de grandes capacidades de comunicación como telefónica y transmisión de datos. La red MAN esta diseñada para satisfacer dichas necesidades a un menor costo obteniendo gran eficiencia y calidad comparado con el de una compañía telefónica.

Las características más sobresalientes de la red MAN son:

- **Velocidad.**
  Las redes MAN deben tener gran velocidad comparativa a las de las redes locales. En sí, una red MAN puede conectar varios dispositivos incluyéndose un número de redes LAN.
- **Área.**
  Las redes metropolitanas pueden cubrir una ciudad entera. La IEEE recomienda que sea de 50 kilómetros para cumplir con requerimientos, por ejemplo, de velocidad.
- **Soporte opcional.**
  La voz y el video son dos puntos opcionales que actualmente se están empleando no solo en redes WAN, sino en redes metropolitanas.
- **Backbone.**
  Las redes MAN deben tener una estructura básica para la conexión de redes o dispositivos, siendo así una sencilla administración.

2.2.3. Redes de área amplia (WAN)

Las redes de área amplia son aquellas que cubren un área geográficamente extensa partiendo desde ciudades en un país, todo un continente hasta el mundo entero.

Sin lugar a dudas la primera red de área amplia que se tuvo fue en los años 50 con las primeras computadoras. Las cuales tenían que utilizar una línea de comunicación (generalmente telefónica) para la transmisión de datos, de esta forma los datos serían procesados por el centro de procesamiento de datos.

Lo que ha revolucionado las comunicaciones a finales de los 80 es el empleo de redes de conmutación de circuitos (se establece, mantiene y termina un circuito o medio físico de transmisión de datos para cada sesión) y redes de conmutación de paquetes (se comparte un enlace dedicado punto a punto para transferir paquetes) pues estos métodos utilizan tecnologías como E1 (jerarquía europea) y T1 (jerarquía americana) con velocidades de 2.048 Mbps y 1.544 Mbps respectivamente.

Cabe mencionar que en una red WAN, las políticas de administración, configuración, seguridad y desempeño, deben ser bastante estrictas independientemente del tipo de empresa. Esto involucra una mejor detección y corrección de errores, confiabilidad en la transmisión y el comportamiento de datos, lo que deriva en una buena calidad de servicio.

En toda red debe haber un alto grado de flexibilidad. Esto se refiere a la posible expansión de la red e implementación de nuevas aplicaciones, técnicas, servicios, etcétera.

Por otro lado sabemos que una red WAN, también es un conjunto de redes LAN conectadas. Estas redes pueden tener tecnologías o topologías diferentes. Según sea el caso se ocupan dispositivos diferentes. En una red WAN o una red MAN, deben tener un backbone (estructura central) para poder conectar las múltiples redes LAN que se requiera. Por ejemplo, para conectar redes de diferentes topologías se ocupa un gateway y para la conexión de dos redes con topologías similares se ocupa un bridge.

2.3. Medios de comunicación

2.3.1. Medios de comunicación terrestres

Los medios de comunicación terrestres son aquellos que transmiten por un medio físicamente continuo.

A continuación se describe los cables mas empleados para la conexión entre dispositivos en una red local. En el caso de la fibra óptica, se puede emplear para la conexión entre dispositivos o como backbone.

2.3.1.1. Cable coaxial

El cable coaxial era el mas empleado en la segunda mitad de la década de los 80 gracias a su bajo costo, resistencia a la interferencia y una instalación relativamente sencilla.

Sin embargo el grosor del cable coaxial o el conjunto de ellos impide introducirlo en ductos de cable pequeños por lo que recientemente se ha optado por instalar cables como par trenzado o fibra óptica.

El cable coaxial consiste en un conductor central de cobre enrollado por una cubierta de material dieléctrico, rodeado a su vez por una hoja de metal (en algunos casos) y una malla entretejida de aluminio que protege al conductor central de cualquier interferencia eléctrica. Por último todo lo anterior es cubierto por un forro exterior de plástico, como se muestra en la figura 2.5.

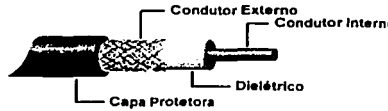


Fig. 2.5. Cable coaxial

Existen dos tipos de cable coaxial: de banda base y de banda ancha.

2.3.1.2. Cable de par trenzado

El cable de par trenzado se divide en cuatro pares de cable de cobre trenzados entre sí y recubiertos por un forro de plástico. Están enredados porque provoca inmunidad a campos magnéticos de cada cable. El cable y el numero de pares en cada cable puede variar dependiendo de la calidad y la longitud en la transmisión. Se emplean plugs y jacks RJ-45 para la conexión del nodo y hub. La longitud máxima de este cable es de 100 metros.

El cable de par trenzado se divide en dos clases: UTP y STP.

UTP (Unshielded Twisted Pair).

Como su nombre lo indica no tiene ningún tipo de protección o escudo entre los pares trenzados y el forro de plástico, figura 2.6.

El cable UTP tiene 6 clasificaciones o categorías, las mas empleadas son las tres siguientes:

- Categoría 3. La categoría 3 tiene como significado que existen 3 trenzas por pie. Puede transmitir datos en redes 10BaseT a 10 Mbps.
- Categoría 4. Esta categoría tiene 4 trenzas por pie. Se utiliza en redes Token Ring y pueden transmitir a 16 Mbps.
- Categoría 5. Este cable tiene 5 trenzas por pie. Se emplea en redes Fast Ethernet y puede transmitir datos a 100 Mbps.
- Categoría 6. Esta categoría tiene 1 año que se liberó en su estándar, y fue diseñado para soportar velocidades de 1 Gbps.

Y ya se esta desarrollando investigaciones para estandarizar la categoría 7 de cableado UTP.

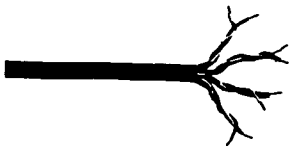


Fig. 2.6. Cable par trenzado

STP (Shielded Twisted Pair)

Esta clase de cable tiene un recubrimiento metálico que protege y reduce a los pares trenzados de interferencias electromagnéticas.

2.3.1.3. Cable de fibra óptica

El cable de fibra óptica reside en tres componentes: primero, un núcleo central de vidrio muy fino con un alto índice de refracción, que se empleará para transmitir haces de luz. Estos viajan por el núcleo central, inciden sobre la superficie externa por medio de ángulos, de forma que la luz se refleja sin pérdidas hacia el interior de la fibra. Así, la luz se transmite a larga distancia reflejándose miles de veces. Segundo, una envoltura que tiene menor índice de refracción pero permite que la luz se refleje con este último. Y tercero, un recubrimiento que tiene como fin, proteger y proporcionar más resistencia al cable.

Una red que utiliza fibra óptica emplea un Láser o LED para enviar una señal en forma de pulsos de luz.

La fibra óptica tiene un solo sentido de comunicación, ya que el haz de luz se transmite en una sola dirección, es decir, la comunicación es unidireccional (figura 2.7).

Las ventajas que presenta son:

- Gran alcance sin pérdida de información (cerca de 100 Km.).
- Velocidades de 1 Gbps.
- Es inmune a interferencia eléctrica o frecuencias de radio, ruido o temperatura.
- Se puede transmitir datos, voz y video.
- Se emplea en topologías de anillo y estrella.

Las desventajas que reúne son el elevado costo y el cuidado en su instalación.

Este tipo de cable se utiliza cada vez con más frecuencia como backbone de las redes LAN gracias a sus propiedades.

Fig. 2.7. Cable fibra óptica

La fibra óptica se divide principalmente en dos tipos por su forma de transmisión: monomodal y multimodal.

Monomodal

Como cualquier tipo de fibra, el manejo de esta debe ser con una amplia experiencia en su instalación además de contar con herramienta específica.

La fibra óptica monomodal (figura 2.8) tiene como característica esencial, menor diámetro que la fibra multimodo.

Entre otras características, esta fibra tiene una gran capacidad de transmisión de datos a gran distancia y baja atenuación. Generalmente se emplean dispositivos láser como fuentes emisoras.

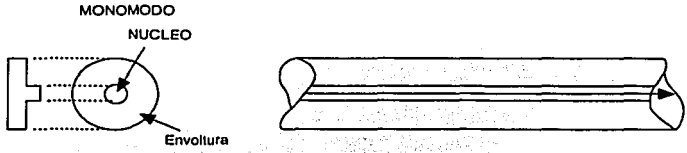


Fig. 2.8. Fibra óptica monomodal

Multimodal

Este modo se caracteriza por la diversidad de ángulos en que se refleja la luz gracias al grosor que tiene este tipo de fibra. Es recomendada para la transmisión de datos, voz y video en distancias no superiores a 3 Km.

A su vez, este modo se divide en dos tipos de fibra. La diferencia más notoria es el índice de refracción. La fibra óptica de índice escalonado (step index, figura 2.9) tiene un índice de refracción constante, lo que permite que la distancia total recorrida por los rayos luminosos sea diferente para cada modo. En la fibra óptica de índice variable (graded index, figura 2.10), el índice de refracción disminuye en forma radial, produciendo que los modos recorran una mayor distancia acelerándose a medida que se acercan a la envoltura del núcleo, mientras los que viajan en forma mas recta lo hacen a menor velocidad debido a la menor densidad que existe en el centro del núcleo, lo que permite que los tiempos de desplazamiento tiendan a igualarse disminuyendo la dispersión modal.

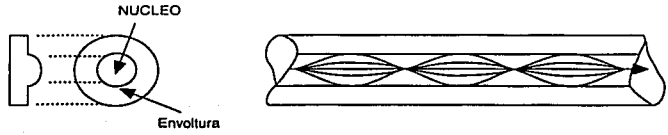


Fig. 2.9. Fibra óptica de índice escalonado

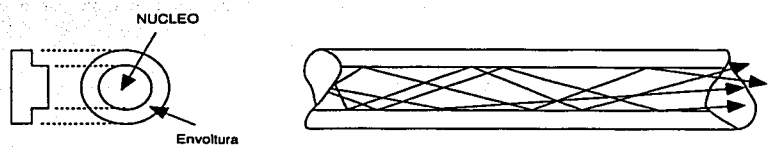


Fig. 2.10. Fibra óptica de índice variable

2.3.2. Medios de comunicación aéreos

Los medios aéreos son las técnicas mas utilizadas en la transmisión de señales para conectar redes locales, ya sea dentro de una ciudad, país o continente. También se aplica a la comunicación entre diferentes continentes pero puede traducirse en un gran costo.

Estos medios de transmisión se emplean porque es difícil instalar algún tipo de cable entre edificios pues estaría invadiéndose la propiedad privada

2.3.2.1. Microondas

Las microondas son ondas electromagnéticas que emplean el espacio aéreo como medio físico de comunicación.

Un sistema de microondas consiste en dos partes. La primera que representa a la empresa-cliente y la segunda es la empresa que brinda el servicio. La infraestructura de la empresa-cliente

comprende de una antena tipo plato o tambor (propiedad de la empresa que provee el servicio) y circuitos para la conexión a switches o concentradores.

Este tipo de enlaces pueden ser punto a punto o punto a multipunto, es decir, se contratan generalmente con la empresa de telefonía local para comunicar un sitio a otro o a varias localidades.

La ventaja que posee es la capacidad de transmisión en un rango considerable, extendido por antenas repetidoras estratégicamente colocada. Por tanto, montañas, edificios, mal tiempo, interferencia eléctrica puede afectar este tipo de comunicaciones. Como solución a lo anterior se puede emplear los satélites, lo cual elevaría el costo de instalación administración y mantenimiento de los enlaces.

2.3.2.2. Rayos infrarrojos

Consiste en la emisión de luz infrarroja utilizando como medio físico de transmisión, el aire. Los dispositivos emisores/receptores debe estar situados o dirigidos uno al otro, es decir, en una conexión punto a punto.

Generalmente se emplea en enlaces entre edificios que se encuentran a muy corta distancia por ejemplo, separados por una calle o carretera. Estos tipos de enlaces se ocupan cuando no se puede instalar un cable directo entre ellos.
El funcionamiento básico es similar a la fibra óptica. Se tiene un emisor-receptor en cada extremo. El haz de la luz tiene que ser muy pequeño para evitar la dispersión. Se emplea para edificios que se encuentran en separados a distancia de una calle, por ejemplo.

2.4. Dispositivos de comunicación

A lo largo de la historia de las redes de computadoras, han surgido necesidades cada vez más complejas para comunicar a la gente de una empresa o corporación, tal vez con otra compañía.

Los dispositivos de comunicación tienen como objetivo dos funciones primordiales. La primera, extender el numero de nodos en una red LAN. Y por otra parte, conectar redes locales y formar una red metropolitana o incluso una red WAN, de esta forma mantener comunicadas a la gente a través de datos, voz o video a distancias cortas o lejanas.

A continuación se describen los dispositivos actualmente empleados.

2.4.1. Hub o concentrador

Son dispositivos que tienen varios puertos (generalmente para conectores RJ-45) a los que se conecta el cable de otros nodos de red y cable del servidor. De esta forma se comparten los recursos de una red.

También se pueden conectar dos concertadores por medio de un cable UTP empleando un puerto de cada aparato. Asimismo se aumenta el número de nodos en caso que se necesite. Cabe resaltar que la forma que se esta conectando estos dispositivos es con la topología en estrella.

En la actualidad existen concertadores con 8, 16, 32, 64 puertos para aumentar el número de nodos en la red local y la extensión de la red.

Una ventaja que presenta un concentrador es una administración sencilla de los cambios de los diferentes nodos que existan en la red. Si algún empleado necesita cambiar de departamento y lleva consigo su computadora, ésta puede conectarse al concentrador más cercano a dicho departamento sin que exista ninguna clase de problema tanto para la conexión de la computadora como el funcionamiento de la red.

Existen nuevos concentradores que permiten "observar", a través de un software especifico, la actividad del trafico de datos. De tal forma que el administrador de la red puede manipular y controlar las diversas opciones del concentrador con el fin de obtener un correcto desempeño de la red. Este dispositivo trabaja en la capa dos (enlace de datos) del modelo de referencia OSI.

2.4.2. Bridge

Es un dispositivo que tiene como fin, segmentar una red, es decir, organizar a los usuarios en el sector que convenga y balancear la carga de tráfico en la red local.

Cuando un paquete se transmite, el bridge revisa la dirección destino, en una tabla de direcciones que corresponden a equipos que se encuentran en la red, si la dirección corresponde al segmento actual de la red, el paquete no cruza a la otra sección.

Generalmente los bridge son rápidos pues sólo tienen la función de toma de decisiones, es decir, solo compara direcciones destino con su registro de direcciones. Por tanto, tienen un costo superior al de un concentrador.

Si se desea conectar dos redes locales, estas deben tener la misma topología pues es muy probable que los campos de la trama (o paquete) no tengan compatibilidad entre topologías diferentes, así como funciones de los diferentes protocolos que se utilicen. Lo que no afecta es el tipo de cable que se emplee en cada red, por ejemplo una red puede tener cable coaxial mientas la otra puede tener cable de par trenzado.

Se aconseja instalar un bridge cuando existe un alto crecimiento en el tráfico de datos y un decremento en el rendimiento de la red.

Las ventajas que presenta son: una simplificación en la administración, se controla el crecimiento de la red, segmentación de la red lo que provoca menor tráfico de datos.

2.4.3. Switch

A medida que aumenta de tamaño una red local, también aumentan las necesidades de un mejor rendimiento de la red. Con un switch pueden resolverse problemas que el bridge no soluciona. Por ejemplo, mayor cantidad de puertos.

El switch analiza las direcciones MAC de los dispositivos contenidos en los paquetes transmitidos y toma decisiones de envío en base a su tabla de direcciones. No procesa información de datos de las capas superiores del modelo OSI, lo que se traduce en un mayor flujo de datos. Asimismo, puede dividir a una red LAN reduciendo el tráfico que circula en los segmentos de la red, enviando solo un porcentaje de dicho tráfico. Del mismo modo, el switch provee comunicación a un número mayor de dispositivos que el bridge, por tanto extiende la longitud de la red LAN.

Trabaja en la capa dos del modelo de referencia OSI al igual que el concentrador y el bridge.

Las principales diferencias entre un switch con el bridge son:

- Una mayor rapidez puesto que conmuta en el hardware lo que el bridge lo hace en el software.
- El switch tiene soporte en un mayor número de puertos.
- El switch tiene conmutación rápida lo que disminuye los retardos en la red. El bridge tiene conmutación del tipo almacenar y reenviar.
- El switch reduce el número de colisiones, genera un ancho de banda dedicado a cada segmento de la red.

2.4.4. Router

Trabaja en la capa tres (capa de red) del modelo OSI. Su función consiste en asignar una ruta óptima de ruteo y transportar los paquetes de información a través de la red.

Para enviar un paquete por la ruta óptima se utilizan algoritmos de ruteo, los cuales crean y conservan las tablas de ruteo, que contienen información de todas las rutas. Un router antes de transmitir, puede tener conocimiento del tráfico y determinar la mejor ruta para su destino. Si alguna ruta o algún dispositivo falla, el ruteador puede cambiar el trayecto para el envío de información.

Cabe mencionar para que exista una comunicación entre dos redes por medio de un router, deben tener el mismo protocolo de red, es decir, deben emplear el mismo protocolo en la capa de red del modelo OSI. Si esto se cumple la conexión puede ser entre topologías diferentes por ejemplo, una red Ethernet con una red Token Ring.

Las compañías utilizan routers que generalmente están conectados para formar una red WAN, de esta forma existe una diversidad de caminos para transferir información. Otra de las ventajas que tiene un router es la opción de restricción en la recepción de paquetes (que presentan ciertas características como direcciones IP) por medio de la configuración de los mismos.

2.4.5. Gateway

Un gateway trabaja en la capa siete (capa de aplicación) del modelo OSI. Es un dispositivo que tiene la capacidad de conectar a dos redes con topologías y protocolos de red totalmente diferentes.

Por ejemplo, la conexión con un gateway de una red Ethernet y una red Token Ring con protocolos IP e IPX respectivamente, sin ninguna clase de problema gracias al funcionamiento en la capa de aplicación. Inclusive entre dispositivos que tengan sistemas operativos diferentes como Windows y Macintosh.

CAPÍTULO 3
PROTOCOLOS

3.1. Características y utilización de protocolos

Los protocolos de comunicación son las reglas y procedimientos utilizados en la red para establecer la comunicación entre los nodos que disponen de acceso a ésta. De modo que para que dos nodos se puedan comunicar entre sí, es necesario que ambos empleen la misma configuración de protocolos.

Los protocolos de red son las normas que definen la comunicación entre dispositivos. Un protocolo define como los nodos se deben identificar en una red, la forma que los datos deben tomar en el tránsito (tramas), y como ésta información debería procesarse una vez alcanzado su destino final. Los protocolos también definen procedimientos para manejar transmisiones perdidas o paquetes dañados.

El comité 802 de IEEE (Institute of Electrical and Electronic Engineers) desarrolla protocolos estándares divididos en capas que se corresponden con el modelo de 7 niveles de la ISO (International Standards Organization).

Los protocolos de red transmiten la información a través de la red en pequeños segmentos llamados paquetes. Si un dispositivo quiere transmitir un archivo a otro nodo, el archivo es dividido en paquetes en el origen, y vueltos a ensamblar en el equipo destino. Cada protocolo define su propio formato de los paquetes en el que se especifica el origen, destino, longitud y tipo del paquete, así como la información redundante para el control de errores.

Para ejemplificar lo anterior, suponga que se quiere trasladar los restos de un arco románico desde un monte hasta otro país. Con este fin se numeran las piezas, se desmonta en orden, según algunas normas; las piezas se agrupan en contenedores (containers). En el puerto, los containers se agrupan y otra empresa de transportes los envía por vía marítima al país destino. Puede suceder que los containers se envíen en distintos barcos, con escalas diferentes. En el puerto del país destino la compañía naviera reagrupará los containers y los trasladará a la empresa de transporte terrestre, que los entregará al arquitecto en el lugar acordado. Allí, en un orden inverso al empleado en el origen se desagruparán las piezas y se montará el arco.

De esta forma el protocolo debe reunir ciertas características y/o propiedades que deben encontrarse en la mayoría de las especificaciones:

- Ausencia de retardo. Garantiza que el protocolo, bajo ninguna condición o circunstancia, llegará a un estado de inactividad total, permaneciendo ahí por tiempo indefinido.
- Complitud. Asegura que la especificación para cada estado dé una respuesta a todas las entradas posibles.
- Actividad. Asegura el cambio de protocolo de un estado a otro

Aunque cada protocolo de red es diferente, todos usan el mismo cableado en una red. El método común de acceder a la red física, permite que coexistan distintos protocolos, y por lo tanto al diseñador de una red puedes usar hardware común. Este concepto es conocido como "independencia de protocolo", que significa que la red física no depende de los protocolos que transporta.

El método de operación de un protocolo de manera general, es la siguiente:

Primeramente se recibe un mensaje, es procesado y envía una respuesta, sin que exista relación entre este evento y otro anterior o posterior.

- El proceso origen, conocerá la dirección de proceso destino y la incluirá en el mensaje.
- Esta dirección, identificará únicamente a un nodo, quien conocerá al nodo destino.
- El dispositivo origen entra en un estado de espera de respuesta en una de sus puertas, cuando envía un mensaje.
- El equipo destino ejecuta la función especificada en el mensaje, construye la respuesta (con resultados y dirección origen) y envía el mensaje respuesta por una puerta de salida, (quedando libre para aceptar otro mensaje).
- La respuesta llega al nodo origen, quien la revisa para asegurarse que viene del lugar correcto antes de aceptarla, y pasa al estado "no espera respuesta" en esa puerta de entrada.

Debe considerarse el hecho que, la red introduce demoras causadas por congestión, encaminamiento, etc., e incluso puede ocurrir pérdida del mensaje. Para esto, el proceso que realiza la consulta deberá tener un reloj que será activado al enviar el mensaje. El reloj enviará una señal al expirar el tiempo indicado en la activación indicando que la respuesta no llegó en el tiempo esperado por lo que el mensaje deberá ser retransmitido.

3.2. Protocolos y Estándares de comunicación

3.2.1. Modelo de referencia OSI

La Organización Internacional de Estándares (por sus siglas en inglés ISO), se fundó el 23 de Febrero de 1947 como una sesión de actividades de ISA (International federation of the national Standardizing Associations) a consecuencia de la Segunda Guerra Mundial.

La ISO tiene como objetivo "facilitar la coordinación y unificación internacional de estándares industriales". Es decir, la ISO tiene actividades de promover el desarrollo de estándares a nivel mundial que permita el intercambio internacional de bienes y servicios, y la cooperación en los campos de actividad intelectual, científica, técnica y económica, según sus propias palabras. En cada país existe sectores industriales que en el momento de facilitar información y equipo, se reúnen de tal forma que la más representativa es la ISO.

La ISO creó el modelo OSI (Open System Interconection) con el fin de tener una estandarización internacional para compartir información con seguridad y eficiencia.

En el modelo de referencia OSI los requisitos de un sistema abierto son:

- Conectividad. Permitir la comunicación con otros sistemas.
- Escalabilidad. La potencia del sistema puede variar sin convertirse en otro sistema.
- Portabilidad. Implementación del sistema en diferentes plataformas de hardware.

El modelo OSI se divide en 7 niveles o capas y cada una tiene una tarea o grupo de tareas para la comunicación entre dispositivos, de tal forma que una capa proporciona información clave a la capa posterior. Cabe destacar que el modelo de referencia sólo proporciona un marco conceptual para la comunicación, la comunicación como tal, se realiza al emplear los protocolos de comunicación. El proceso que se produce desde que un usuario envía un mensaje hasta que llega a su destino consiste en una bajada a través de todas las capas (con sus respectivos protocolos) hasta llegar al primero. Allí se encontrará en el canal de datos que le dirigirá al usuario destino, y volverá a subir por todas las capas hasta llegar a la ultima de ellas. A continuación de describirá cada una de las capas.

3.2.1.1. Capa física

Esta capa especifican las características eléctricas, mecánicas, de procedimiento y funcionales para establecer, mantener y desactivar una conexión física entre dispositivos de red.

Se definen características de hardware como conectores, cables y el tipo de codificación que se empleará. Cabe destacar que se necesita el mismo tipo de codificación para los extremos de otra forma no habrá una correcta decodificación. En esta capa únicamente se trabaja con bits.

También se especifica características como niveles y asignación de voltaje (que definirán 0 ó 1 lógicos), velocidades de transferencia, distancias máximas de transmisión. De igual forma se establece si los bits se enviarán en comunicación *duplex* (comunicación entre dos nodos pero en un sentido a la vez) o *full duplex* (comunicación entre dos dispositivos en los dos sentidos simultáneamente).

3.2.1.2. Capa de enlace de datos

La capa anterior (capa física) le proporciona a esta capa, bits que ahora serán interpretados como bloques de información que contienen datos así como información de control.

Esta capa proporciona el tránsito de datos a través del enlace de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes características de red y protocolo, incluyendo el direccionamiento físico, la topología de red, la notificación de error, la secuencia de tramas y el control de flujo. El direccionamiento físico (a diferencia del direccionamiento de red), define como se nombran los dispositivos en la capa de enlace de datos. La topología de red consiste en especificaciones de la capa de enlace de datos, que con frecuencia definen la forma de cómo se conectarán físicamente los dispositivos, en topología bus o en topología anillo. La notificación de error alerta a los protocolos de las capas superiores cuando se presenta un error en la transmisión y la secuencia de tramas de datos reordena las que se han transmitido fuera de secuencia. Finalmente, el control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con más tráfico del que pueda manejar simultáneamente.

A su vez, esta capa es divida por IEEE en dos subcapas: LLC (Logical Link Control) y MAC (Media Acces Control). En la figura 3.1 se muestra las subcapas de la red enlace de datos.

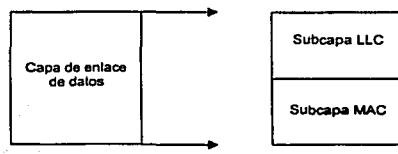


Fig. 3.1. Subcapas de la capa de enlace de datos

La subcapa LLC administra las comunicaciones entre dispositivos unidos por un enlace individual de red y soporta los servicios orientados (conexión lógica donde se envían los datos siguiendo la misma ruta durante toda la conexión) y no orientados a conexión (los paquetes de información pueden ser enviados, cada uno, por rutas diferentes), utilizados por los protocolos de las capas superiores. La subcapa MAC administra el protocolo de acceso al medio de transmisión

física de la red. La especificación IEEE MAC define las direcciones MAC, las cuales permiten a múltiples dispositivos identificarse de manera única entre sí en la capa de enlace de datos.

Protocolos de este nivel son CSMA/CD, el Token-passing-ring, Token-passing-bus, HDLC, FDDI MAC.

3.2.1.3. Capa de red

Esta capa se encarga de decidir por donde se han de transmitir los datos dentro la red proporcionando las rutas óptimas en cada ocasión, es decir, proporciona el ruteo que permiten múltiples enlaces dentro de una red. La capa de red soporta servicios orientados y no orientados a la conexión de los protocolos de las capas superiores. Los protocolos de la capa de red son de hecho protocolos de ruteo.

Algunos de los protocolos de esta capa son DDP, IP, IPX y Routing Protocol.

3.2.1.4. Capa de transporte

Las funciones de esta capa son el control de flujo, el multiplexaje, la administración de circuitos virtuales (rutas de transmisión) y la verificación y recuperación de errores.

El control de flujo administra la transmisión de datos entre dispositivos para que el dispositivo transmisor no envíe mas datos de los que el receptor pueda procesar. El multiplexaje permite que los datos de diferentes aplicaciones sean transmitidos en un enlace físico único. Es la capa de transporte la que establece, mantiene y termina los circuitos virtuales. La verificación de errores implica la creación de varios mecanismos para detectar los errores en la transmisión, en tanto que la recuperación de errores implica realizar una acción, como solicitar la retransmisión de los datos para resolver cualquier error que pudiera ocurrir.

Algunos ejemplos de protocolos para esta capa son UDP, TCP y NCP.

3.2.1.5. Capa de sesión

Crea, mantiene y finaliza las sesiones de comunicación entre nodos. Organiza funciones que permiten que dos usuarios se comuniquen a través de la red que incluyen tareas de seguridad, contraseñas de usuarios y la administración del sistema. Entre las tareas de administración del sistema se encuentran la capacidad de cancelar sesiones y controla la terminación ordenada de una sesión. Puede monitorear el uso del sistema y registrar el tiempo de uso de los usuarios.

Entre los protocolos de esta capa se encuentran ZIP (Zone Information Protocol), AppleTalk y SCP (Session Control Protocol).

3.2.1.6. Capa de presentación

Tiene funciones de codificación y conversión que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea legible por la capa de aplicación de otro sistema. Algunos ejemplos de esquemas de codificación y conversión de la capa de presentación incluyen formatos de presentación de datos comunes, esquemas de compresión de datos comunes y esquemas de encriptación de datos comunes.

Los formatos de presentación de datos comunes o el uso de formatos estándares de video, sonido e imagen, permiten el cambio de datos de aplicación entre diferentes tipos de sistemas de computadoras. Los esquemas de conversión se utilizan para intercambiar información entre sistemas utilizando diferentes representaciones de texto y datos, como EBCDIC y ASCII. Los esquemas estándar de compresión de datos permiten que los datos que se comprimen en el dispositivo origen se puedan descomprimir adecuadamente en el destino. Los esquemas estándar de encriptación de datos permiten que los datos encriptados en el dispositivo origen sean descifrados de manera adecuada en el destino.

Las implementaciones en la capa de presentación no suelen estar asociadas a un grupo particular de protocolos. Algunos estándares bien conocidos para video son QuickTime y MPEG.

Entre los formatos de imágenes gráficas bien conocidos están GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group) y TIFF (Tagged Image File Format).

Para una verdadera comunicación, ambas capas de presentación de las computadoras deben contener los mismos protocolos o reglas para el manejo de datos.

3.2.1.7. Capa de aplicación

Las aplicaciones de la capa de aplicación incluyen la identificación de usuarios, la determinación de la disponibilidad de recursos y la sincronización de la comunicación.

Esta capa es la mas cercana al usuario final, lo cual significa que tanto la capa de aplicación de OSI como el usuario interactúan de manera directa con la aplicación de software. En este nivel están los programas de administración de bases de datos, el correo electrónico, los programas de servidores de archivos, y de servidores de impresión. El software de aplicaciones como el procesamiento de texto o las hojas de cálculo no están en la capa de aplicaciones, solo los protocolos que les permiten funcionar.

Existen dos tipos clave de implementaciones de la capa de aplicación: las aplicaciones TCP/IP y las aplicaciones OSI. Las primeras son protocolos, como Telnet, FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol) y HTTP (HyperText Transfer Protocol); estos forman parte del grupo de protocolos de Internet. Las aplicaciones OSI son protocolos, como FTAM (File Transfer, Acces and Management), VTP (Virtual Terminal Protocol) y CMIP (Common Management Protocol).

3.2.2. TCP/IP

Cuando se habla de una red que emplea como protocolo de comunicaciones TCP/IP, en realidad se hace referencia al conjunto de protocolos que emplea, de los cuales los más conocidos son dos; TCP e IP, pero existen otra serie de ellos dentro del mismo conjunto. El propósito fundamental de esta familia de protocolos es la conexión de sistemas informáticos diferentes.

La idea inicial de lograr esta intercomunicación de redes partió del DoD (Departamento de Defensa de los Estados Unidos) concretamente DARPA (Defense Advanced Research Projects Agency) para lo cual crearon los protocolos TCP/IP empleados en la entonces recién creada ARPANET. Este conjunto de protocolos se mostraron eficientes en su cometido, y fueron sucesivamente adoptados por otros centros aparte de los militares como universidades y empresas privadas, debido además a que no imponían ninguna restricción respecto al hardware a utilizar. En la actualidad, la red ARPANET, o mas exactamente, la red en la que se ha convertido, se encuentra difundida por todo el planeta, e incluye entre las redes que conecta, redes locales, WAN y MAN, de

tal forma que conforma un red bastante grande llamada Internet. Es importante indicar que los protocolos TCP/IP aparecieron antes que el modelo OSI, y por tanto podrían no seguir este modelo en absoluto. Sin embargo, ambas arquitecturas no son tan diferentes, y de hecho, el modelo OSI es frecuentemente empleado para definir los cometidos de cada uno de los protocolos que emplea la familia TCP/IP.

3.2.2.1. Arquitectura DPA

La arquitectura DPA (Department of Defense Protocol Arquitecture) es la que emplea el TCP/IP. Según ésta, la comunicación se realiza siempre entre aplicaciones, y en este proceso intervienen tres partes o agentes:

- **Procesos.** Son los entes fundamentales que se comunican entre sí. Estos se hallan en el nivel más alto de la arquitectura. La comunicación entre procesos se realiza cuando el proceso exporta el mensaje al host donde reside. Mediante la red el dispositivo origen se comunica con el host destino.
- **Sistemas Centrales.** Son los dispositivos o host en los cuales los procesos son ejecutados.
- **Redes.** Son el medio a través del cual los procesos se comunican entre sí, uniendo los host.

Para una mejor comprensión de TCP/IP, se muestra en la tabla 3.2, la división en niveles de la arquitectura DPA, comparada con el modelo OSI.

Arquitectura OSI		Arquitectura DPA
Aplicación	7	Procesos / Aplicación
Presentación	6	
Sesión	5	
Transporte	4	Host a Host
Red	3	Internet
Enlace de datos	2	Acceso a red / Red local
Física	1	

Tabla. 3.2. Arquitectura OSI vs. Arquitectura DPA

Como se aprecia, las capas OSI correspondientes a la plataforma de aplicación corresponden con la capa de Procesos / Aplicación del modelo DPA. Por otra parte, este agrupa las capas de Enlace de datos y Física en una sola, el de red local. La equivalencia mas directa la encontraríamos por tanto en los niveles Host a Host e Internet respectivamente.

Una arquitectura de comunicaciones debe proporcionar una serie de facilidades al sistema que la implemente. Así las funciones principales que la arquitectura DPA proporciona son las siguientes: emulación de terminales, transferencia de archivos, correo electrónico y gestión del sistema.

Al igual que en las redes locales, en una red TCP/IP, existen diferentes servicios accesibles a los usuarios. Entre ellos están:

- Servidores de archivos.
- Servidores de nombres.

- Servidor de terminales.
- Arquitectura cliente/servidor).
- Servidores de impresión.

El protocolo TCP se encarga de proporcionar la comunicación fiable de extremo a extremo de la red, o lo que es lo mismo, de un usuario a otro. Es importante recordar que en una red TCP/IP, cada usuario puede pertenecer a un continente distinto, por lo cual la comunicación deberá atravesar varias docenas de redes diferentes, con toda la complejidad que ello implica para conseguir que dicho camino sea fiable. Eso significa que TCP debe ocuparse de realizar un seguimiento de lo que se envía, comprobar que ha llegado íntegro, y si no es así reenviarlo. Dichas funciones entrarían en el modelo OSI principalmente dentro de la capa de Transporte, aunque este protocolo no pertenezca a dicha arquitectura.

TCP/IP está diseñado para que pueda ser empleado sobre una amplia gama de redes con diversas tecnologías. De este modo existen redes TCP/IP sobre enlaces T1 en Estados Unidos o E1 en Europa y México (1.5 Mbps y 2 Mbps), redes X.25, ATM, redes vía satélite, etc. Por ello, TCP/IP se ha convertido en un estándar, de hecho, para la conexión de redes locales.

Una red TCP/IP, como Internet, esta compuesta por un conjunto de redes heterogéneas unidas entre sí por distintos dispositivos. En dicho conjunto de redes la información es enviada en datagramas. Los datagramas son un conjunto de datos que conforman un único mensaje, y que todas las redes pueden manejar. Para poder conectarse un usuario con otro, se emplea un sistema de identificación mediante las direcciones IP. Este es un conjunto de 32 bits, dividido en cuatro octetos, y representado en decimal con notación de puntos, de este modo: 132.248.114.6. En TCP/IP las agrupaciones de ocho bits, no son llamados bytes, debido a que existen sistemas que emplean bytes de tamaño diferente de 8 bits. De todas formas, lo mas habitual es, en lugar de utilizar direcciones IP emplear un sistema de nombres, como Pedro@compañía.com.mx, es decir, un formato con la siguiente sintaxis: nombre_usuario@nombre_host.entidad.sector, que el sistema se encarga de transformar en la dirección IP correspondiente.

Cuando un aplicación tiene un mensaje para transmitir, se lo pasa al TCP, el cual se encarga de dividirlo en datagramas y se los pasa al IP. Este los enruta al otro extremo de la comunicación. El TCP supervisa este enrutamiento, encargándose de reensamblar los datagramas en el extremo destino en el orden correcto, además de controlar que lleguen todos, reenviando los que no lo hayan hecho.

3.2.2.2. Internet Protocol (IP)

La tarea de IP consiste en el enrutamiento de todos los datagramas, únicamente. Para él, cada datagrama es independiente de los demás y puede ser tratado de forma diferente. Es TCP quién se encarga de supervisar la recepción correcta y completa del mensaje. Por este motivo, en redes pequeñas, la labor de IP es bastante sencilla, mientras que TCP carga con la mayor parte del trabajo.

Este protocolo y su nueva versión se estudiarán en el capítulo 5.

3.2.2.3. Transmission Control Protocol (TCP)

La labor de TCP se basa en dividir los mensajes enviados por las aplicaciones en segmentos, mandar estos al IP, reensamblar en el extremo destino la información en el orden correcto y controlar la integridad del mensaje recibido. Para ello, y teniendo en cuenta que los datagramas son enviados por IP en rutas potencialmente distintas, el TCP coloca sobre cada

datagrama una cabecera con las informaciones necesarias para controlar la transmisión como se muestra en la figura 3.3:

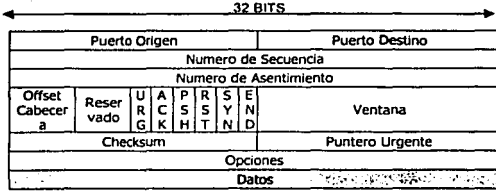


Fig. 3.3. Datagrama TCP

La descripción de los campos de la estructura del segmento TCP es la siguiente:

- Puerto origen y puerto destino. Para TCP, las direcciones de conexión entre las distintas máquinas son referenciadas como puertos. Su longitud es de 16 bits cada uno.
- Numero de secuencia. Mediante este campo, el TCP controla que los datagramas sean recibidos por el otro extremo de la comunicación en el orden correcto. Su longitud es de 32 bits.
- Numero de asentimiento. Controla la comunicación que se está realizando de modo correcto, el receptor devuelve al emisor el número de secuencia que espera recibir de éste, confirmando, por tanto, que el orden de los segmentos se ha mantenido hasta este momento. Mediante este campo, TCP puede controlar cuando, por ejemplo, ha habido un fallo de transmisión y en que punto ha sucedido. Cuando pasado un tiempo determinado y el emisor no recibe ningún numero de Asentimiento vuelve a enviar los octetos correspondientes. Su longitud es de 32 bits.
- Offset de cabecera. La cabecera TCP tiene una longitud variable, con un mínimo de 20 octetos, ya que el campo de Opciones puede no existir. Mediante este campo se indica cual es la longitud en octetos de toda la cabecera. Es decir el numero de palabras de 32 bit que tiene la cabecera TCP. Su longitud es de 4bits.
- Reservados. Su longitud es de 6 bits, y su valor es cero.
- Banderas. Cada una de las seis banderas tiene una longitud de 1 bit, y su función es la siguiente:
    - URG. Con valor '1' si se esta utilizando el modo de Puntero Urgente.
    - ACK. Con valor '1' si la trama devuelve un Numero de Asentimiento.
    - PSH. Con valor '1' indica que el datagrama es el ultimo de los que componen el mensaje.
    - RST. Con valor '1', reinicia una conexión con problemas.
    - SYN. Con valor '1' cuando se establece la conexión.
    - END. Con valor '1' finaliza de forma ordenada una conexión, es decir, cuando se ha solicitado dicha finalización.
- Ventana. Mantiene el control de flujo asegurando que una máquina rápida no va a saturar una lenta y mantiene una relación de velocidad aceptable en la comunicación. TCP se basa en emplear este campo para indicar la cantidad de información que puede procesar el receptor. Su longitud es de 16 bits.
- Puntero urgente. Indica al otro extremo que interrumpa la secuencia de proceso habitual del datagrama para saltar a un octeto determinado. Así, las comunicaciones asíncronas son procesadas con la rapidez necesaria (por ejemplo, pulsar una combinación de teclas que interrumpa una salida de información), y se evita utilizar mensajes específicos de interrupción. Su longitud es de 16 bits.

- Opciones. Las opciones pueden ser empleadas para diferentes funciones, cada una de ellas indicada por una palabra de 32 bits, como seguridad, informe de errores, control, etc., su longitud es variable. Una opción definida es el tamaño máximo del segmento TCP.
- Datos. Este campo no forma parte de la cabecera TCP

3.2.2.4. Otros protocolos TCP/IP

En algunas ocasiones, como peticiones cortas hacia un servidor, no necesitan de la seguridad ni de la fragmentación y reensamblaje en datagramas que proporciona TCP. Es incluso posible que tales peticiones quepan en un solo datagrama. Por este motivo, existe otro protocolo de la misma capa de TCP, llamado UDP.

UDP (User Datagram Protocol). Es un protocolo de la capa de transporte (modelo OSI) no orientado a conexión. UDP es básicamente, una interfase entre IP y los procesos de las capas superiores. Los puertos del protocolo UDP distinguen entre las diversas aplicaciones que corren en un solo dispositivo.

A diferencia de TCP, UDP no agrega IP funciones de confiabilidad, control de flujo y recuperación de errores. Debido a la longitud de la cabecera es mas corta, por tanto, tienen menos bytes lo que aumenta la velocidad de transmisión y generan un menor gasto indirecto en la red.

UDP es útil en situaciones donde no se requieran mecanismos de confiabilidad de TCP, como cuando un protocolo de las capas superiores ofrezca las funciones de recuperación de errores y control de flujo.

UDP es el protocolo de transporte de varios protocolos bien conocidos de la capa de aplicación, entre los que se incluyen NFS (Network File System), SNMP (Simple Network Management Protocol), DNS (Domain Name System) y TFTP (Trivial File Transfer Protocol).

ICMP (Internet Control Messages Protocol). Es un protocolo de la capa de Red (modelo OSI) que ofrece paquetes de mensajes para reportar errores y demás información respecto al procesamiento de paquetes IP de regreso al origen. Este protocolo genera varios tipos de mensajes útiles, entre los que se incluyen el de Destino inalcanzable; solicitud y respuesta de eco; Redirección; Tiempo excedido; Anuncio de ruteador y Solicitud de ruteador. Si un mensaje ICMP no puede ser entregado, no se genera un segundo mensaje. Esto es para evitar un flujo interminable de mensajes.

SLIP (Serial Line IP). Este protocolo es empleado cuando el enlace entre dos puntos se realiza a través de un puerto serie. Es el predecesor del protocolo PPP.

PPP (Point to Point Protocol). Este protocolo se emplea para la transmisión de datagramas por el puerto serie en enlaces punto a punto y esta formado por tres componentes principales:

- Un método para el encapsulamiento de datagramas a través de enlaces seriales. PPP utiliza el protocolo HDLC (Control de Enlace de Datos de Alto Nivel) como base para encapsular datagramas a través de enlaces punto a punto.
- Un LCP (Protocolo de Control del Enlace) para establecer, configurar y probar la conexión del enlace de datos.
- Una familia de protocolos de control de la red (NCP) para establecer y configurar diferentes protocolos de la capa de red; el protocolo PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de la capa de red.

DNS (Domain Name System). Es un sistema de ayuda a los usuarios de Internet a utilizar la red de una forma más sencilla permitiéndoles especificar sitios Web u otros servicios con los que se quieren comunicar mediante nombres con cierto significado. Cuando las computadoras se comunican unas con otras a través de Internet emplean el protocolo IP. Este protocolo distingue a un host de otro mediante la dirección IP y así puede enrutar los datos de uno a otro. Estas direcciones IP son únicas, lo cual quiere decir que cada host tiene su propia dirección IP y que esta es diferente del resto de direcciones IP existentes. Sin embargo, el uso de estas direcciones IP es complicado, ya que es difícil recordarlas, por lo que preferimos utilizar nombres con algún significado, a los que estamos acostumbrados en la vida diaria. El DNS es necesario para nuestras aplicaciones de manera que puedan convertir los nombres que se emplean en nombres comprensibles para las máquinas (direcciones IP) y proveer al usuario final de una forma cómoda de comunicarse vía Internet. Los dispositivos prefieren direcciones basadas en números por la sencilla razón de que el hecho de trabajar con números requiere un menor procesamiento de estos datos. Por ejemplo, digamos que una dirección denominada 'com' viene representada por el número 231, para representar esta palabra en binario, la máquina necesita por lo menos de 3 bytes, ya que cada carácter se representa con al menos 1 byte. Sin embargo, la representación del número 231 en binario requiere tan solo 8 bits (un único byte). Como resultado de esto se puede apreciar que a la hora de comparar el nombre 'com' con otro nombre, implica la comparación de al menos tres bytes, mientras que comparar el numero 231 con otro número requiere la comparación de un solo byte.

ARP (Address Resolution Protocol). Una de las características de TCP/IP es la de ser independiente del tipo de red que se está empleando, y por tanto del hardware. Para que dos máquinas de una determinada red se puedan comunicar, cada una debe conocer la dirección MAC de la otra. Por medio del mapeo de direcciones IP con direcciones MAC en la tabla ARP, si esta se encuentra en la tabla, la incluye en el campo correspondiente de la trama de la red 802.x correspondiente. Pero si desconoce la dirección MAC de otro, pero sí su dirección IP, mediante el ARP realiza una petición Broadcast a todos los sistemas disponibles, solicitando la dirección física de la dirección IP. Cuando recibe una respuesta del nodo cuya dirección IP ha enviado, actualiza su tabla ARP. Así, la dirección IP 198.25.689.43, podrá corresponderse, por ejemplo, con una dirección MAC ff:8e:30:fa:9b:cc, de un nodo de red 802.3.

Los protocolos de aplicación, que corren "por encima" del TCP/IP poseen unas direcciones especiales denominadas "well-known ports", de forma que cuando se selecciona una conexión hacia un servidor telnet, por ejemplo, debe especificarse cual de los well-known ports se elige para la misma. Por ejemplo, una sesión de emulación de terminal, es decir, telnet, tiene como numero de puerto el 23 en el caso de la máquina que va actuar como servidor, mientras que en la máquina que va a conectarse a ella, el cliente, el número de puerto será uno de los denominados efímeros. Estos empiezan desde el 1024 inclusive hacia arriba.

3.3. Control de enlace y transferencia de datos

Para una buena comunicación de las cuatro capas inferiores del modelo OSI (física, enlace de datos, red y transporte), necesitamos solucionar problemas que regularmente se presentan como son:

- Codificación
- Fragmentación
- Detección de errores
- Ruteo
- Transmisión segura

3.3.1. Codificación

La codificación es la forma en que la información es transmitida en términos de bits entre nodos para el envío de datos binarios en forma de señales. Realizándose por medio de un adaptador entre el nodo y el medio de transmisión. En la codificación se ha buscado:

- Minimizar la longitud del código
- Darle protección contra errores
- Llevar suficiente información de base de tiempo o reloj ck para garantizar sincronía.
- Un espectro adecuado al canal disponible con poca o nula componente de directa reduciendo las bajas frecuencias y eliminando las altas frecuencias.
- Ser inmune al cambio de fase y que el receptor pueda decodificar incluso señales invertidas.
- Evitar la propagación de errores.

Como todo esto no es posible, los códigos se subclasifican en:

- De mínima longitud
- De detección y corrección de errores
- De línea que cumple con los cuatro últimos puntos mencionados.

3.3.1.1. Ancho de banda

Es el intervalo de frecuencias que son conducidas adecuadamente por el canal, es decir en las que la potencia se conserva arriba del 50% de su valor máximo en dB es de 3dB (figura 3.4).

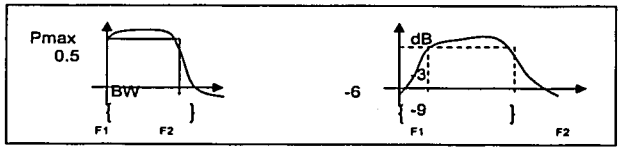


Fig. 3.4 Ancho de banda

La codificación se realiza en la capa física; entre los tipos de codificación más comunes están:

- NRZ (no retorno a cero)
- RZ
- AMI

NRZ-LU (non return to zero)

En la codificación NRZ (figura 3.5) los dígitos binarios son representados con dos estados alto y bajo, el 0 binario con un nivel bajo de voltaje es decir cero volts, mientras que el 1 binario con un nivel alto, un volt. Por ello es llamado unipolar.

Características:

- Si los ceros coinciden con cero volts es unipolar (TTL 0 y 5 volts)
- Si los ceros coinciden con valores negativos es polar. Esto implica que se reduzca la componente directa.
- No hay forma de descubrir si ocurrió un error por el ruido, es decir no detecta ni corrige errores cada bit se reconoce a si mismo.

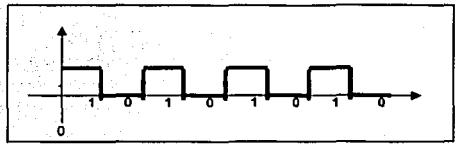


Fig. 3.5. Código NRZ-LU

Código RZ

Existe el unipolar y polar. En el código RZ unipolar (figura 3.6) los ceros binarios se codifican con cero volts, los unos binarios se codifican con un nivel alto durante el primer medio periodo.

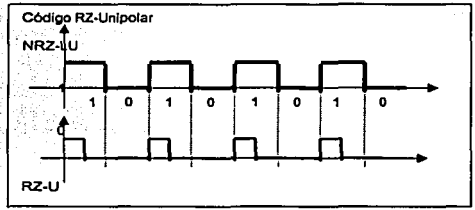


Fig. 3.6. Código RZ unipolar

Ventajas:

- Existe mejor sincronía que con NRZ-LU, dada que con trenes de unos la codificación coincide con las marcas de reloj con ello se facilita la extracción de reloj.
- Se tiene la mitad de la Componente de Directa que tiene NRZ-LU
- No existe propagación de errores ni capacidad de corrección
- La inversión de la fase puede ser detectable pero para recuperar la señal debe invertirse la señal nuevamente.

En el código RZ polar los unos binarios se codifican con un nivel alto o positivo el primer medio periodo, los ceros binarios se codifican con un nivel bajo o negativo en el primer medio periodo.

Ventajas:

- La componente de directa es mínima y desaparece en muchos casos.
- Existe mejor sincronía comparándolos con otros códigos, ya que el reloj puede extraerse completamente rectificando los ceros.
- No propaga errores aunque no existe capacidad reducida de corrección
- No es detectable la inversión de fase, no es inmune ni corregible.

Código RZ-Polar

Los unos se codifican con un nivel alto o positivo el primer medio periodo, los ceros se codifican con un nivel bajo o negativo el primer medio periodo, como se muestra en la figura 3.7.

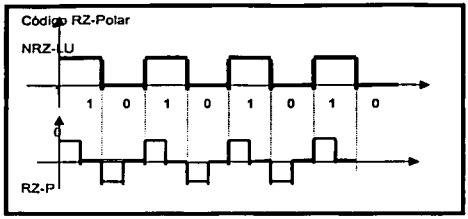


Fig. 3.7. Código RZ polar

Código RZ bipolar o código AMI (Alternated Milk Invertion)

Dicha codificación se realiza en dos pasos: pasar a RZ unipolar y alterna marcas (figura 3.8).

Ventajas:

- Componente directa nula
- Mejor sincronía que la de NRZ-LU
- Puede detectar un error entre dos bits correctos, pues se observa la violación o la regla de marcos alternadas.
- Capacidad limitada para corregir errores según lo anterior.

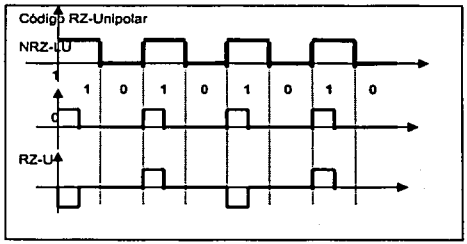


Fig. 3.8 Código AMI

3.3.2. Fragmentación

Al momento del envío de información a través de la red, es necesario conocer el inicio y el final de dicha información. En capa dos del modelo OSI (enlace de datos), la información viaja a través de Frames, los cuales son un conjunto de bits (o Bytes) en donde viene especificado el inicio y el final del mismo. También es necesario reconocer el tipo de información, esto es la señalización del frame y la información de las siguientes capas, dado que un paquete no contiene un tamaño fijo de información, se requiere utilizar técnicas para detección del mismo.

La fragmentación, que se lleva acabo en capa dos se puede desarrollar por medio de dos métodos distintos, de acuerdo a la representación de la información.

3.3.2.1. Byte Oriented

Sentienel

En este método, la información es considerada como un conjunto de Bytes. El frame es formado por Bytes de sincronización. El cuerpo del frame está agrupada entre dos etiquetas (Sentinel Characters), STX (Start of Text) y (End of Text). Como ETX puede aparecer en el cuerpo de la información, cada vez que esto sucede, se le agrega una etiqueta adicional DLE (Data Link Escape) el envío de la misma. Al momento de recibir el frame, se revisa la información.

Si se recibe un ETX, existen dos casos. Que ETX sea parte del cuerpo o sea el indicador de fin del cuerpo de la información. Para verificar tales situaciones, se analiza la información siguiente, si ésta es un DLE, quiere decir que es parte del cuerpo, para lo cual, se elimina el DLE y se continúa recibiendo información del cuerpo, si no es un DLE, quiere decir que se a recibido todo el frame.

Uno de los protocolos más comunes que utilizan este método es el BISYNC (Binary Synchronous Communication Protocolo).

Counting

En éste método, la información es enviada por Bytes, la diferencia entre Sentinel estriba, que no existen etiquetas que indiquen el inicio y el fin de la información. En este método, el número de Bytes que forman el cuerpo de la información es enviado en la transmisión. Al recibir el frame, se lee dicho parámetro y se conoce así el tamaño del frame.

La desventaja que tiene este método surge cuando COUNT es recibido incorrectamente, por ejemplo por un error en la línea.

3.3.2.2. Bit Oriented

En Bit Oriented, los frames son considerados como un conjunto de bits, a diferencia de los métodos anteriores que la información es considerada un conjunto de Bytes.

Dentro de Bit Oriented, dos protocolos son comúnmente utilizados por diversas tecnologías de red, tales como:

HDLC (High Lavel Data Link Control)

Es considerado uno de los protocolos de capa dos más importantes, ya que forman la base para la creación de protocolos más sofisticados tales como los presentados por tecnologías como X.25, Frame Relay, ISDN. HDLC es un protocolo bit-oriented, simples, half o full duplex.

Es utilizado para el intercambio de información y control de transmisión. Dos banderas son utilizadas para indicar el inicio y el final del frame. El campo de dirección contiene la dirección de la segunda estación(no utilizada si se tiene una conexión Peer to Peer), el campo de información que contiene los datos a ser transmitidos y el FCS para detección de errores.

El campo de control identifica tres tipos de frames a ser enviados: Información, Supervisión e innumerable.

Dentro de las redes LAN, como es el caso de Ethernet y de Token Ring, el Framing se realiza utilizando el método de Bit Oriented y su FCS (Frame Check Sequence) usando el método de redundancia cíclica.

3.3.3. Detección y corrección de errores

Los errores ocurren en un sistema de comunicación digital, principalmente debido al ruido que es introducido por los componentes de ese sistema y dentro del medio a través del cual se transmite la información.

Antes de que algo sea hecho para aliviar, o corregir errores, se debe determinar si los errores han ocurrido.

Esto requiere algunas técnicas para la detección de error. Hay un gran número de técnicas comúnmente usadas para detectar errores, la más comúnmente empleada es la comprobación de redundancia cíclica.

Para la correción de estos errores se emplea una técnica de reenvío de paquetes llamada Automatic Repeat Request (ARQ).

3.3.3.1. Comprobación de redundancia cíclica

El método CRC se basa en la división binaria. Una secuencia de bits de redundancia es añadida al final de la unidad de datos, de manera que la secuencia resultante sea exactamente divisible por un número binario predeterminado.

Los bits de redundacia que conforman el CRC se derivan de la división de la unidad de datos entre un divisor predeterminado: el residuo de esta operación es lo que conformará el CRC.

Para ser válido el CRC debe contar con 2 propiedades:

- Debe tener exactamente 1 bit menos que el divisor
- Añadido al final de la unidad de datos, debe hacer que la secuencia de bits resultante sea exactamente divisible por el divisor.

Tanto la teoría como la aplicación de este método son bastante directas. La única complejidad asociada estaría en derivar el CRC (figura 3.9).

Paso 1. Se añade una cadena de ***n 0's*** al final de la unidad de datos original. El valor de n deber ser 1 menos que el total de bits de divisor predeterminado.

Paso 2. La unidad resultante del paso 1 es divida por el divisor utlizado el proceso de división binaria. El residuo resultante de esta división será el CRC.

Paso 3. Se reemplaza la secuencia de ***n 0's*** del paso 1 por el CRC de ***n bits*** resultante del paso 2. (Puede darse el caso que el CRC se componga solo de 0's)

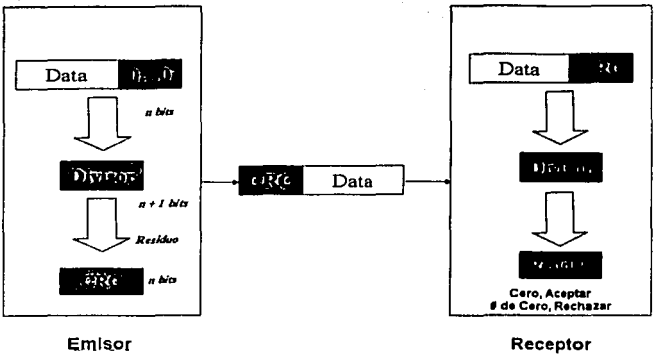


Fig. 3.9. Derivación de CRC

La unidad de datos original llega al receptor, seguida por el CRC. El receptor tratará la cadena entrante como una sola unidad y procesará la división de la cadena entrante entre el mismo divisor empleado por el emisor para calcular el CRC.

Si la cadena es recibida sin error, el verificador de CRC obtendrá como resultado un residuo = 0 y la unidad datos será procesada; de lo contrario, si la unidad de datos sufrió alteraciones durante la transmisión, el verificador obtendrá como resultado un residuo # 0 y la unidad de datos no será procesada.

La representación de un Polinomio como un Divisor es como se muestra en la figura 3.10.

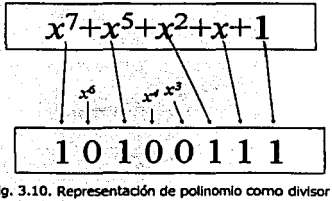


Fig. 3.10. Representación de polinomio como divisor

El generador de CRC (divisor) no es representado como una cadena de 1's y 0's sino, como una expresión algebraica polinomial. El formato de polinomio resulta útil para la representación por dos razones:

- Provee un mecanismo corto de representación.
- Puede ser usado para presentar el concepto matemáticamete (lo cual esta fuera del alcance de esta clase)

Los polinomios seleccionados deben tener al menos las siguientes propiedades:

- No debe ser divisible por ***x***.
- Deber ser divisible por ***(x + 1)***

La primera condición garantiza que los errores de ráfagas de longitud igual al grado del polinomio sean detectados. La segunda condición garantiza que todos los errores de ráfaga que afecten un numero impar de bits sean detectados.

No podemos elegir x (10 binario) o x^2+x (110 binario) como polinomios porque ambos son divisibles por x. Pero si se podría elegir x + 1 (11 binario) ya que este no es divisible por x pero si por x+1. Igual pasaría con x^2+1.

Existen polinomios estándares usados por protocolos utilizados para generar CRC. Los Códigos CRC pueden detectar errores de ráfaga de longitud menor o igual al grado del polinomio y todos los patrones de error con un número impar de errores si el polinomio tiene un número par de coeficientes.

3.3.3.2. Automatic Repeat Request (ARQ)

Lo que es necesario ahora es un código que detecte el mayor número posible de errores ya que si se detecta un error lo que se hace es pedir una retransmisión por parte del emisor, y si no se detecta error alguno, se supone que la trama ha llegado sin errores. Existen tres tipos principales de ARQ:

- ARQ de parada y espera
- ARQ de envío continuo y rechazo simple
- ARQ de envío continuo y rechazo selectivo

PROTOCOLO MÁS SENCILLO LÓGICAMENTE CORRECTO

Lo más simple es enviar los datos trama a trama y que el receptor no juegue ningún papel. Como se ve en la figura 3.11 si no se toma ninguna medida más, si llega algún error el bloque transmitido se pierde.

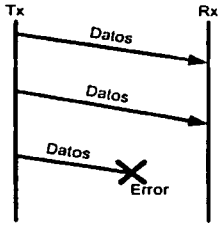


Fig. 3.11. Envío de datos segundo caso

Para evitar la pérdida de información se pueden introducir los asentimientos del receptor. El emisor espera a que le llegue un asentimiento para enviar la trama siguiente (figura 3.12).

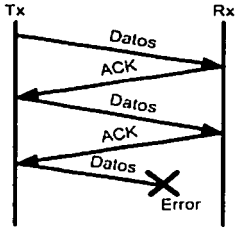


Fig. 3.12. Envío de datos tercer caso

Ahora no se pierde ninguna trama, pero un error hace que el sistema se bloquee ya que el emisor espera indefinidamente (lo que implica además una memoria en el emisor que sea infinita ya que tiene que almacenar toda la información que le va llegando pero no puede transmitirla).

Evitar este problema es simple: no hay más que introducir un tiempo de espera máximo pasado el cual el emisor retransmite la trama. En este intervalo hay que tener en cuenta el tiempo de transmisión y propagación de la trama y del asentimiento y el tiempo máximo de proceso en el receptor.

El problema que se introduce ahora es bastante claro: un retraso del receptor puede provocar la aparición de tramas duplicadas por un reenvío del emisor. Esto es también un problema ya que no olvidemos que el receptor no puede distinguir si una trama es el duplicado de una anterior o no.

Para resolver este problema, lo que se hace es introducir redundancia en las tramas de tal manera que se distingan la última trama enviada de la que se transmite después. Para ello, se introduce un nuevo bit en la trama de tal manera que las tramas quedan marcadas de dos formas distintas y el receptor espera siempre una de las dos, si llega otra la descarta pensando que es un duplicado (figura 3.13).

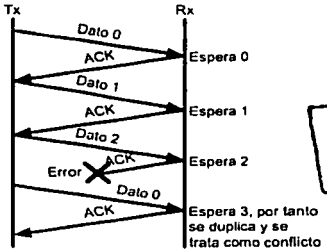


Fig. 3.13. Envío de datos cuarto caso

Como se aprecia en la figura 3.13, se regresa al problema del inicio: se pueden perder tramas.

La solución final y que parece resolver todos los problemas es introducir un bit en los asentimientos que distingan los asentimientos a dos tramas consecutivas (de la misma forma que se distinguían dos tramas consecutivas).

Para facilitar la introducción a estas técnicas se suponen las siguientes hipótesis simplificatorias:

- Se supone el flujo unidireccional
- Se supone que las tramas de control llegan sin errores
- Se supone que la probabilidad de no-detección de error es tan baja que se puede considerar que el código detecta todos los errores.

ARQ de parada y espera

En este sistema de transmisión (figura 3.14), el emisor envía una trama y espera a que le llegue el asentimiento del receptor para enviar la siguiente (es posible el funcionamiento de este sistema dadas las hipótesis simplificadoras). El receptor puede enviar un asentimiento positivo (ACK): la trama me ha llegado sin errores o bien un asentimiento negativo (NAK): ha ocurrido un error. Si al emisor le llega un NAK, retransmite la última trama, en caso contrario transmite la siguiente. En este sistema el emisor solo tiene que tener en memoria la última trama que ha enviado ya que es la única que tiene pendiente de ser asentida.

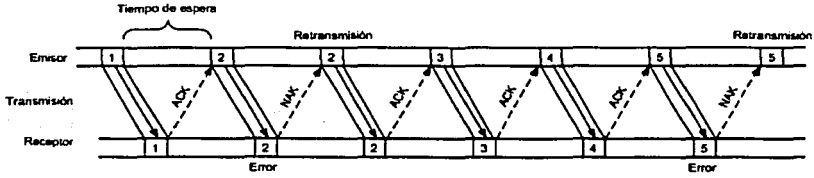


Fig. 3.14. ARQ de parada y espera

ARQ de rechazo simple

En este caso, se supone que el emisor no espera a recibir un asentimiento del receptor sino que continúa transmitiendo tramas que a su vez almacena en buffer hasta que sean asentidas, es una ventana deslizante en el emisor. Para diferenciar una trama de las demás les añade un número de secuencia infinito, pero que no aumente el número de bits de redundancia (es uno de los problemas en la práctica). El receptor asiente cada trama con su número correspondiente lo que libera la trama correspondiente en el buffer del emisor. Si una trama es errónea, el emisor vuelve atrás y retransmite a partir de esa trama (lo que hace inviable este sistema para probabilidades de error elevadas). El receptor solo tiene que almacenar una trama en su registro pues al final siempre le llegan en orden (figura 3.15).

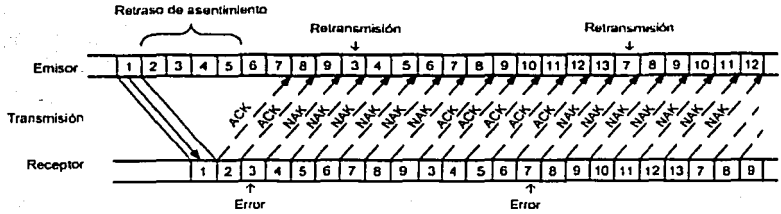


Fig. 3.15. ARQ de rechazo simple

ARQ de rechazo selectivo

Para evitar perder tiempo en transmisión, se busca repetir solo las tramas con error y no el resto. Para eso se usa el emisor del ARQ anterior: transmisión continua salvo que solo retransmite la trama defectuosa (se sabe por el número de secuencia del asentimiento). El receptor se complica ya ha de guardar en un registro todas las tramas posteriores a un error hasta que le llegue la retransmisión de la trama para poder entregarlas en orden. Esto complica el sistema bastante: son necesarias ventanas deslizantes tanto en receptor como en emisor y para probabilidades de error bajas no da una gran diferencia en eficacia respecto del sistema ARQ anterior (figura 3.16).

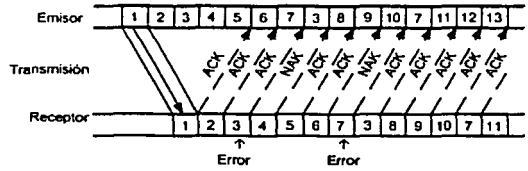


Fig. 3.16. ARQ de rechazo selectivo

3.3.4. Ruteo

El ruteo es el camino a seguir para que la información llegue correctamente a su destino desde un nodo inicial. Un algoritmo de ruteo es el método que se sigue para obtener dicha ruta. Dentro de los algoritmos de ruteo se encuentran los siguientes:

Source Routing

Dentro del header, la dirección completa desde el nodo fuente al nodo destino es almacenada. Dicha información es relacionada con los puertos del ruteador por donde se envía la información.

Entre los inconvenientes de éste método están: que cada nodo debe contener un amplio conocimiento de la topología de red.

EL header es de longitud variable (en relación al número de nodos por donde se envía la información), lo cual, tiene consigo problemas en cuanto al tamaño del frame.

Virtual Circuit

Trabaja bajo el modelo de interconexión de Connection Oriented. Primeramente se realiza la conexión y posteriormente se envía la información. Este método requiere una tabla (tabla 3.17) en cada ruteador que contenga la siguiente información:

Entrada		Salida	
Puerto	VCI	Puerto	VCI

Tabla 3.17. Tabla de ruteo

Donde VCI = Virtual Circuit Channel, es decir dada la entrada por el número de puerto y VCI, la salida debe ser dada como lo especifica la tabla.

El circuito virtual logra obtener un parámetro de longitud estático dentro de nuestro Header. Los ruteadores identifican si un nodo está vivo o es inalcanzable antes del envío de la información.

Dentro de sus desventajas esta el que es necesario esperar un tiempo de RTT (Round Trip Time) al momento de crear la ruta inicial. La conexión se pierde al momento que falla un nodo o enlace.

Datagramas

Trabaja bajo el modelo de interconexión Connectionless. En este método cada paquete contiene la dirección destino. Aquí no existe un tiempo RTT, la desventaja es que existe un mayor envío de información y no se tiene idea si existe el nodo destino.

En los algoritmos de ruteo, se requiere que cada uno de los ruteadores tenga una tabla de ruteo, en donde se encuentra la forma de llegar al nodo final, pero la forma de obtener dichas tablas son generadas por algoritmos específicos denominados Algoritmos de ruteo, por ejemplo Distance Vector y Link State.

3.3.5. Transmisión segura

Una vez que se tenga la ruta por donde viajará la información, se necesita tener la seguridad de que los frames lleguen a su destino, ya que se da el caso de:

- El transmisor envía la información, pero por motivos de línea ésta nunca llega al receptor.
- La información llega correctamente, pero al enviar la confirmación ésta no llega al transmisor.

Por ello es necesario emplear técnicas que aseguren una transmisión confiable. En la mayoría de esas técnicas se utilizan dos parámetros como son: el identificador y el tiempo de vida. Dos técnicas son usadas en forma general:

Stop and wait

Después de transmitir un frame, el emisor espera por un ack = identificador antes de transmitir el siguiente frame. El emisor retransmite si después de un cierto tiempo (tiempo de vida) no ha recibido el ack. El receptor debe tener la capacidad de descartar frames cuando estos son repetidos.

Una de las desventajes de esta técnica es que no aprovecha a toda su capacidad el ancho de banda, ya que es necesario esperar el ack para enviar el siguiente frame.

Sliding Window

En éste método el emisor envía un número de frames antes de recibir un ack. El receptor manda los ack de los frames que ha recibido. Si el emisor no recibe el ack de un cierto frame, vuelve a enviar éste. El receptor debe tener la capacidad de descartar frames si éstos ya han llegado pero el ack se perdió en el camino de regreso.

3.4. Estándares para redes LAN

El IEEE (Institute of Electrical and Electronic Engineers) es una organización internacional que ha desarrollado una familia de estándares referentes a redes locales. Se trata del Proyecto 802 del comité "Computer Society Local Network". La diversidad de protocolos de enlace, métodos de acceso, medios físicos, dispositivos conmutables, aplicaciones, etc., ha impuesto la necesidad de unificar criterios para hallar una solución armónica y eficiente, que ahorre esfuerzos aislados y busque un nivel de compatibilidad a través del desarrollo de estándares de uso universal para beneficio del usuario final.

El comité del proyecto 802 se dividió de la siguiente manera:

- Un subcomité se dedicaba a los estándares de redes locales relacionadas con el modelo OSI.
- Cinco subcomités trabajando en estándares de redes locales.
- Dos subcomités consultivos técnicos o de asesoría.

En este proyecto se dividió el nivel de "enlace de datos" en dos grupos:

- El subnivel inferior, denominado MAC (Media Acces Control, control de acceso al medio), que proporciona el acceso compartido al nivel físico de la red de modo que múltiples estaciones puedan compartir el medio físico.
- Y el subnivel superior llamado nivel LLC (Logical Link Control, control de enlace lógico), que proporciona un servicio de enlace de datos, ensamblado y desensamblado, multiplexación y comprobación de direcciones.

El comité del proyecto 802 ha dado lugar a una serie de documentos. Tratan fundamentalmente sobre los niveles físico y de enlace de las redes de área local, según el modelo OSI del ISO:

- **802** Descripción general y arquitectura.
- **802.1** Glosario, gestión de red e *internetworking*.
- **802.2** Control de enlace lógico (LLC).
- **802.3** CSMA/CD. Método de acceso y nivel físico.
- **802.3u** Fast Ethernet. Método de acceso y nivel físico.
- **802.3z** Gigabit Ethernet. Método de acceso y nivel físico.
- **802.4** Token Bus. Método de acceso y nivel físico.
- **802.5** Token-Passing Ring. Método de acceso y nivel físico.
- **802.7** Banda Ancha. Aspectos del nivel físico.
- **802.9** Acceso integrado de voz y datos. Método de acceso y nivel físico.
- **802.10** Seguridad y privacidad en redes locales.
- **802.11** Wireless LAN (Redes Inalámbricas). Método de acceso y nivel físico.
- **802.12** 100VG-AnyLAN. Método de acceso y nivel físico.

3.4.1. Fast Ethernet

3.4.1.1. Introducción

Cuando Ethernet comenzó su apertura comercial a principios de los ochenta muchos consideraban que 10 Mbps era una velocidad excesiva y que esto encarecía innecesariamente la red; por aquel entonces ningún ordenador era capaz de enviar a esa velocidad, por ejemplo en 1983 un mainframe VAX 8600 (considerado en su tiempo una máquina potente) podía transmitir unos 6 Mbps en el mejor de los casos; con los protocolos de transporte habituales los rendimientos eran sensiblemente inferiores.

En 1988 Van Jacobson envió un artículo a usenet informando que había conseguido una velocidad de transferencia de 8 Mbps sobre Ethernet entre dos estaciones de trabajo Sun utilizando una versión optimizada de TCP. A partir de ese momento las mejoras en el hardware (CPUs, discos, tarjetas controladoras, etc.) y en el software (sistemas operativos, protocolos de transporte, etc.) empezaron a hacer cada vez más fácil que un solo equipo saturara una Ethernet.

Entonces la única solución estándar para pasar a velocidades superiores era FDDI (que por cierto es un estándar ANSI e ISO, pero no IEEE). Sin embargo FDDI nunca se mostró como una alternativa interesante para los usuarios de Ethernet. Aunque robusta y fiable, tenía una gestión compleja y permanecía en unos precios inaccesibles para la mayoría de las instalaciones, o solo asumibles cuando se trataba de la red principal o 'backbone', pero no para el acceso del usuario final. Además su compatibilidad con Ethernet es reducida, ya que FDDI no es CSMA/CD y utiliza una estructura de trama diferente. Esto complicaba las cosas cuando se quería migrar desde Ethernet, y más aun si habían de coexistir ambas redes.

En un intento por cubrir esta demanda Grand Junction, que en la actualidad es parte de WBU (Unidad de Negocios de Grupo de Trabajo) de sistemas Cisco, sacó en 1992 una versión de Ethernet que funcionaba a 100 Mbps. Esto tuvo un éxito considerable y provocó la creación ese mismo año en el seno del IEEE de un grupo de estudio sobre redes de alta velocidad, con la misión de estudiar la posibilidad de ampliar el estándar a 100 Mbps. Se plantearon dos propuestas:

- Mantener el protocolo CSMA/CD en todos sus aspectos, pero aumentar en un factor 10 la velocidad de la red. Al mantener el tamaño de trama mínimo (64 bytes) se reducía en diez veces el tamaño máximo de la red, lo cual daba un diámetro máximo de unos 400 metros. El uso de CSMA/CD suponía la ya conocida pérdida de eficiencia debida a las colisiones.
- Aprovechar la revisión para crear un nuevo protocolo MAC sin colisiones más eficiente y con mas funcionalidades (mas parecido en cierto modo a Token Ring), pero manteniendo la misma estructura de trama de Ethernet.

La primera propuesta tenía la ventaja de acelerar el proceso de estandarización y el desarrollo de productos, mientras que la segunda era técnicamente superior. El subcomité 802.3 decidió finalmente adoptar la primera propuesta, que siguió su camino hasta convertirse en lo que hoy conocemos como Fast Ethernet, aprobado en junio de 1995 como el suplemento 802.3u a la norma ya existente. Para acelerar el proceso se utilizaron para el nivel físico buena parte de las especificaciones ya desarrolladas por ANSI para FDDI. Los medios físicos soportados por Fast Ethernet son fibra óptica multimodo, cable UTP categoría 3 y categoría 5 y cable STP (Shielded Twisted Pair).

Los partidarios de la segunda propuesta, considerando que sus ideas podían tener cierto interés, decidieron crear otro subcomité del IEEE, el 802.12, que desarrolló la red conocida como 100VG-AnyLAN. Durante cierto tiempo hubo competencia entre ambas redes por conseguir cota de mercado; hoy en día la balanza se decanta ampliamente hacia Fast Ethernet. Algunos fabricantes (notablemente HP, autor de la propuesta) aun mantienen un amplio catálogo de productos para

100VG-AnyLAN. Merece la pena recalcar que 100VG-AnyLAN, aunque puede funcionar con estructura de trama Ethernet (y también con Token Ring, de ahí la denominación de AnyLAN) no utiliza CSMA/CD y por tanto no puede denominarse Ethernet.

La red Fast Ethernet se extendió con una rapidez incluso superior a las expectativas más optimistas. Como consecuencia de esto los precios bajaron y su uso se popularizó hasta el usuario final. Esto generaba un requerimiento de velocidades superiores en el backbone que no podían ser satisfechas por otras tecnologías (salvo quizá por ATM a 622 Mbps, pero a unos precios astronómicos). La experiencia positiva habida con Fast Ethernet animó al subcomité 802.3 a iniciar en 1995 otro grupo de trabajo que estudiara el aumento de velocidad de nuevo en un factor diez, creando lo que se denomina Gigabit Ethernet. Aunque en 1995, recién aprobado Fast Ethernet, parecía descabellado plantear estas velocidades para redes convencionales, las previsiones de aumento en rendimiento y nivel de integración de los chips hacían prever que para 1998 sería factible construir controladores de red para esas velocidades con tecnología convencional a precios asequibles. Siguiendo un calendario similar al empleado en Fast Ethernet y con un grupo de personas muy parecido se inició un proceso que culminó el 29 de junio de 1998 con la aprobación del suplemento 802.3z.

Comparándolo a las especificaciones de los sistemas a 10Mbps, el sistema a 100-Mbps presenta un factor de reducción 10 en los tiempos de bit, que es la cantidad de tiempo que se tarda en transmitir un bit en el canal Ethernet. Esto produce un aumento en un factor 10 en la velocidad de transmisión de los paquetes a través del sistema. Sin embargo, el resto de características importantes del sistema Ethernet incluyendo el formato de trama, la cantidad de datos que una trama permite, y el mecanismo de control de acceso al medio se siguen manteniendo.

Las especificaciones de Fast Ethernet incluyen mecanismos de Auto-Negociación de la velocidad del medio. Esto hace posible a los vendedores el proporcionar tarjetas Ethernet de velocidad dual que pueden ser instaladas y correr tanto a 10Mbps como a 100Mbps de manera automática.

Existen tres tipos de medio físico que han sido especificados para transmitir las señales Ethernet a 100 Mbps como se especifica en la figura 3.18.

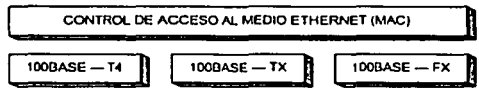


Fig. 3.18. Medios físicos para Fast Ethernet

Los tres tipos de medio se muestran con sus identificadores IEEE. Los identificadores IEEE tienen tres partes de información. La primera parte, "100", se refiere a la velocidad del medio, que es de 100 Mbps. La parte "BASE" se refiere a "banda base", que es el tipo de señal aplicada. La señal en banda base significa simplemente que las señales Ethernet son las únicas señales presentes en el medio físico.

La tercera parte del identificador proporciona una indicación del tipo de segmento. El tipo de segmento "T4" es un segmento de par trenzado que utiliza cuatro pares de cable par trenzado de calidad telefónica. El tipo de segmento "TX" es un segmento de par trenzado que utiliza dos pares de cables y que está basado en el estándar medio físico par trenzado de datos desarrollado por ANSI (American National Standards Institute). El tipo de segmento "FX" es un segmento

enlazado de fibra óptica basado en el estándar medio físico de fibra óptica desarrollado por ANSI, el cual usa dos hebras de cable de fibra. Los estándares TX y FX son conocidos conjuntamente como 100-BASE-X.

Los estándares 100BASE-TX y 100BASE-FX utilizados en Fast Ethernet han sido adoptados de los estándares de medio físico desarrollados por ANSI. Los estándares de medio físico de ANSI fueron desarrollados originalmente para el estándar de red X3T9.5, conocido como FDDI (Fiber Distributed Data Interface), y son ampliamente utilizados en LANs FDDI.

Fast Ethernet adaptó estos dos estándares de ANSI para utilizarlos en las nuevas especificaciones del medio físico. El estándar T4 fue también proporcionado para hacer posible el uso de cable par trenzado de menor calidad para las señales Ethernet a 100Mbps.

3.4.1.2. Componentes usados en la conexión a 100 Mbps

El siguiente diagrama muestra los componentes que pueden ser usados para hacer la conexión al medio a 100 Mbps.

La figura 3.19 muestra los componentes definidos en el estándar IEEE para hacer la unión a un segmento de 100 Mbps. Estos componentes difieren un poco de los usados en un sistema de 10 Mbps.

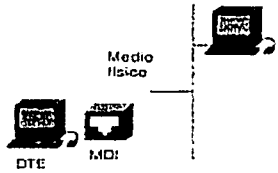


Fig. 3.19. Componentes para red de 100 Mbps

Medio físico

Empezando por la parte derecha del diagrama de la figura, encontramos el medio físico utilizado para transportar las señales Ethernet entre computadoras. Este podría ser uno de los tres tipos de medio a 100 Mbps. Se hace una conexión al medio con el interfaz dependiente del medio (MDI). Este es un conector de par trenzado de 8 pines o un conector de fibra óptica en el sistema 100Base-T.

Dispositivo de capa física

Este es el siguiente dispositivo mostrado en la figura. Puede ser un conjunto de circuitos integrados dentro del puerto de una tarjeta de red, siendo invisible al usuario.

Equipo Terminal de Datos, o Computadora

El dispositivo que propiamente se conecta en red esta definido como equipo terminal de datos (DTE) en el estándar del IEEE. Cada EQUIPO conectado a una red Ethernet esta equipada con una interfaz Ethernet. La interfaz Ethernet proporciona una conexión al medio Ethernet y contiene los dispositivos electrónicos y el software necesario para poder realizar las funciones de control de acceso al medio requeridas para enviar una trama a través del canal Ethernet.

Se debe tener presente que los puertos Ethernet en los concentradores no utilizan una interfaz Ethernet. El puerto de un concentrador se conecta al medio Fast Ethernet utilizando el mismo equipamiento PHY y MDI.

Los hubs o switches gestionados hacen posible al administrador de red la monitorización remota de los niveles de tráfico y las condiciones de error en puertos hub, además de poder desactivar los puertos que tengan problemas.

3.4.1.3. Control de acceso al medio (MAC)

El formato de trama como el control de acceso al medio de las redes Fast Ethernet siguen manteniéndose igual que para las redes Ethernet a 10 Mbps.

La subcapa MAC utiliza el método CSMA/CD para la transmisión y recepción de tramas, que consiste en lo siguiente:

Antes de iniciar la transmisión, el emisor efectúa una revisión del medio con el fin de detectar si se está transmitiendo alguna otra trama. Si se está realizando otra transmisión se debe esperar a que concluya. Cuando se detecta que no hay actividad se inicia la transmisión. Paralelamente se está revisando el medio para comprobar si ha habido colisión con otras tramas. Si no se produce colisión, se lleva a cabo toda la transmisión. Si se detecta colisión, se procede a la transmisión de una trama *jam* que permite que todos los Equipos detecten la colisión. Posteriormente, se corta la transmisión de la trama inicial, y tras un intervalo de tiempo aleatorio se reinicia la transmisión. La duración del intervalo de tiempo será un múltiplo del doble del tiempo de propagación de la señal sobre el camino más largo de todos los que componen la red, más un margen de seguridad:

- **CS (Carrier Sense):** Cuando la interfaz del servidor tiene un paquete para transmitir, escucha el ether para determinar si hay mensajes siendo transmitidos. Si no detecta transmisión alguna, la interfaz comienza a enviar.
- **MA (Multiple Access):** Todas las computadoras conectadas al cable pueden transmitir cuando hay datos por enviar, por lo anterior es posible que 2 nodos determinen que la red esta ociosa y comiencen a transmitir al mismo tiempo.
- **CD (Collision Detected):** Si dos computadoras envían datos al mismo tiempo, sus transmisiones pueden chocar. Cada nodos monitora el cable mientras esta transfiriendo para verificar que una señal externa no interfiera con la suya. Cuando una colisión es detectada, la interfaz aborta la transmisión y espera hasta que la actividad cese antes de volver a intentar la transmisión. Cada computadora espera un tiempo al azar antes de retransmitir. Como cada una espera tiempo determinado, la posibilidad de colisionar de nuevo es mínima.

3.4.1.4. Formato de trama

En la figura 3.20 representa el formato de trama utilizado en las redes Fast Ethernet es la trama 802.3, con una longitud mínima de 64 bytes y una longitud máxima de 1512 bytes.

Comienzo de trama	Preámbulo	Dirección Destino	Dirección Origen	Longitud	Datos	Relleno	Secuencia de detección de errores	Fin de trama

Fig. 3.20. Trama Fast Ethernet

Cada trama se divide en 8 campos, de longitud fija todos excepto dos, los de datos y relleno.

Los campos de la trama son los siguientes:

- *Preámbulo.* Tiene una longitud de 7 bytes, formada por la siguiente combinación de unos y ceros: 10101010. Este campo hace posible la sincronización para que el resto de los campos sean recibidos correctamente.
- *Delimitador de Comienzo de campo.* Esta compuesto por el siguiente octeto:
- 10101011. Aparece a continuación del preámbulo.
- *Dirección destino.* Tienen una longitud de 2 o 6 bytes, en cualquier caso fija para cada aplicación. El primer bit de la dirección destino indica si es una dirección individual o la dirección de un grupo de nodos. Cuando todos los bits de la trama se encuentran a 1, se trata de una trama de difusión, y la trama será recibida por todos los equipos de la LAN.
- *Dirección fuente.* Tiene el mismo formato que el campo de dirección destino, y sirve para especificar la dirección de la estación emisora.
- *Longitud de Datos.* Está compuesto de 2 bytes en los que se codifica el número de bytes que ocupa el campo de datos.
- *Datos.* Este campo es de longitud variable, y son los datos que se transmiten en la trama.
- *Relleno.* Como el campo de datos es de longitud variable, es posible que la trama final resultante no cumpla el requerimiento de longitud mínima de la trama, que es de 64 bytes. En este caso, a continuación del campo de datos se colocan los bits de relleno que falten para completar la trama de longitud mínima.

3.4.1.5. EL SISTEMA 100Base-TX

La interfaz 100Base-TX de la figura 3.21 se muestra conectada directamente a un puerto switch 100Base-TX.

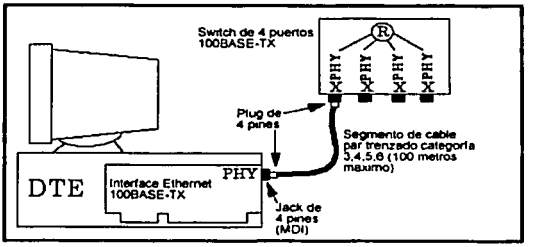


Fig. 3.21. Elementos de conexión 100BASE-TX

El medio físico 100Base-TX está basado en las especificaciones publicadas en el estándar de ANSI medio físico TP-PMD. El sistema 100Base-TX opera a través de dos pares de cables, un par para recibir las señales de datos y el otro par para transmitirlas. Partiendo de que la especificación ANSI TP-PMD permite indistintamente el uso de cable par trenzado con blindaje o sin blindar, el sistema 100Base-TX permite ambos también.

El cableado que se usa más popularmente en la actualidad es el par trenzado sin blindaje. Los dos alambres de cada par del cable tienen que estar trenzados conjuntamente en la toda la

longitud del segmento, y mantenerse trenzados hasta aproximadamente media pulgada de cada conector o punto de terminación del cable. Esta es una técnica estándar utilizada para mejorar las características de conducción de las señales del par de cables sin blindaje.

Componentes del sistema 100-Base-TX

El conjunto siguiente de componentes se utiliza para construir el segmento de par trenzado 100Base-TX y para realizar conexiones a él.

MEDIO DE RED

El medio 100Base-TX está diseñado para permitir segmentos por encima de los 100 metros de longitud usando cable par trenzado sin blindaje con una impedancia característica de 100 ohmios y se conoce como las especificaciones de cable de categoría 5 de EIA/TIA. Los segmentos de 100Base-TX están limitados a 100 metros de longitud para asegurar que las especificaciones del round trip timing sean correctas.

Por ejemplo, si se usa cable de par trenzado en un sistema 10Base-T, es posible alcanzar una longitud de segmento de 150 metros con éxito. Esto no es cierto en el sistema Fast Ethernet, donde la longitud del segmento viene delimitada por razones del tiempo de propagación de la señal. El estándar de cableado EIA/TIA recomienda una longitud máxima de segmento de 90 metros. Esto proporciona 10 metros de cable para conectar los trozos de cable al final de cada enlace, para pérdidas de señal en los cables de terminación intermedios, etc.

Hay probadores de cable de par trenzado Ethernet que permiten realizar una revisión del cable y asegurarse de que se cumplen las especificaciones eléctricas del estándar. Estas especificaciones incluyen el acoplamiento de la señal, que es la cantidad de señal que se inducen entre los pares de transmisión y recepción, y la atenuación de la señal, que es la cantidad de señal que se pierde en el segmento.

El sistema 100Base-TX utiliza dos pares de cables, lo cual significa que cuatro de los ocho pines del conector MDI (RJ-45) son los usados para transportar las señales Ethernet. En la tabla 3.22 se muestra la configuración que se debe emplear para la transmisión-recepción de señales para el plug RJ-45.

Conector de 8 pines 100BASE – TX	
Número del Pin	**Señal**
1	Transmisión +
2	Transmisión -
3	Recepción +
4	Sin usar
5	Sin usar
6	Recepción -
7	Sin usar
8	Sin usar

Tabla 3.22. Configuración de transmisión-recepción para plug RJ-45 para 100BASE-TX

Los segmentos Ethernet 100Base-TX están definidos como segmentos del enlace en las especificaciones Ethernet. Un segmento de enlace se define formalmente como un medio punto a

punto que conecta dos y solamente dos MDIs. La red más pequeña posible construida con un segmento de enlace debe consistir en dos computadoras, uno en cada extremo del segmento.

Las señales de transmisión y recepción de datos en cada par del segmento 100Base-TX están polarizadas, con una hebra de cada par de señales portando la señal positiva (+), y la otra portando la señal negativa (-).

El estándar 100Base-TX puede también amoldarse al cable de par trenzado con blindaje con una impedancia característica de 150 ohmios. Este tipo de cable se puede encontrar en algunos sistemas de cableado. Si se usa cable par trenzado con blindaje equipado con conectores de 9-pin tipo D, el conector se une según las especificaciones TP-PMD del ANSI:
Pin 1->Recepción(+)
Pin 5->Transmisión (+)
Pin 6->Recepción(-)
Pin 9->Transmisión(-)

CRUCE DE CONEXIONES 100BASE-TX

Cuando conectamos dos estaciones a un segmento, los pines de transmisión de datos de uno de los MDI tienen que ser conectados los pines de recepción de datos del otro MDI, y viceversa. Para un único segmento que conecte sólo dos computadoras, se puede hacer esto construyendo un cable cruzado especial, como se muestra en la figura 3.23. Los pines de transmisión son los TD y los de recepción los RD.

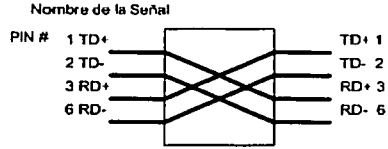


Fig. 3.23. Cruce de conexiones 100BASE-TX

Sin embargo, cuando está conectando múltiples segmentos en un sistema, es mucho más fácil realizar la conexión del cable directamente y no preocuparse de si los cables del sistema han sido correctamente cruzados. La forma de hacerlo es haciendo el cruce dentro del concentrador hub.

3.4.1.6. EL SISTEMA 100Base-FX (Fibra óptica)

En la figura 3.24 se muestra la interfaz 100Base-FX conectado directamente a un puerto switch 100Base-FX.

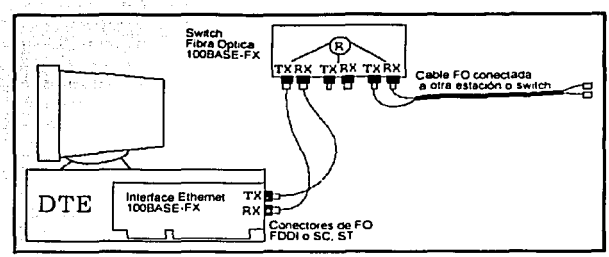


Fig. 3.24. Elementos 100BASE-FX

Componentes 100Base-FX

El siguiente conjunto de componentes es utilizado para construir los segmentos de fibra óptica 100Base-FX, y para hacer conexiones a él. Los concentradores 100Base-FX y el test de integridad de enlace son los que se emplean en 100Base-TX, teniendo el mismo funcionamiento expuesto anteriormente. Estos componentes son los siguientes:

MEDIO DE RED

El medio 100Base-FX está diseñado para permitir longitudes de segmento de hasta 412 metros. Aunque es posible enviar señales mediante la fibra óptica a través de longitudes mucho mayores, el límite de 412 metros en Fast Ethernet existe para asegurar que se cumplen las especificaciones del Round Trip Timing.

La especificación 100Base-FX necesita dos hebras de cable de fibra óptica multimodo (MMF) por enlace, una para transmisión de datos, y otra para la recepción, con el cruce de señal (TX a RX) configurado en el enlace.

Cuanto mayor número de conectores haya y cuanto mayor sea la longitud del cable de fibra óptica, mayor será la pérdida óptica que se produzca. La pérdida óptica se puede medir con instrumentos capaces señalar exactamente, qué pérdida óptica puede haber en un segmento determinado con una longitud de onda determinada.

CONECTORES MDI

La interfaz dependiente del medio (MDI) para un enlace 100Base-FX debe ser uno de tres tipos de conectores de fibra óptica. De los tres, el conector SC duplex es el recomendado alternativamente en el estándar. El conector SC está diseñado para un fácil manejo. Este conector es directamente insertado en su sitio para completar automáticamente la conexión.

Otro tipo de conector que puede ser usado es el FDDI Media Interface Connector (MIC). Este es un conector estándar codificado utilizado en los sistemas de red local FDDI.

El tercer tipo de conector para fibra óptica que puede ser utilizado es llamado comúnmente como conector ST. Este es el mismo conector que se usa en un enlace 10Base-FL. Este es un conector tipo bayoneta, más complicado que los dos anteriores.

Los segmentos de enlace tienen la misma configuración que en 100Base-TX. Una de las instalaciones mas usadas utilizan concentradores hub multipuerto o hubs de intercambio de

paquetes, para proporcionar una conexión entre un gran número de segmentos de enlace (al igual que 100Base-TX). Se tiene que conectar la interfaz Ethernet de la computadora a un extremo del segmento de enlace, y el otro extremo del segmento de enlace se conecta al hub. De esta forma se puede conectar tantos segmentos de enlace, y tantas computadoras como puertos tenga el hub.

3.4.1.7. EL SISTEMA 100Base-T4

La interfaz 100Base-T4 mostrado en la figura 3.25 está conectado directamente a un puerto hub 100Base-T4.

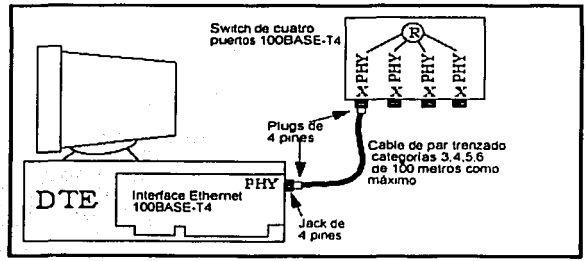


Fig. 3.25. Elementos de conexión 100BASE

El sistema 100Base-T4 opera mediante cuatro pares de cables, con un sistema de señalización que hace posible proporcionar las señales Fast Ethernet sobre cable estándar de par trenzado sin blindaje.

Componentes de 100Base-T4

El siguiente conjunto de componentes es utilizado para construir los segmentos de par trenzado. Los concentradores 100Base-T4 son los mismos empleados en 100Base-TX. Estos componentes, son los siguientes:

MEDIO DE RED

El medio 100Base-T4 está diseñado para permitir segmentos de hasta 100 metros de longitud usando cable par trenzado sin blindar.

Los segmentos 100Base-T4 están limitados a un máximo de 100 metros, para asegurar que las especificaciones del round trip timing se cumplan.

Las recomendaciones de cableado son las mismas que en los segmentos 100Base-TX expuestos en el apartado del sistema 100Base-TX, al igual que los instrumentos utilizados para probar el correcto funcionamiento de los segmentos.

El sistema 100Base-T4 utiliza cuatro pares de cables, que requieren que los ocho pins del conector MDI (estilo RJ45) sean utilizados, como se muestra en la tabla 3.26. En la figura 3.27 se muestra la configuración interna del plug RJ-45 para 100BASE-T4.

Conector de 8 pines 100BASE – T4	
Número del Pin	Señal
1	TX_D1+
2	TX_D1-
3	RX_D2+
4	BI_D3+
5	BI_D3-
6	RX_D2-
7	BI_D4+
8	BI_D4-

Tabla 3.26. Configuración de transmisión-recepción para plug RJ-45 para 100BASE-TX

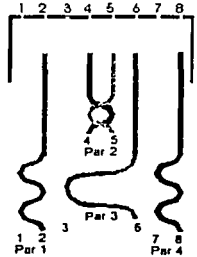


Fig. 3.27. Configuración interna del plug RJ-45 para 100BASE-T4

Como se muestra en la figura, de los cuatro pares, un par es para transmitir datos (TX), otro par es para la recepción (RX), y los otros dos pares de datos bidireccionales (BI). Cada par está polarizado, con un cable portando la señal positiva (+) y el otro la señal negativa (-).

Directivas de configuración de 100Base-T4

Los segmentos 100Base-T4 están definidos como segmentos de enlace en las especificaciones Ethernet. Un segmento de enlace se define formalmente como un medio punto a punto que conecta dos y solamente dos MDI. La red más pequeña posible construida con un segmento de enlace debe consistir en dos computadoras, uno en cada extremo del segmento.

Una de las instalaciones mas usadas utilizan concentradores hub multipuerto o hubs de intercambio de paquetes, para proporcionar una conexión entre un gran número de segmentos de enlace. Se tiene que conectar la interfaz Ethernet de la computadora a un extremo del segmento de enlace, y el otro extremo del segmento de enlace se conecta al hub. De esta forma se puede conectar tantos segmentos de enlace, y tantas computadoras como puertos tenga el hub, y las computadoras se comunican todos a través del hub.

3.4.1.8. AUTO-NEGOCIACIÓN

La función de Auto-Negociación es un parte opcional del estándar Ethernet que hace posible que los dispositivos intercambien información sobre sus capacidades sobre un segmento de

enlace. Esto permite a los dispositivos realizar una configuración automática para conseguir el mejor modo de operación posible sobre un enlace. Como mínimo, el mecanismo de Auto-Negociación puede proporcionar una configuración automática de la velocidad de transmisión para los dispositivos de velocidad múltiple de cada extremo del enlace. Las interfaces Ethernet de múltiple velocidad pueden aprovechar la máxima velocidad que puede ofrecer un puerto hub de múltiple velocidad.

El protocolo de Auto-Negociación incluye también otras capacidades. Por ejemplo, un hub que es capaz de soportar la transición en full-duplex en alguno o todos sus puertos, puede darse cuenta de este hecho mediante el protocolo de Auto-Negociación. Las interfaces conectados al hub que soporten también la transmisión full-duplex pueden configurarse a sí mismos para utilizar la transmisión full-duplex en su interacción con el hub.

FAST LINK PULSE

El mecanismo de Auto-Negociación utiliza las señales conocidas como Fast Link Pulse (FLP). Estas señales son una versión modificada de las señales Normal Link Pulse (NLP) que se utilizan para verificar la integridad de enlace, como fueron definidas en las especificaciones originales de 10Base-T. Las señales FLP son generadas automáticamente a nivel alto, o pueden ser seleccionadas manualmente mediante la interfaz de gestión de un dispositivo de Auto-Negociación, además no interfieren con el tráfico normal de la red, ya que aparecen durante tiempos de tráfico nulo.

Las señales FLP se usan para enviar información sobre las capacidades de los dispositivos. El protocolo de Auto-Negociación contiene reglas para la configuración de dispositivos basados en esta información. Así es como un hub y el dispositivo enlazado a él pueden negociar y configurarse automáticamente a sí mismos para tener la mayor velocidad de operación posible.

3.4.2. 100VG-AnyLAN

El protocolo de prioridad bajo demanda, comúnmente conocido como 100VG-AnyLAN, es un estándar de red de área local (LAN) que busca proporcionar una velocidad superior, un medio compartido en el que se puedan sustituir los lentos protocolos de red en el medio existente.

Una red de prioridad bajo demanda consiste en nodos finales, concentradores, switches, puentes, routers y enlaces de red.

Los componentes fundamentales de 100VG-AnyLAN son los nodos finales y los concentradores. Un nodo final es conectado a la red a través de una tarjeta interfaz que se conecta al bus del sistema. El dispositivo que interconecta los nodos finales y el resto de componentes en 100VG-AnyLAN es el concentrador. Otros componentes son los puentes, routers y switches.

Una configuración básica de 100VG-AnyLAN (figura 3.28) consiste en un número pequeño de nodos locales, o nodos finales (normalmente entre 6 y 32), que son conectados a un concentrador. Una red mayor puede ser construida mediante una cascada de concentradores como se muestra en la figura de abajo.

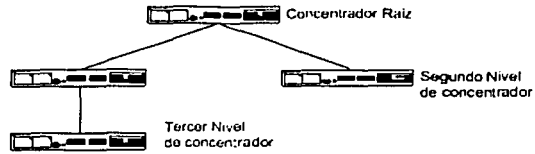


Fig. 3.28. Configuración básica 100VG-AnyLAN

Los nodos finales son típicamente PCs o computadoras más potentes, estaciones de trabajo, puentes, routers, switches, o servidores . Ellos son los actores de la red, transmitiendo y recibiendo datos vía el concentrador. Los nodos finales tienen dos modos de operación: privada y promiscua. Los nodos promiscuos reciben todas las tramas de la red, mientras que los nodos privados sólo reciben los mensajes enviados específicamente a ellos.

3.4.2.1. Topología

Este punto se centra en los contenidos de una red 100VG-AnyLAN desde el punto de vista de la topología. Los conceptos de hubs en cascada, distancias LAN y consideraciones de formato proporcionarán una estructura completa de la implementación de la red.

Una red 100VG-AnyLAN, como mínimo, consiste en un concentrador, dos nodos finales y enlaces de red. Cada uno de los nodos finales de la red están conectados a los concentradores. Esta es la configuración más usual para pequeños grupos de segmentos, pero las redes más grandes son típicamente conectadas en forma de cascada. Sólo un máximo de 5 niveles de cascada está permitido por el protocolo por razones del tiempo de la señal.

En la figura 3.29 se muestra una red 100VG-AnyLAN con routers. Es importante darse cuenta de que los routers y puentes se comportan como nodos finales en los que se conectan a puertos locales en lugar de a puertos de enlace superior en el concentrador. En términos de acceso a la red, ellos tienen el mismo 'estatus' en el proceso de registro de Prioridad Bajo Demanda que una estación de trabajo ordinaria.

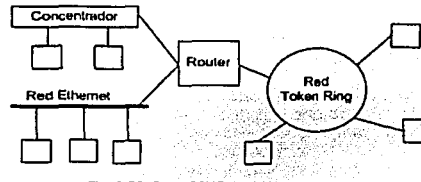


Fig. 3.29. Red 100VG-AnyLAN con routers

Control de acceso al medio (MAC)

El subnivel de control de acceso al medio (MAC) actúa como inspector de la transferencia de datos para un nodo específico. El MAC gestiona las peticiones de transmisión a la red, recibiendo

datos de las capas superiores y manipulando los datos antes de la transmisión. La manipulación de datos incluye la construcción de las tramas que encapsulan los datos. Cuando el MAC ha finalizado de manipular los datos para la transmisión, el control se pasa a la subnivel PMI (Physical Medium Independent).

Si el nodo está recibiendo datos, entonces la responsabilidad del subnivel MAC incluye extraer los datos de las tramas y revisar en busca de errores de transmisión en las tramas recibidas. Cuando el subnivel MAC ha terminado de revisar las tramas, el control es pasado, junto con los datos, a niveles superiores en el protocolo.

TRANSMISIÓN DE PAQUETES DE DATOS

La transmisión de paquetes de datos consiste en una serie de secuencias de 'estrechar la mano' donde la parte que envía realiza una petición y la otra parte confirma la petición. La secuencia de envío de un paquete de datos es pedida por un nodo final y controlada por el concentrador. Para la transmisión de un paquete de datos ocurre lo siguiente:

1. Si un nodo final tiene un paquete de datos preparado para enviar, transmite una señal de control que puede ser o bien una 'Request_Normal' o 'Request_high'. En otro caso, el nodo final transmite la señal de control 'Idle_Up'.
2. El concentrador registra todos los puertos locales para determinar qué nodos finales están pidiendo enviar un paquete de datos y a qué nivel de prioridad han sido pedidas (normal o alto).
3. El concentrador selecciona el siguiente nodo final con mayor prioridad pendiente. Los puertos se seleccionan en orden de puerto. Si no hay peticiones con prioridad alta pendientes, entonces el siguiente puerto de prioridad normal es seleccionado (en orden de puerto). Esta selección provoca que el puerto seleccionado reciba la señal 'Grant' o de concesión. La transmisión del paquete empieza cuando el nodo final detecta la señal de concesión.
4. El concentrador entonces envía la señal de Entrada al resto de nodos finales, alertándolos de la posibilidad de un paquete de entrada. El concentrador decodifica la dirección de destino de la trama siendo ésta transmitida de la misma forma que la ha recibido.
5. Cuando un nodo final recibe la señal de control de Entrada, se prepara para recibir un paquete parando la transmisión de peticiones y escuchando el medio para recibir el paquete.
6. Una vez que el concentrador ha descifrado la dirección de destino, el paquete es entregado a la dirección del nodo final o de los nodos finales y a cada nodo promiscuo. Aquellos nodos que no reciben el paquete de datos reciben la señal 'Idle_Down' procedente desde el concentrador.
7. Cuando el nodo final (o nodos finales) reciben el paquete de datos, vuelven al estado anterior a la recepción del paquete, bien enviando una señal 'Idle_Up' o realizando un petición para enviar un paquete de datos. Este proceso es utilizado en todas partes por el protocolo de prioridad bajo demanda para permitir a los nodos finales la transmisión de paquetes de datos a otros nodos.

100VG-AnyLAN está diseñada para operar de forma compatible con los formatos de trama Ethernet y Token Ring. Esto significa que el software y los protocolos sobre el nivel de enlace (LLC) sólo necesitan saber que están operando en una red Ethernet o Token Ring, teniendo en cuenta sus formatos de trama. El nivel LLC proporciona al nivel MAC las primitivas que contienen la información empleada para la construcción de la trama Ethernet o Token Ring. El subnivel MAC construye entonces una trama con los elementos que convengan. De esta manera, 100VG-AnyLAN trabajará bien en modo Ethernet o Token Ring.

Futuras Ampliaciones

En Julio de 1995, el grupo de trabajo 802.12 del IEEE propuso cuatro peticiones de autorización de proyecto (PAR) al comité ejecutivo 802 para cambios y mejoras del actual estándar IEEE 802.12. Estos cuatro proyectos son los relacionados a VGAny-LAN de alta velocidad.

VGAny-LAN DE ALTA VELOCIDAD

El suplemento VGAny-Lan de alta velocidad tiene como ambición proporcionar un mayor velocidad de apoyo a la redes 100Mbps o más lentas. La velocidades que se investigan actualmente son de 400Mbps, 1Gbps y 4Gbps. Los requerimientos de la capa física tienen que ser definidos para funcionar a velocidades mayores de 100 Mbps. El suplemento definido será compatible con el estándar 802.12 existente.

Este suplemento definirá una capacidad opcional conocida como "modo estallido" (burst mode). Con este modo de operación estas redes tendrán la posibilidad de enviar más de una trama en el mismo instante de tiempo.

Funcionamiento Full-Duplex

Este suplemento intente mejorar la capa MAC para proporcionar el modo de operación full-duplex en la conexión entre dos nodos. La capacidad de conectar dispositivos punto a punto en la configuración 802.3, aunque no de forma estándar, es posible y muy frecuente. Esta posibilidad es la que se quiere estandarizar en las redes 802.12.

3.4.3. FDDI

A mediados de los años 80, ANSI propuso el estándar X3T9.5 que llego a ser conocido como FDDI (Fiber Distributed Data Interface) con una velocidad de transmisión de 100 Mbps con fibra óptica como medio físico de transmisión. FDDI describe las capas física y de enlace de datos del modelo de referencia OSI, con conectores y características propias de la fibra óptica. Principalmente se aplica como red primaria o backbone de redes locales. A principios de los 90 se propuso otra parte de este estándar llamado CDDI (Copper Distributed Data Interface). FDDI y CDDI son topologías que utilizan un Token como acceso al medio, aunque las conexiones en estrella a través de concentradores son posibles.

FDDI se parece mucho en cuanto a sus protocolos a los de la red IEEE 802.5, especialmente en todo lo que se refiere al paso del token. Sin embargo, hay una diferencia significativa. En una red de longitud tan grande (100 Km.) sería una perdida de eficacia esperar a que el token recorra todo el anillo. Para resolver este problema se generan varios tokens, lo que produce que en el anillo, FDDI puedan convivir varias tramas simultáneamente.

Se emplean dos anillos (figura 3.30) que tienen la función de continuar con la comunicación cuando una estación no esta funcionando correctamente cerrando el anillo con los dos anteriores. El flujo de tráfico es en direcciones opuestas (llamado giro contrario). La red está constituida por una colección de interfaces de anillo conectadas por medio de líneas punto a punto. Por el anillo va circulando la trama especial (token), que da derecho a transmitir a aquella estación que lo haya capturado. Una vez capturado el token, la estación dispone de una cierta cantidad de tiempo para transmitir sus tramas, que se encargará de retirar de la red la propia estación emisora, tras lo cual habrá de liberar el token. Las tramas van circulando por la red pasando secuencialmente por las estaciones activas.

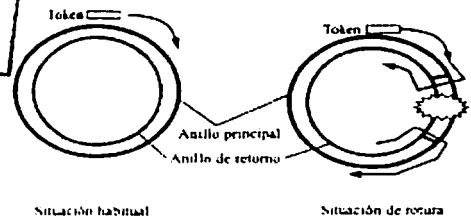


Fig.3.30. Funcionamiento básico de FDDI

Todas las conexiones en la red están hechas a través de MIC (Media Interface Connector), conectores de fibra multimodo y a través de conectores ST para fibra monomodo. La ventaja más importante que presenta la fibra óptica es la inmunidad a interferencia eléctrica causada por RFI (Interferencia de Frecuencias de Radio) y EMI (Interferencia Electromagnética). Los conectores RJ – 45 son empleados para CDDI.

3.4.3.1. Diferencias con el estándar IEEE 802.5

Se han hecho algunas adaptaciones y optimizaciones para adaptarse al máximo la capacidad de alta velocidad y largas distancias. Una de las diferencias es que en FDDI se permite que una estación libere el token tan pronto como haya terminado de transmitir. Otra de las diferencias es la manera de reservar el ancho de banda para las transmisiones síncronas y asíncrona, es decir, cuando transmitir los datos asíncronos (pues los asíncronos tienen su ancho de banda asegurado). Cuando se captura el token, este es retenido un cierto tiempo durante el cual se pueden transmitir varias tramas, aunque en la mayoría de las implementaciones del 802.5 solo se permite transmitir una trama. Una última diferencia es la forma es que las estaciones acceden al token.

En el 802.5, todos los datos se reciben bit a bit. Se puede identificar el bit de token en el campo correspondiente de la trama de token, pudiendo la estación cambiar este bit y redefiniendo la transmisión como una trama. En FDDI, cuando una estación espera el token, lo captura por completo interrumpiendo la transmisión de éste al reconocerlo.

3.4.3.2. Tolerancia a fallos

La red FDDI tiene varios mecanismos para mantener la continuidad del anillo, y por tanto, ningún tipo de ruptura en el funcionamiento de la red. A continuación se describen los más importantes.

WRAP

Como los anillos transmiten en sentidos opuestos, es decir, sin uno transmite en el sentido de las manecillas del reloj, el otro lo hace en sentido contrario. Normalmente solo se utiliza uno de los anillos, que llamaremos primario. Si el anillo primario fallara, se utilizaría el secundario en su lugar. En caso de que se desactivaran ambos anillos en el mismo punto, por rotura u otros motivos,

entonces habría que aislar el segmento del anillo en el que se ha producido el fallo, de manera que las dos estaciones duales que se encuentran en cada uno de los extremos del segmento que ha fallado se encarguen de restablecer el anillo. Lo hacen enlazando, en su punto de conexión, el anillo primario con el secundario (WRAP, figura 3.31), de forma que se vuelve a tener un anillo cerrado y funcionando correctamente. Algunas estaciones primarias podrían quedar aisladas.

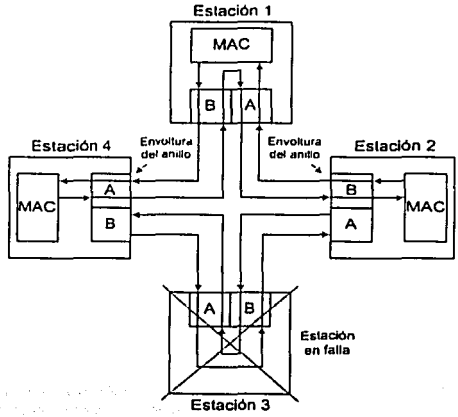


Fig.3.31. Mecanismo Wrap

Cuando una falla ocurre en un enlace (por rotura de algunas de las fibras), las estaciones vecinas realizan también un "wrap" de los anillos primario y secundario que se mantenga la comunicación en todas las estaciones. Esto se representa en la figura 3.32.

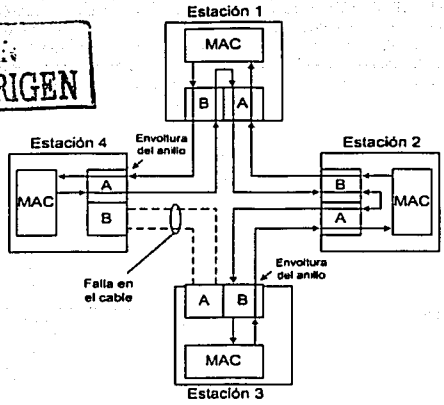


Fig.3.32. Mecanismo Wrap

Bypass

Un bypass o interruptor óptico de desvío proporciona una operación continua en el anillo doble si falla un dispositivo de la red. Esto se utiliza tanto para evitar la segmentación del anillo como para eliminar de la red a las estaciones en estado de falla. El interruptor óptico de desvío realiza esta función utilizando espejos ópticos que pasan la luz directamente desde el anillo hasta el dispositivo DAS durante la operación normal de la red. En el caso de una falla en el dispositivo DAS, por ejemplo que se apague, el interruptor óptico de desvío pasará la luz a través de sí mismo utilizando espejos en su interior y, por lo tanto, mantendrá la integridad en el anillo. La ventaja de esta característica es que el anillo no entrará en una condición de envoltura en el caso de que se presente una falla en un dispositivo. La figura 3.33 muestra cómo funciona un interruptor óptico de desvío en una red FDDI.

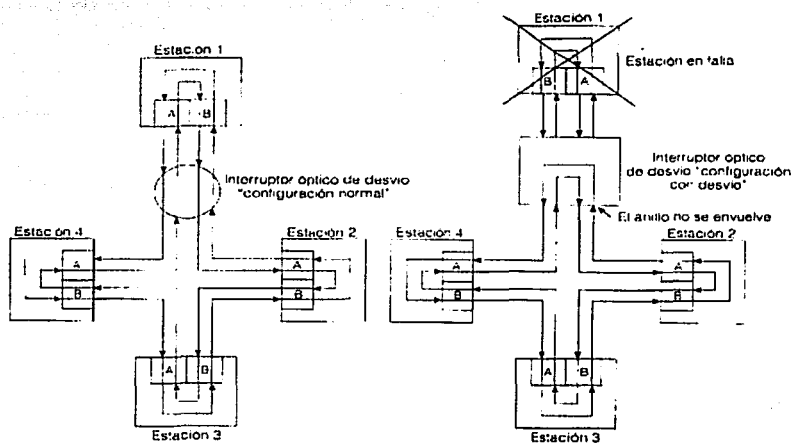


Fig.3.33. Bypass

3.4.3.3. Arquitectura de red

La arquitectura FDDI cubre el nivel físico y la subcapa MAC de la capa de enlace de datos. Se utiliza el estándar 802.2 de la subcapa LLC para redes de área local, lo cual hace de FDDI una interfaz común para interconectar redes locales de todo tipo (802.2, 802.5, etc.).

En realidad, FDDI no es una sola especificación, sino que es un grupo formado por cuatro especificaciones diferentes, cada una de las cuales cubre una determinada función. La combinación de estas especificaciones permite ofrecer conectividad a alta velocidad entre los protocolos de las capas superiores como TCP/IP e IPX, y los medios de transmisión como la fibra óptica.

La capa física se divide en dos subcapas, PMD (Physical Medium Dependant) y PHY (Physical Layer Protocol), y la capa de enlace de datos en las subcapas MAC (Media Access Control) y LLC (Logical Link Control), adoptando esta ultima el estándar 802.2 como se había comentado.

Subcapa PMD, Physical Medium Dependent Interface

Se dedica a la conversión de electrones en luz.

Dentro del modelo OSI, la capa física ocupa el menor nivel, ésta se encarga de definir la transmisión de bits en el medio físico.

La norma PMD especifica:

- Características y tipos de transmisores, receptores, cables, conectores, etc. Se considera su funcionalidad y economía.

- Establece como nodos físicos a los conectados al anillo FDDI y como estaciones a las interconectadas físicamente a la red por un medio de cobre o fibra óptica.
- Define varias opciones:
  - Fibra Multimodo (MMF-PMD)
  - Fibra Monomodo (SMF-PMD)
  - Fibra de Bajo Costo (LCF-PMD)
  - Par Trenzado Blindado (STP-PMD)
  - Par Trenzado Sin Blindar (UTP-PMD)
  - FDDI Sobre SONET (Synchronous Optical Network)

El modelo ANSI define los medios para conectar físicamente un cable a una estación FDDI, como:

- Conectores ST
- Conectores SC.

Los conectores ST se usan habitualmente para conectar fibra óptica a una estación FDDI. El protocolo de la capa física define lo siguiente:

- Recuperación de reloj y datos: recupera la señal de reloj desde los datos ingresados.
- Proceso de codificación/decodificación: convierte los datos desde la MAC al interior de una transmisión sobre el anillo FDDI.

FDDI define dos tipos de dispositivos para redes locales: estaciones y concentradores. Además existen dos tipos de estaciones:

- Dual Attached Station (DAS)
- Single Attached Station (SAS)

Las estaciones son dispositivos que tienen el papel más importante como computadoras, impresoras, etc. Las estaciones pueden ser Dual o Single Attached Station.

Los concentradores son dispositivos que hacen posible la conexión de una estación SAS a la red. Cuando una SAS esta apagada, el concentrador asegura la continuidad del anillo cerrando el puerto de dicha estación. Tienen la función parecida a un Hub con una topología en estrella. Cuando los concentradores están conectados al anillo lo pueden hacer de dos formas, Dual si están conectados a los dos anillos o single si esta conectado a un anillo. Por tanto, existen dos tipos de concentradores Dual Attached Concentrator y Single Attached Concentrator.

Un DAC tiene tres tipos de puertos: A, B y M. El puerto A conecta la entrada del anillo primario y la salida del anillo secundario y el puerto B conecta la salida del anillo primario y la entrada del anillo secundario. El puerto M conecta a al puerto S (Slave) de una estación SAS.

Una SAC tiene dos puertos: S y M. El puerto M se conecta a las estaciones SAS y el puerto S se conecta al DAC o a otro puerto M de un SAC.

Las estaciones DAS conectadas a al anillo siempre son Dual Attach y necesitan estar activas y corriendo todo el tiempo. Las estaciones DAS tienen dos puertos, A y B, como se indica en la figura 3.34. El puerto A conecta la entrada del anillo primario y la salida del anillo secundario y el puerto B conecta la salida del anillo primario y la entrada del anillo secundario.

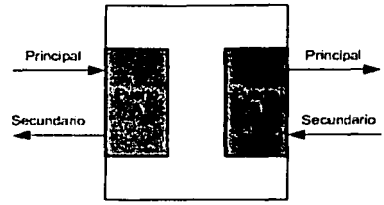


Fig.3.34. Puertos de una estación DAS

Las estaciones SAS no deben estar conectadas a ambos anillos. Solo tienen un puerto y siempre deberían estar conectadas a través de un switch. Una estación SAS tiene un puerto S (Slave) que se conecta al puerto M (Master) del concentrador. Actualmente se crea dos enlaces SAS. Pero en lugar de instalar dos tarjetas SAS se emplea una DAS. En la figura 3.35 se muestra como se conectan los diferentes dispositivos dentro de la red FDDI.

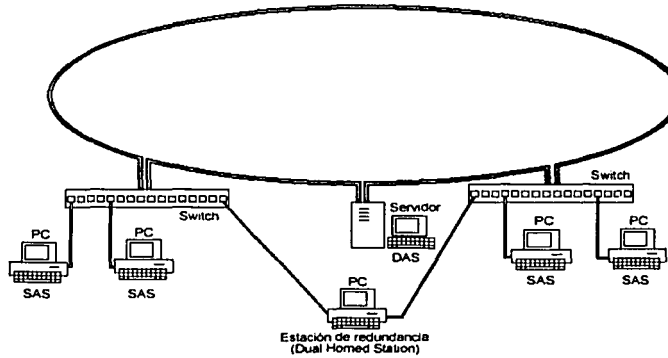


Fig.3.35. Dispositivos de una red FDDI

El número máximo de estaciones es de 500 con una longitud del anillo de 100 kilómetros teniendo en cuenta el doble anillo, se pueden alcanzar los 200 Km.

3.4.3.4. Funciones del PMD

Dentro de las funciones del PMD, se tiene que para ser transmitidos los datos entre estaciones, éstos son reunidos primeramente en bits de datos en una serie de señales y luego se transmiten estas señales sobre el cable de unión entre las dos estaciones. La norma PMD trata con todas las áreas que son asociadas con transmisión física de los datos, como son:

- Transmisores y receptores ópticos y eléctricos.
- Fibra óptica o cable de cobre.
- Interfaz de conexión al medio (MIC), Conectores.
- Retardo por desvío óptico.

Capa PHY, Physical Layer Protocol

Subnivel físico superior que define aspectos independientes del medio físico.
El protocolo de la capa física define lo siguiente:

- Recuperación de reloj y datos: recupera la señal de reloj desde los datos ingresados.
- Proceso de codificación/decodificación: convierte los datos desde la MAC al interior de una transmisión sobre el anillo FDDI.
- Símbolos: son las más pequeñas señales existentes usadas para comunicación entre estaciones. Los símbolos están comprimidos en códigos de cinco bits.
- Elasticidad tope: estimación de las tolerancias para reloj entre estaciones.
- Función de alisamiento: corrige tramas que han perdido el encabezamiento.
- Filtro repetidor: corrige la violación del código e invalida estados de la línea.
- Recuperación de reloj y datos.

3.4.3.5. Definición de tramas MAC

La máxima longitud de la trama FDDI es limitada 4500 bytes para evitar problemas de desincronización. La longitud máxima de 4500 bytes es determinada por la codificación empleada, denominada 4B/5B (4 bytes/5 bytes), con una frecuencia de reloj de 125 MHz, siendo por tanto la eficacia del 80%. El formato es como se indica en la figura 3.36.

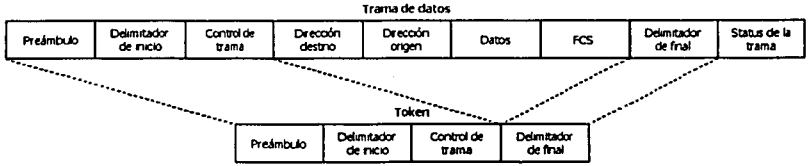


Fig.3.36. Trama FDDI

PA = Preámbulo cuatro o más símbolos de Idle (para sincronismo).
SD = Delimitador de inicio. Indica el comienzo de una trama a través de un patrón de señalización que lo diferencia del resto de la trama (utiliza los símbolos "J" y "K").
FC = Control de trama. Indica el tamaño de los campos de dirección y el tipo de trama (síncrona o asíncrona).
DA = Dirección destino. Contiene una dirección unidifusión (singular), una dirección multidifusión (grupo) o una dirección de difusión (a todas las estaciones) utiliza hasta seis bytes.
SA = Dirección origen. Identifica a la estación que envió la trama. Tal como sucede con las direcciones Ethernet y Token Ring, las direcciones de origen y destino de FDDI tienen una longitud de 6 bytes.
INF= Datos. Contiene información destinada a un protocolo de las capas superiores o información de control (N bytes).
FCS= Secuencia de verificación de trama, redundancia de la trama (con CRC-32). Este campo es llenado por la estación origen con un valor de la verificación de redundancia cíclica que se calcula

en función del contenido de la trama igual que en Ethernet o Token Ring, la dirección destino recalcula el valor para determinar si la trama se dañó por la red. Si fue así, se elimina la trama.
ED = Delimitador de fin de trama.
FS = Estado de la trama. Permite que la estación origen determine si se ha presentado un error y si la trama fue confirmada y copiada por una estación receptora.

3.4.3.6. Otras posibles soluciones

CDDI

CDDI (Copper Distributed Data Interface) no es otra cosa que FDDI utilizando cables de cobre en lugar de fibra óptica como medio de transmisión. Sólo afecta al PMD. Para seguir cumpliendo los requerimientos de ruido y velocidad de transmisión se reduce la distancia máxima de enlace a 100 m.

La principal ventaja que aporta CDDI es la reducción en los costos de implantación de FDDI, sobre todo cuando se quiere hacer llegar FDDI hasta los terminales de usuario (FDDI- on-desk). Los terminales suelen estar ya cableados, por lo que sustituir el cobre por la fibra óptica aparece como un costo innecesario en muchos casos. Además, los receptores y transmisores ópticos que emplea FDDI resultan demasiado caros frente a los dispositivos electrónicos que utiliza CDDI. Por lo demás, los cambios en el código no son relevantes y la reducción en la distancia máxima no es importante, puesto que CDDI se utilizaría dentro de los edificios, en los que las distancias suelen ser inferiores a esos 100 metros críticos.

LCF-PMD

LCF-PMD (Low-Cost Fiber Physical Medium Dependent) surge también como ante necesidad económica. Se busca reducir el costo de implantación de una red FDDI. Para ello, se cambia de nuevo el PMD. Se introduce nuevos tipos de fibra, más baratos y de peores prestaciones. Igual que en CDDI, se amplían los márgenes de ruido, y se reducen las longitudes de los enlaces, ahora hasta los 500 metros. El resto del protocolo no se altera.

CAPÍTULO 4
TECNOLOGÍAS WAN

4.1. Frame Relay

4.1.1. Introducción

La propuesta inicial para la estandarización de Frame Relay se presenta en 1984 en el International Telecommunication Standardization Sector (ITU-T), antiguamente llamado Comité Consultivo Internacional de Telefonía y Telegrafía (CCITT). En esta epoca el American National Standards Intitute (ANSI) también comenzó sus trabajos sobre Frame Relay. En Estados Unidos, Frame Relay es un estandar del ANSI.

Se basa en el principio de conmutación de paquetes, lo que lo hace bueno para transferencias de datos. Dichos datos se dividen en tramas de longitud variable conteniendo cada una de ellas información acerca del direccionamiento a seguir. La principal diferencia con la conmutación de paquetes es que esta trabaja a nivel 3 del modelo OSI, mientras que Frame Relay trabaja a **nivel 2**, pero sin incluir todas las funciones típicas de esta capa.

Así pues, encontramos grandes diferencias entre la conmutación de paquetes que se utiliza en redes como X.25 y la que se realiza en Frame Relay. X.25 fue diseñada para poner especial atención en la recuperación de los errores que se pueden llegar a producir durante la transmisión de paquetes, asegurando que cuando ciertos datos se envían desde un emisor estos llegarán al receptor de modo correcto y en el orden correspondiente. Todo esto implica una serie de verificaciones y correcciones en los nodos intermedios para asegurar las propiedades de la transferencia, y por tanto un descenso de la velocidad de transferencia condicionado al procesamiento de cada nodo intermedio.

Sin embargo Frame Relay se basa en el hecho de que cada día las conexiones en redes WAN son más fiables, dado que la mayoría de los dispositivos son digitales y el medio de transmisión utilizado principalmente es la fibra óptica, que posee un porcentaje de error mucho menor que el porcentaje de error medio que se producía en la época de la implantación de X.25.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

Sus dos principios fundamentales para conseguir este aumento de velocidad son:

- Si se produce cualquier error con una trama, esta será descartada y no se intentará llevar a cabo ningún procedimiento de recuperación.
- Los sistemas finales son los responsables de recuperarse de situaciones de error.

Como se ha comentado, Frame Relay ni siquiera implementa todas las funciones propias del nivel 2, sino que solamente un subconjunto de ellas como son:

- Revisar la posibilidad de error. Si se ha producido alguno, entonces se descarta la trama.
- Leer la información de direccionamiento de la trama y colocar la trama de entrada en su salida correspondiente.
- Revisar si el nodo Frame Relay está congestionado, en cuyo caso modificará los bits de notificación de la congestión o descartará tramas.

Aunque las redes Frame Relay tienen ya cinco años de operación exitosa en varias partes del mundo, en México apenas empiezan a ofrecerse a gran escala. El surgimiento en México de servicios eficientes de transporte de datos se ve impulsado por el fin del monopolio de telefonía de larga distancia en 1996 y la competencia consecuente por un mercado muy grande de transmisión de información.

En la tabla 4.1 se proporciona una lista de las funciones suministradas por cada uno de los niveles OSI para X.25 y Frame Relay. Gran parte de las funciones de X.25 se eliminan en Frame Relay. La función de direccionamiento se desplaza desde la capa 3 en X .25 a la capa 2 en Frame Relay. Todas las demás funciones del nivel 3 de X.25 no están incorporadas en el protocolo de Frame Relay.

X.25		Frame Relay
Establecimiento de circuito Control de circuito Control de flujo de circuito Direccionamiento	Red	
Control de enlace Creación de tramas Control de errores Control de flujo de enlaces Fiabilidad	Enlace	Direccionamiento Creación de tramas Control de errores Gestión de interfaces
Conexión Física	Físico	Conexión Física

Tabla 4.1. Funciones X.25 y Frame Relay sobre modelo OSI

4.1.2. Tecnología

Las redes Frame Relay se construyen a partir de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión (DLCI), a través de la ruta establecida para la conexión en la red.

Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales: DTE (Data Terminal Equipment) y DCE (Data Communication Equipment). Los DTEs se consideran como equipo terminal para una red específica, y por lo general, se encuentran en las instalaciones de un cliente, por ejemplo: terminales, PCs, ruteadores y bridges. Los DTEs son dispositivos de interconectividad de redes, propiedad de la compañía telefónica. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en un red, que son en realidad los dispositivos que transmiten datos a través de la WAN. Un ejemplo, de DTE es un DSU/CSU (Data Service Unit/Channel Service UNIT) o un FRAD (Frame Relay Access Device).

Para poder utilizar una red Frame Relay, el cliente del servicio debe conectar su ambiente de cómputo interno a un ruteador, si se trata de una red local, que contenga una tarjeta que maneje Frame Relay, o a un FRAD. Estos elementos deben conectarse a su vez a la línea de acceso a la red a través de un DSU o un DSU/CSU que pueden ser dispositivos externos o estar integrados en los ruteadores y FRADs, por una conexión V.35 o por una conexión estilo RS-232 de alta velocidad. Dependiendo del modelo específico, el router proporciona uno o más puertos los cuales pueden ser directamente conectados virtualmente a cualquier tipo de LAN.

Entre las estaciones de los usuarios y los nodos de la red (UNI, User-to-Network Interface) se transmiten únicamente tramas a nivel de la capa de enlace de datos. Frame Relay ofrece un servicio orientado a conexión basado en el establecimiento de circuitos virtuales bidireccionales creados por los DTEs a través de una red PSN (Packet Switched Network) de Frame Relay, y el intercambio de tramas del tipo HDLC (High-level Data Link Control).

Cada circuito virtual se identifica de manera única por medio del DLCI (Data Link Connection Identifier). Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Esto implica que si deseamos establecer una comunicación con mas de un destino deberemos pagar por tantos circuitos virtuales como destinos haya. De este modo cada circuito virtual se someterá a una especie de proceso de mapeo para averiguar cual es la ruta que debe seguir un paquete para llegar a su destino correspondiente. Los circuitos virtuales pueden ser SVC (Switched Virtual Circuits) o PVC (Permanent Virtual Circuit)

4.1.2.1. Circuitos virtuales conmutados (SVC)

Los SVCs son conexiones temporales *que* se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

- *Establecimiento de la llamada.* Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
- *Transferencia de datos.* Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- *Ocioso.* La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.
- *Terminación de la llamada.* Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual, los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Se espera que los SVC se establezcan, conserven y finalicen utilizando los mismos protocolos de señalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipo DCE Frame Relay soportan SVCs; por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

4.1.2.2. Circuitos virtuales permanentes (PVC)

Los PVCs son conexiones establecidas en forma permanente, que se utilizan en transferencias de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de establecimiento de llamada y finalización que se utilizan con los SVCs.

Los PVCs siempre operan en alguno de los estados siguientes:

- *Transferencia de datos.* Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- *Ocioso.* Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVCs, los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en un estado ocioso.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

Normalmente los valores de DLCI (tabla 4.2) son asignados por el proveedor del servicio Frame Relay. Los DLCIs tienen un significado local, lo que significa que los valores en sí mismos no son únicos en la WAN Frame Relay; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión.

Valores de DLCI

Rango	Uso
0	Reservados para Señalización de llamadas de control
1 – 15	Reservados
16 – 1007	Asignables para PVCs
1008 – 1022	Reservados*
1023	Local Management Interface

* Uso de Extensión opcional de 1019 – 1022 para grupos multicast

Tabla 4.2. Valores DLCI

Por ejemplo, si el usuario A desea una comunicación con el usuario B, primero establecerá un circuito virtual que los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI.

Una vez que las tramas son entregadas a la red, son conmutadas según unas tablas de ruteo encargadas de asociar cada cada DLCI de entrada a un puerto de salida y un nuevo DLCI. En el destino las tramas son reensambladas, como se indica en a figura 4.3.

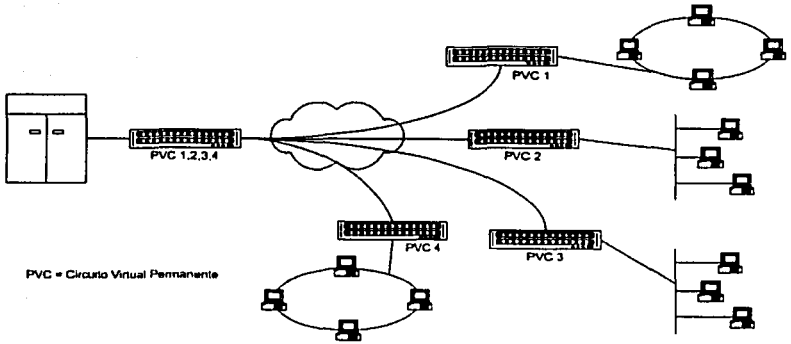


Fig. 4.3. Red Frame Relay

Al establecer un circuito virtual el usuario negocia con la red tres parámetros: CIR, Bc y Be, que definen las características de rafagueo (*burstiness)* de su tráfico. El CIR (Commited Information Rate) es la velocidad media de transferencia de información a la que el usuario desea transmitir. El CIR se mide sobre un intervalo de tiempo T que es proporcional al tamaño de las ráfagas. Bc (commited burst size) que son transmitidas por la fuente de información: T=Bc/CIR. El Bc es el número máximo de bits que la red se compromete a transportar sobre cualquier intervalo de tiempo T (normalmente inferior a 8 segundos). Por ejemplo, si la velocidad de acceso (AR) es de 64 Kbps, la duración (s) de las ráfagas es de 1.5 segundos y el tiempo (T) entre ráfagas es de 6 segundos, entonces el Bc es de 96 Kb: y el CIR es de 16 Kbps.

4.1.3. Formato de trama

El tamaño máximo del campo de información depende de los diferentes proveedores de servicio: el Foro Frame Relay recomienda que sea de por lo menos 1600 bytes y en la práctica la mayoría de los proveedores soportan tramas de hasta 4096 bytes, que es el máximo permitido para una operación confiable (sobre errores dobles en la trama) del campo FCS (Frame Check Sequence) de dos bytes.

Con 10 bits reservados para el DLCI (Data Link Connection Identifier) podrían multiplexarse hasta 1024 circuitos virtuales por puerto físico. Sin embargo, algunos identificadores están reservados y sólo se tienen disponibles 976 (del 16 al 991) para el usuario. En la figura 4.4 se muestra el formato de trama de Frame Relay.

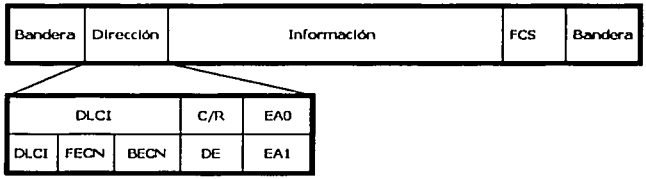


Fig. 4.4. Trama de Frame Relay

A continuación se describirá cada una de los campos de la trama.

- *Banderas.* Delimitan el comienzo y la terminación de la trama. El valor de este campo es siempre el mismo y se representa como el número binario 01111110. También se emplea para separar tramas consecutivas.
- *Direcciones.* Contiene la información siguiente:
  - DLCI: El DLCI de 10 bits es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Cada conexión virtual que se multiplexe en el canal físico será representada por un DLCI único. Los valores de DLCI tienen significado local solamente, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual.
  - EA (Dirección Extendida): La EA se utiliza para indicar si el byte cuyo valor EA es 1, es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte sea el último octeto DLCI. Aunque todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCIs más largos. El octavo bit de cada byte del campo Direcciones se utiliza para indicar el EA.
  - C/R: El C/R es el bit que sigue después del byte DLCI más significativo en el campo Direcciones. Se introduce por compatibilidad con protocolos anteriores, como los del tipo DIC. El bit C/R no está definido hasta el momento y no se emplea en Frame Relay.
  - *Control de la saturación:* Este campo consta de 3 bits que controlan los mecanismos de notificación de la saturación en Frame Relay. Éstos son los bits FECN, BECN y DE, que son los últimos 3 bits en el campo Direcciones.
    FECN (Notificación de la Saturación Explícita Hacia Adelante) es un campo de un solo bit que puede fijarse en un valor de 1 por medio de un interruptor para indicar a un dispositivo DTE terminal, como un ruteador, que ha habido saturación en la dirección

de la transmisión de la trama del origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de reaccionar de manera inteligente ante estos indicadores de saturación. Hoy en día, los protocolos DECnet y OSI son los únicos protocolos de las capas superiores que implementan estas características.

BECN (Notificación de Saturación Explícita Hacia Atrás) es un campo de un solo bit que, al ser establecido en 1 el valor por un switch, indica que ha habido saturación en la red en la dirección opuesta a la de la transmisión de la trama desde el origen al destino. Al igual que el campo anterior se emplean para el control del flujo.

El bit DE (Elegibilidad para Descarte) es fijado por el dispositivo DTE, un ruteador por ejemplo, para indicar que la trama marcada es de menor importancia en relación con otras tramas que se estén transmitiendo. En una red saturada las tramas que se marcan como "elegible para descarte" deben ser descartadas antes que cualquier otra. Lo anterior representa un mecanismo justo de establecimiento de prioridad en las redes Frame Relay.

- *Datos.* Los datos contienen información encapsulada de las capas superiores. Cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil que variará en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar el PDU (Paquete de Protocolos de las Capas Superiores) a través de una red Frame Relay.
- *Secuencia de verificación de tramas.* Asegura la integridad de los datos transmitidos. Este valor es calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión. Se trata de dos octetos que contienen el CRC de la trama obtenida a través del polinomio $X^{16}+X^{12}+X^5+1$ de CCITT. Opera con todos los bits excepto con los flags.

Comprobación de errores

Una trama es errónea si contiene las siguientes características:

- No delimitada por dos Flags.
- Menos de dos octetos entre las dos Flags.
- Error en el CRC.
- DLCI erróneo.
- Excede el tamaño máximo permitido.

4.1.4. Redes Frame Relay en la actualidad

La demanda por servicios públicos de Frame Relay es muy grande en todo el mundo, siendo actualmente la tecnología más usada en las redes de área amplia. En México se ofrecen servicios públicos Frame Relay desde 1995 (proporcionados por InterVan de Intersys) y se espera que el mercado despegue con la introducción en 1996 de UniNet de TELMEX y del servicio Frame Relay de Avantel.

Todos los proveedores de servicios Frame Relay ofrecen puertos de acceso de 64 Kbps y E1, algunos ofrecen puertos de velocidades menores de 64 Kbps, E1 fraccional y múltiplos de E1, y algunos proveedores planean ofrecer enlaces E3 que proporcionan una velocidad de acceso de 34 Mbps (En los Estados Unidos se utilizan velocidades de 56 y 64 Kbps, 1.5 Mbps (T1) y 45 Mbps (T3)).

Las topologías lógicas de redes privadas virtuales más utilizadas son (en orden decreciente): estrella, malla parcial, malla completa y punto a punto.

Las dos aplicaciones que más utilizan Frame Relay en la actualidad son la interconexión de LANs y el acceso a Internet.

En una línea privada se puede transmitir a máxima velocidad (la velocidad del puerto físico de acceso) durante todo el tiempo, mientras que en un circuito virtual sólo pueden enviarse ráfagas a máxima velocidad y la velocidad media de transferencia de información debe permanecer por abajo del CIR. En contrapartida, el costo de un circuito virtual debe ser inferior al de una línea privada, sobre todo cuando se tienen líneas de larga distancia.

Originalmente, las redes Frame Relay ofrecieron sólo el servicio de PVCs en el que las conexiones entre los usuarios son establecidas por el administrador de la red y están disponibles permanentemente para la transmisión de datos. En este sentido, los PVCs son una alternativa al uso de líneas privadas. Actualmente, los proveedores de servicios Frame Relay empiezan a soportar SVCs en los que los usuarios pueden establecer conexiones temporales dinámicamente sin intervención del administrador de la red. Una diferencia muy importante entre los PVCs y los SVCs es que en los primeros el ancho de banda asignado a un circuito virtual ocupa recursos permanentemente en la red, mientras que en los segundos el ancho de banda negociado durante la fase de establecimiento de la conexión se libera al terminarse el SVC y puede ser utilizado posteriormente por otro circuito virtual. Debido a esto, los SVCs pueden basar sus tarifas en la duración de la conexión y/o en la cantidad de datos transmitidos y permitirán ofrecer ahorros a los clientes en una gran cantidad de aplicaciones. En general, los SVCs se utilizan cuando no se justifica tener una topología fija de conexiones permanentes y los usuarios requieren verdadero ancho de banda a la demanda. Por ejemplo, en el caso de transferencias esporádicas de grandes cantidades de información pueden crearse SCVs con un CIR alto durante un período corto de tiempo.

Frame Relay puede ser usada como una interfase a un proveedor público de servicios o a una red de equipo privado. Un método típico de implementación de red privada es equipar los tradicionales multiplexores T1 con interfases Frame Relay para dispositivos de datos, así como interfases no-Frame Relay para otras aplicaciones tales como voz y videoconferencia. La figura 4.5 muestra tal configuración.

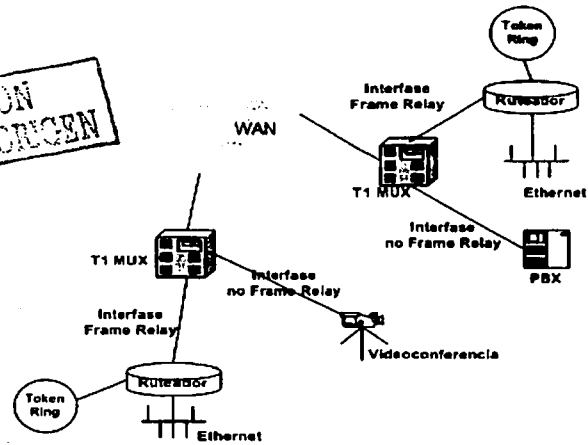


Fig. 4.5. Implementación de una red Frame Relay

4.2. ISDN (Integrated Services Digital Network)

4.2.1. Introducción

La digitalización de la red telefónica analógica ha dado a lugar a la Integrated Digital Network (IDN), en la que lo único que no es digital son las líneas de acceso de los usuarios.

El CCITT define a ISDN de la siguiente forma:

> "Una red que procede por evolución de una Integrated Digital Network (IDN) telefónica y que facilita conexiones digitales extremo a extremo para soportar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios tienen acceso a través de un conjunto limitado de interfases normalizados de usuario multiservicio"

Y también:

> "Un elemento clave de la integración de servicios para una ISDN es proporcionar un abanico de servicios utilizando un conjunto limitado de tipos de conexión y disposiciones de interfaz usuario-red de propósito general".

ISDN es un tipo de red de comunicación cuya aplicación fundamental es brindar conexión simultánea por un par de hilos de cobre (cables telefónicos) y transmitir voz, datos, texto, música, video. Estos servicios los proporciona u ofrecen las compañías regionales de larga distancia. Dentro de las aplicaciones de ISDN están las líneas telefónicas adicionales en las casas para dar servicio a la industria de ventas por teléfono, la transferencia de archivos a alta velocidad y la videoconferencia.

ISDN proporciona acceso integrado o combinado a dichos servicios. Un acceso integrado, implica que un usuario de ISDN tiene acceso tanto de voz como de otro tipo, desde una terminal y a través de una sola línea.

Al ser una red digital permite integrar señales analógicas, mediante la transformación analógico/digital, y digitales ofreciendo una capacidad básica de comunicación de 64 Kbps. La integración de los diferentes servicios ésta asegurada debido a la estructura digital de la propia red, ya que las señales digitales se transforman de código y las analógicas, mediante técnicas de muestreo, se digitalizan para su posterior envío.

En la figura 4.6 se puede observar un ejemplo de la integración de las diferentes señales mencionadas en ISDN.

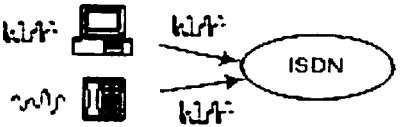


Fig. 4.6. Integración de señales analógicas y digitales

Los accesos a velocidades superiores a dos Mbps se engloban en la ISDN de banda ancha y se definen según la jerarquía de transmisión digital o en el modo de transferencia asíncrono (ATM).

El CCITT se dio a la tarea de dar recomendaciones que definen los conceptos y principios del ISDN y especificar sus capacidades de servicios, características de red, interfases usuario/red, interfases de interconexión y aspectos de mantenimiento. Lo anterior esta contenido en las

recomendaciones aprobadas por el CCITT en 1988. Estas recomendaciones se dividen en seis series, que van de la serie I.100 a la serie I.600:

4.2.2. ISDN en el modelo OSI

Los protocolos definen reglas para el intercambio de información entre los diferentes niveles de una red. El modelo OSI para redes está estructurado en siete niveles de los cuales solo los primeros tres se emplean para ISDN (figura 4.7).

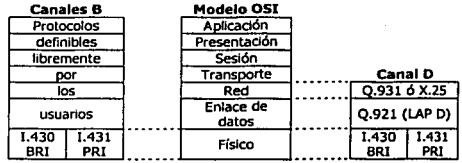


Fig. 4.7. Referencia ISDN con modelo OSI

4.2.2.1. Capa Física

Basado en la recomendación I.430, describe la conexión física entre el Equipo Terminal y el Terminador de Red. Define las características eléctricas, el tipo de conector, codificación de línea y framming. La conexión física es síncrona, serie y full-duplex. Los canales B y D son multiplexados en el tiempo sobre la misma línea física en una misma trama, desde NT1 en casa del usuario y la central telefónica.

Los formatos de trama de la capa 1 (capa física) de ISDN difieren en función de si la trama está direccionada hacia un destino externo (de la terminal a la red) o hacia un destino interno (de la red hacia la terminal). En la siguiente figura se muestran ambas interfases de la capa física.

Las tramas tienen una longitud de 48 bits, de los cuales 36 representan datos.

4.2.2.2. Capa de Enlace de Datos

Describe los procedimientos que aseguran la comunicación libre de errores sobre el enlace físico y define la conexión lógica entre el usuario y la red. El protocolo también proporciona las reglas para la conexión de múltiples terminales sobre la misma línea física (multipunto).

La capa 2 del protocolo de señalización de ISDN es el procedimiento LAP D (Procedimiento de Acceso al Enlace, canal D). LAP D es parecido a HDLC (High-Level Data Link Control) y a LAP B (Procedimiento de Acceso al Enlace, Balanceado). Como la extensión de las siglas LAP D lo indica, esta capa se utiliza a través del canal D para asegurar que la información de control y señalización fluya y sea recibida adecuadamente. El formato de trama de LAP Des muy parecido al de HDLC y, como HDLC, LAP D utiliza tramas de supervisión, de información y no numeradas.

4.2.2.3. Capa de Transporte

Define la interfaz los mensajes de señalización entre el usuario y la red. El protocolo implementado a este nivel determina las rutas tomadas a través de la red para conectar a los usuarios entre sí.

Para la señalización en ISDN se utilizan dos especificaciones de la Capa 3: la I.450 (tambien conocida como ITU-T Q.930) y la I.451 (también conocida como ITU-T Q.931) de la ITU. En conjunto, estos protocolos soportan conexiones entre usuarios, utilizando conmutación de circuitos y de paquetes. Se especifica una gran cantidad de mensajes de establecimiento de llamada, terminación de llamada, información y misceláneos, incluyendo SETUP, CONNECT, RELASE, USER INFORMATION, CANCEL, STATUS, y DISCONNECT. Estos mensajes son funcionalmente semejantes a los que ofrece el protocolo X.25.

4.2.3. Tipo de Acceso de ISDN

El tipo de acceso se refiere al tipo de servicio que se contrata con la compañía telefónica a continuación se describen los dos más importantes.

4.2.3.1. Acceso Básico (2B+D) o BRI (Basic Rate Interface)

Denominado acceso Básico de usuario c acceso 2B+D, está formado por:

- 2 B. Dos canales conmutados a 64 Kbps para transferencia de información extremo a extremo en modo digital.
- 1 D. Un canal de señalización y control en modo paquete según el protocolo denominado LAP D (Protocolo de acceso al Enlace por Canal D en Ingles) con una velocidad efectiva de 16 Kbps. Debido a que este canal se mantiene mucho tiempo inactivo se especifica que puede emplearse para informaciones del cliente en modo paquete. (recomendación X.25). También puede soportar la transmisión de datos de usuario en determinadas circunstancias.

La interfase BRI también ofrece el control de entramado, entre otras características, lo que permite que la tasa total sea de 192 Kbps. Este acceso se emplea para entornos con bajo volumen de tráfico, y que puede satisfacer las necesidades de la mayoría de usuarios individuales, viviendas y pequeñas oficinas.

Es posible la utilización de ambos canales B para una misma comunicación, en realidad para videotelefonía o videoconferencia se emplean los dos canales de forma simultánea debido a que la utilización de un solo canal B no permite una conexión clara en imagen.

4.2.3.2. Acceso Primario. (30B+D)

El acceso Primario o acceso 30B+D se constituye en la forma siguiente:

- 30 B. Treinta canales conmutados de velocidad 64 Kbps, para información de cliente.
- 1 D. Es un canal de señalización a 64 Kbps, empleado también para el envío de información en modo paquete.

En Estados Unidos y Japón se ofrecen 23 canales B y un canal D, con una tasa total de 1.544 Mbps. Se emplea en entornos con alto volumen de tráfico, como oficinas con PBX, LAN o bases de datos.

Como en todo sistema de transmisión digital necesitamos de elementos de sincronización, se añade un canal más a 64 Kbps para la sincronización de trama. De esta forma el acceso Primario se compone de 32 canales de 64 Kbps (32 x 64 = 2048 Kbps = 2 Mbps.)

En el acceso Primario ISDN se permiten además agrupaciones de varios canales para transferencia de información:

- Canales HO 6 canales a 64 Kbps
- Canales H12 velocidad 384 Kbps.
- 30 canales a 64 Kbps, velocidad 1920 Kbps.

Es lógico suponer que el acceso básico está definido para Clientes o aplicaciones que requieran poca capacidad de transferencia de información, mientras que el acceso Primario está definido para clientes con media necesidad de información. Para clientes con gran capacidad de información se hará necesario la utilización de accesos en banda ancha.

Configuración de referencia

La configuración de referencia está definida por agrupaciones funcionales (equipos con una función específica) y puntos de referencia o interfaces puntos definidos en los que la ISDN presenta características de transmisión o conmutación determinadas

4.2.3.3. Agrupaciones funcionales

Las agrupaciones funcionales son elementos que desarrollan una función, en este caso corresponden a equipos o elementos del mismo Cliente o central.

TC, Terminación de central

Situada en la central de Conmutación, se encarga del mantenimiento del acceso de usuario y realiza la conexión de canales. Soporta la señalización del usuario y el envío de información en modo paquete.

TL, Terminación de Línea

Situada en la central, se encarga de los aspectos de transmisión convirtiendo el código binario al código de línea empleado. Controla la sincronización del acceso. Ésta agrupación funcional se encuentra unida a la TC formando una agrupación.

TR1, Terminación de red No.1

Es el primer elemento en el domicilio del Cliente y obligación de la compañía explotadora del servicio, permite la sincronización con los equipos conectados a continuación y controla la conexión con la central. Adecúa las señales de la línea a códigos adecuados para la conexión de los equipos y permite la verificación a distancia, pudiéndose evaluar la calidad del enlace.

TR2, Terminación de red No.2

Realiza funciones de control en la instalación del Cliente como: tratamiento de la señalización, multiplexación de canales de información, conmutación local, concentración de tráfico y mantenimiento de la instalación del usuario.

ET1, Equipo Terminal No.1

Es el Equipo Terminal ISDN. Este está preparado para señalización en modo paquete y gestión de canales de información. Algunos ejemplos pueden ser Teléfonos ISDN equipos de Videotelefonía, Tarjetas de PC, etc.

AT Adaptador de Terminales

Equipo ISDN que tiene la capacidad de adaptar interfaces. Convierte las señales de otros equipos no ISDN a señales adecuadas a la interfase correspondiente (interfase "S").

ET2 Equipos Terminales No.2

Equipos no ISDN que pueden conectarse mediante una interfase normalizada a la red Fax Grupos dos y 3, teléfonos analógicos, módem.

4.2.4. Servicios

Se definen a continuación los tres diferentes servicios que ofrece la ISDN en los diferentes accesos de usuario de banda estrecha.

4.2.4.1 Servicios portadores

Existen diferentes servicios Portadores englobados en dos categorías diferentes: servicios Portadores en modo circuito y servicios portadores en modo paquete.

Servicios portadores en modo circuit

Presentan la posibilidad de conexiones a velocidades de 64 Kbps o superiores mediante conmutación de circuitos. Se definen tres servicios en función del tratamiento de la señal digital:

a) servicio portador a 64 Kbps sin restricciones.
Se define como el servicio portador que puede emplear uno o varios canales a 64 Kbps, sin ninguna estructura predefinida, de forma que la central es transparente a la información del usuario. Por extensión del servicio que puede prestar se denomina también servicio portador de datos.

b) servicio portador para conversación.
Se define como el servicio portador que mediante la utilización de un canal a 64 Kbps permite la comunicación de voz extremo a extremo. Está estructurado según la codificación de una señal digitalizada de ancho de banda cuatro KHz. Es el servicio de voz de la ISDN.

c) servicio portador 3.1 KHz.
Se define como el servicio portador que emplea un canal de 64 Kbps para intercambio de información con un ancho de banda de 3.1 KHz. Desde 300 Hz a 3400 Hz. Necesita de un adaptador de terminales. Las señales analógicas pueden generarse en un Fax de Grupo 2, en un módem, en un teléfono analógico, etc.

SERVICIOS PORTADORES EN MODO PAQUETE

Permite la explotación del canal D para comunicaciones en modo paquete con otros usuarios de la red. Así mismo puede interconectar un ET con la red de conmutación de paquetes X.25

SERVICIO PORTADOR EN MODO PAQUETE VIRTUAL

Se define como el servicio portador en modo paquete que emplea procedimientos de llamada para el establecimiento de la conexión en modo paquete. Su velocidad binaria es de 9600 bps, aunque en algunos casos puede llegar a velocidades similares a la del canal D.

SERVICIO PORTADOR EN MODO PAQUETE PERMANENTE

Se define así al servicio de conmutación de paquetes exento de las fases de establecimiento de llamada, de esta forma la conexión se efectúa entre dos entidades de conmutación de paquetes de forma permanente y la transferencia de información efectiva supera al servicio anterior, si bien no puede elegirse el destinatario de la información. Aunque la velocidad binaria de transferencia de datos es igual a la del caso anterior, la ausencia de elementos de control de la comunicación permite enviar más información con menos paquetes.

4.2.5. Línea de transmisión

Se entiende por línea de transmisión al medio físico necesario que sirve de soporte al acceso del usuario. Se comentan a continuación las características de las líneas para cada acceso:

- Acceso Básico: línea de transmisión a dos hilos mediante cable de cobre. Gracias a los códigos de línea empleados, sistemas de reducción del ancho de banda de transmisión, se pueden alcanzar los cinco Kilómetros. sobre cable de pares de calibre normal. En el caso de excesiva pérdida debido a la distancia se pueden emplear sistemas de regeneración o multiplexores que son capaces de multiplexar 12 accesos básicos en una trama a dos Mbps.
- Acceso Primario: la línea de transmisión estará formada por dos pares de hilos o por fibra óptica. En el caso de Clientes que posean fibra óptica se tenderá un agregado a 2Mbps para el acceso. Si el Cliente no posee fibra óptica se emplearan dos pares de cable metálico (cobre), similares a los empleados en el acceso Básico, mediante unos módem 88 (Banda Base) a dos Mbps se podrá poner en servicio el acceso.

4.2.5.1. Equipos terminales de cliente

Aunque la ISDN tiene en funcionamiento poco tiempo, las posibilidades de comunicación que presta han forzado a muchas empresas del sector de las comunicaciones a desarrollar equipos de muy diversa índole, adecuados a necesidades de los posibles Clientes de la red.

EQUIPOS TERMINALES ISDN

Existe una gran variedad de equipos terminales de Cliente para la ISDN, a continuación se describen algunos de estos equipos:

- *Telefonía.* En la actualidad existe variedad de modelos Homologados. En general permiten los servicios suplementarios más comunes.
- *Adaptadores.* Se pueden conectar:
  - Teléfonos analógicos.
  - Teléfonos inalámbricos analógicos.
  - Fax de Grupos 2/3.
  - Módem según recomendación "V".
  - Contestadores analógicos.
  - Los adaptadores que trabajan con canal O.
- *Nucleox uno y 4.* Permiten la conexión de diferentes equipos terminales a la línea ISDN para trabajar en modo paquete o modo circuito.
- *Equipos de transmisión de datos.* Son CODEC que transforman las señales digitales del ordenador en señales específicas de interfase S en ISDN.
- *Equipos de Back-Up (8IR-64).* Equipo que permite líneas de 8ack-up por ISDN. Se establece un circuito Punto a Punto y en el caso de caída del circuito se establece una llamada ISDN por canal 8.
- *Tarjetas específicas para PC.* En la actualidad se comercializan tarjetas que permiten la conexión para voz y datos para la transferencia de archivos.

EQUIPOS PARA ISPBX

El grupo ISPBX se define como un servicio de la ISDN que permite la asociación de varios accesos ISDN, ya sean básicos o primarios, con un bloque de numeración. De esta forma se ofrece al usuario la posibilidad de gestionar sus comunicaciones de forma Local, empleando para ello un PBX ISDN. Este servicio es una de los más atractivos en la actualidad ya que el PBX permitirá el uso de diferentes equipos terminales, gestionando cada uno de ellos de forma independiente y transparente a la información de usuario:

- Teléfonos analógicos.
- *Teléfonos Propietario.* Con una interfase digital definido por el propio fabricante.
- *Equipos Terminales ISDN.* Videotelefónos. Teléfonos. Fax de Grupo 4.
- *Equipos analógicos.* MODEM. Fax Grupos 2/3. Contestadoras.
- *Equipos inalámbricos.* Teléfonos sin hilos de interfase específica definido por el fabricante.

Algunos de los servicios que prestan estos PBX son: llamada en espera, conferencia a tres, retrollamada, llamadas dirigidas a grupos de extensiones desvíos internos o externos, selección directa a extensiones y algunas otras características de utilización muy interesantes para el rendimiento en transferencia de información del usuario.

4.2.6. B-ISDN (Broadband Integrated Service Digital Network)

Es una red de telecomunicaciones capaz de soportar aplicaciones multimedia, y que además posee poderosos sistemas de control de red que permiten operaciones y complejas y servicios de administración sofisticados. Un ejemplo de esto es el hecho de poder establecer conexiones no sólo tomando en cuenta el número marcado, sino también evaluando la identidad de la persona que llama, la cantidad de recursos asignados a esa persona, así como el tráfico de la red en el momento de la llamada.

4.2.6.1. Estándares

El concepto de B-ISDN se introduce por primera vez en 1988 con la recomendación 1.121 del CCITT. Para 1990 el Grupo de Estudio XVIII aprueba algunas recomendaciones básicas, entre las que se incluyen aspectos generales de B-ISDN, servicios específicos de Red, características fundamentales de ATM, aplicaciones ATM, operación y mantenimiento de los accesos a B-ISDN.

Características de B-ISDN:

- Un solo canal de transmisión y recepción Bajo costo.
- Utilizada por los estándares actuales de redes locales.
- Multiplexaje por frecuencia.
- Conexiones conmutadas por demanda en Broad band.
    - Permanentes.
    - Semipermanentes.
- Aplicaciones.
    - Punto a punto.
    - Punto a multipunto Modo de conmutación Paquetes Circuitos.
- Naturaleza de servicios.
    - Orientados a conexión.
    - No orientados a conexión.
- Configuraciones.
    - Unidireccionales.
    - Bidireccionales.
- Tráfico.

- Velocidad constante CBR (Constant Bit Rate).
- Velocidad variable VBR (Variable Bit Rate).

4.2.6.2. Servicios

Los servicios de B-ISDN (figura 4.8) se clasifican en:

- Servicios interactivos. Son aquellos en los cuales hay un intercambio bidireccional de información ya sea entre dos subscriptores o un proveedor de servicios. Estos servicios a su vez se dividen en:
  - Servicios conversacionales. Proporcionan el medio para una comunicación bidireccional en tiempo real.
  - Servicios de mensajería. Ofrecen comunicación subscriptor a subscriptor mediante unidades de almacenamiento en oficina y manejo de mensajes. Este tipo de servicios normalmente no están garantizados.
  - Servicios de recuperación por solicitud. Proporcionan al usuario la capacidad de obtener cierta información específica.

- Servicios de distribución: Estos servicios se proporcionan sin control con control de presentación:
  - Sin control de presentación: Proporcionan un flujo continuo de información que se distribuye desde una fuente central hacia un número ilimitado de receptores conectados a la red. El subscriptor puede accesar a esta información pero no tiene control sobre ella. Un ejemplo análogo de este servicio es la señal de televisión pública. Todos los destinatarios tienen la señal al mismo tiempo.
  - Con control de presentación: Estos servicios también distribuyen información de una fuente central a un gran número de usuarios, sin embargo la información se envía a una secuencia de entidades de información, con repetición cíclica de tal modo que el usuario tiene la habilidad de accesar y controlar el inicio y orden de la presentación de la información. Un ejemplo es el pago por evento, en donde sólo los usuarios que desean pagar y recibir un determinado programa lo hacen así.

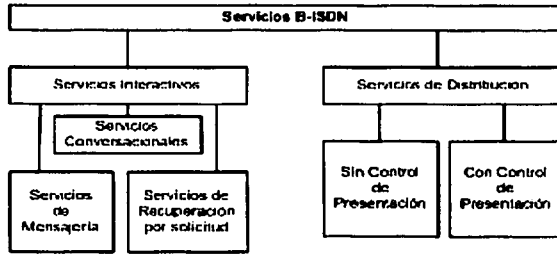


Fig. 4.8. Servicios B-ISDN

Se requiere un canal de al menos 150 Mbps para soportar video de alta resolución mientras que para soportar simultáneamente más de un servicio se requiere que el subscriptor tenga una línea de 600 Mbps. La única tecnología que soporta esta tasa de transmisión es la fibra óptica.

4.3. ATM

4.3.1. Introducción

ATM *(Asynchronous Transfer Mode,* o Modo de Transferencia Asíncrono) es una de las más modernas técnicas de conmutación para telecomunicaciones, altamente eficiente, que se puede aplicar a diferentes tipos de información y a diferentes velocidades de transmisión. No es una técnica limitada a redes de telefonía o de datos, sino que permite que una red se utilice para la transferencia de diferentes tipos de señales, de manera simultánea (p. ej. teléfono, datos y video). Es, por lo tanto, la técnica integrada de conmutación que formará la base de la Red Digital de Servicios Integrados de Banda Ancha, B-ISDN *(Broadband Integrated Services Digital Network). Se* considera a ATM como un subconjunto de B-ISDN.

En 1987, la ITU-T (entonces CCITT) selecciona el ATM como la respuesta adecuada para integrar las ventajas de la conmutación de paquetes y de la conmutación de circuitos. En 1990, la ITU-T añadía un conjunto de 13 Recomendaciones a la serie I (ISDN) para especificar los aspectos más importantes de ATM. En esencia, las características más significativas de las redes ATM son:

- Utilización del canal o la red por múltiples usuarios simultáneamente.
- Cada usuario con necesidades de telecomunicación diferentes (p. ej. teléfono, transmisión de datos, interconexión a LANs, transmisión de video, etc.) y
- Cada aplicación corriendo a diferentes velocidades de transmisión, es decir, cada aplicación tiene diferentes necesidades de ancho de banda.
- la asignación dinámica y flexible del ancho de banda.
- la ganancia estadística, es decir, su capacidad de optimizar la relación entre la suma de las velocidades de pico de las fuentes y la velocidad del enlace.

Por estas razones, la tecnología ATM, que fue propuesta originalmente por la Industria de las Telecomunicaciones, es recomendada en la actualidad como solución universal para redes de banda ancha por los más importantes organismos de las industrias de Comunicaciones y Computadoras, como la mencionada ITU-T, el ATM Forum o el IETF.

Los conceptos de ATM son, en esencia, muy simples:

- Operación por conmutación de paquetes, si bien se utilizan paquetes de longitud fija (48 octetos de información y 5 octetos de control), denominados celdas. Esta opción de celdas de tamaño fijo permite el uso de nodos de conmutación a velocidades muy altas.
- Orientado a conexión al nivel más bajo. La información se transfiere por canales virtuales asignados durante la duración de la conexión.
- La asignación del ancho de banda se realiza en función de la demanda de envío de tráfico.
- No se realiza control de errores en el campo de datos, y el control de flujo se realiza fundamentalmente por los equipos de usuario. Con ello se maximiza la eficiencia.
- Proporciona transparencia temporal, es decir, pequeñas variaciones de retardo entre las señales de la fuente y el destino. Por ello permite la transferencia de señales isócronas.
- Las celdas se transmiten a intervalos regulares; si no hay información se transmiten celdas no asignadas.
- Se garantiza que las celdas llegan a su destino en el mismo orden en el que fueron transmitidas.

Aunque estas capacidades las ofrecen también tecnologías predecesoras (anteriores tecnologías), la diferencia con ATM es que es capaz de hacer ajustes *en cada instante* en la asignación de recursos de red disponibles entre los diferentes usuarios compitiendo por su uso. En lugar de asignar una capacidad fija entre las dos partes que se están comunicando, por el período de una sesión o llamada, ATM se asegura que la capacidad de la línea se utilice de manera óptima, al transportar únicamente la información útil o que se necesita. Por ejemplo, las pausas o silencios

en una conversación telefónica no necesitan transmitirse, y en su lugar se pueden enviar pequeños paquetes de datos. Esta asignación dinámica de recursos se logra mediante una tecnología llamada *cell relay switching (conmutación de retransmisión de celdas).*

ATM proporciona un ancho de banda expandible desde algunos megabits por segundo (Mbps) hasta muchos gigabits por segundo (Gbps). Debido a su naturaleza asíncrona, ATM es más eficiente que las tecnologías síncronas como el TDM *(Multiplexaje por División de Tiempo).*

4.3.2. Formato de celda

El formato de la celda de 53 bytes consiste de un encabezado de 5 bytes y 48 bytes para la información.

En la figura 4.9 se observa el formato básico de la celda ATM, el formato del encabezado UNI y el del encabezado NNI de la celda ATM. A diferencia del encabezado UNI, el encabezado NNI no incluye el campo GFC. Además, el encabezado NNI tiene un VPI que ocupa los primeros 12 bits, y permite que haya troncales más grandes entre switches públicos ATM.

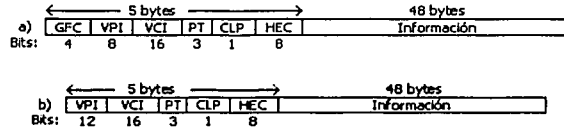


Fig 4.9. Formato de la celda ATM, (a) en el UNI y (b) en el NNI

La definición de los campos de la celda se describe a continuación:

- *Generic Flow Control, GFC.* Proporciona funciones locales como la identificación de múltiples estaciones que comparten una sola interfase de ATM. En general, este campo no se utiliza pues no se ha estandarizado y se fija su valor en ceros. Únicamente aparece en el formato de encabezado de la interfaz usuario-red. Este campo puede servir para ayudar al cliente a controlar el flujo de tráfico para diferentes calidades de servicio (QoS), y puede utilizarse en una de dos maneras, para aliviar condiciones pico de sobrecarga en la red. En la primera, para configuraciones punto a punto, el GFC puede controlar el flujo desde un TE individual. En la segunda, para configuraciones punto a multipunto, el GFC proporciona control de flujo adicional al ya existente. Sin embargo, este campo también puede utilizarse como control de acceso al medio cuando se tienen múltiples terminales a nivel de interfaz usuario-red.
- *Virtual Path Identifier, VPI.* En conjunto con el VCI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en camino a su destino.
- *Virtual Channel Identifier, VCI.* En conjunto con el VPI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en camino a su destino.
- *Payload Type, PT.* Indica en el primer bit si la celda contiene datos del usuario o datos de control. Si la celda contiene datos del usuario, el segundo bit indica si hay saturación y el tercer bit indica si la celda es la última de una serie de celdas que representan una sola trama AAL5. Para celdas de información de control, la carga tiene información de las funciones de supervisión dependiendo del tipo particular de celda y control de tráfico.

- *Cell Loss Priority, CLP.* Indica si la celda se debiera eliminar al encontrar un alto grado de saturación a su paso por la red. Si el bit CLP es igual a 1, la celda se deberá eliminar para dar preferencia a las celdas cuyo bit CLP sea igual a cero.
- *Header Error Control, HEC.* Emplea el ciclo de verificación redundante (CRC) para la protección de error del encabezado de la celda

4.3.3. Interfases y dispositivos

Los estándares ATM definen dos interfaces significativas y una especificación adicional por el Foro ATM, B-ICI:

- User Network Interface, UNI.
- Network to Network Interface, NNI.
- Broadband Inter Carrier Interface.

Existen cuatro tipos de equipo para conformar una red ATM:

- Equipo terminal ATM.
- Switch ATM.
- Crossconects ATM.
- Multiplexores ATM.

La UNI conecta los equipos terminales (clientes y ruteadores) con switches, crossconect o multiplexores ATM.

La NNI conecta dos switches ATM. B-ICI conecta dos switches públicos de diferentes proveedores de servicio. La figura 4.10 muestra las especificaciones de interfase ATM para redes públicas y privadas.

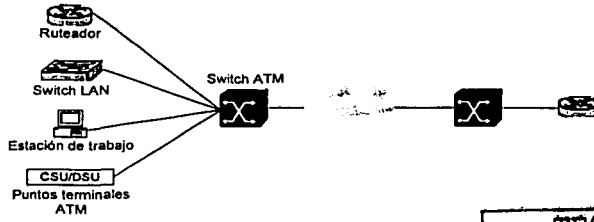


Fig. 4.10. Interfase ATM

4.3.4. Conexiones Virtuales

Al ser ATM una técnica orientada a conexión, tiene que establecerse una conexión virtual entre usuarios finales antes de que se comience a transmitir la información. Las conexiones pueden establecerse mediante procedimientos de señalización del plano de control o pueden ser permanentes o semipermanentes, establecidas por procedimientos del plano de gestión.

A cada conexión se le asigna un conjunto de parámetros de tráfico y de QoS, de acuerdo con las peticiones del usuario, siempre que puedan ser proporcionadas por la red. Esta asignación se realiza normalmente durante el establecimiento de la conexión, mediante un proceso denominado Control de Admisión de conexión (CAC). Este proceso determina los parámetros que se

asignan a la conexión en función de los requisitos de los usuarios; se establece entonces lo que se denomina un "contrato de tráfico".

Durante la transferencia tiene lugar también otro proceso denominado Control de Parámetros de Usuario, UPC, denominado familiarmente "policía de tráfico", cuya misión es monitorear la conexión y tomar las medidas oportunas en caso de que la conexión exceda los límites asignados.

Estas conexiones virtuales significan que se establecen canales virtuales (CV, Virtual Channels) a través de la red ATM antes de cualquier transferencia de datos.

En ATM hay dos tipos de conexiones: las trayectorias o rutas virtuales (VP, Virtual Path), que se identifican por medio de identificadores de trayectoria virtual (Virtual Path Identifier, VPI) y los canales virtuales, que se identifican por la combinación de un VPI y un VCI (Virtual Channel Identifier).

Una trayectoria virtual es un conjunto de canales virtuales que están conmutados de manera transparente a través de una red ATM con base en VPI comunes. Sin embargo, todos los VCIs y VPIs tienen significado local solamente a través de un enlace particular y se calculan de nuevo en cada switch, según sea necesario. La combinación VPI/VCI sí es única y suficiente para identificar cualquier conexión activa en la interfase.

Una ruta o trayectoria de transmisión es un conjunto de VPs. La figura 4.11 muestra como se encadenan los VCs para crear VPs, que a su vez, se enlazan para crear una trayectoria de transmisión.

Fig. 4.11. Trayectoria de tranmisión

Un multiplexor ATM permite que varios canales virtuales de diferentes rutas virtuales se junten en una sola. Un Crossconect ATM permite que se reordenen las rutas virtuales sin que se afecten los canales virtuales que contienen. Un switch ATM completo tiene la capacidad no sólo de interconectar rutas virtuales, sino también de conmutar canales virtuales de diferentes rutas virtuales.

Las conexiones lógicas en ATM se denominan Conexiones de Canal Virtual (VCC, Virtual Channel Connection), concepto heredado del circuito virtual de las redes de paquetes X.25, también similar a la conexión lógica en Frame Relay.

Adicionalmente a las VCC, en ATM se introduce el concepto de Trayecto Virtual. Una conexión de Trayecto Virtual, (VPC, Virtual Path Connection), es un conjunto de VCC que tienen los mismos puntos de terminación. Por consiguiente, todas las celdas del conjunto de los VCC se conmutan conjuntamente en una única VPC. De esta forma, se reducen los costos de control y gestión de la red.

4.3.4.1. Servicios

En las redes ATM existen dos tipos de servicios: PVC, Permanent Virtual Connection y Switched Virtual Connection.

Los PVCs se establecen por medio de un operador humano, y son conexiones que están definidas por configuración de la red y siempre existirán entre dos o más puntos finales. Permiten la conectividad directa y es similar a una línea privada. Una de las ventajas de una PVC es que garantiza la disponibilidad de una conexión y no requiere los procedimientos asociados con el establecimiento de llamada entre switches. Las desventajas de las PVCs, son la conectividad estática y el establecimiento manual.

En una SVC se genera y libera dinámicamente y permanece en uso sólo mientras se lleva a cabo la transferencia de datos. En este sentido, es similar a una llamada telefónica.

4.3.5. Modelo de referencia

La arquitectura ATM utiliza un modelo lógico para describir la funcionalidad que soporta. La funcionalidad de ATM corresponde a la capa física y parte de la capa de enlace de datos del modelo de referencia OSI.

El modelo de referencia ATM se compone de los siguientes planos que se extienden a través de todas las capas:

- *Control.* Es responsable de la creación y administración de las solicitudes de señalización.
- *Usuario.* Este plano es responsable de la administración de transferencia de datos.
- *Administración.* Este plano tiene dos componentes:
  - *La administración en capa* se encarga de administrar las funciones específicas de la capa como detección de fallas y los problemas de los protocolos.
  - *La administración en plano* se encarga de administrar y coordinar las funciones relacionadas con todo el sistema.

El modelo de referencia ATM se compone de las siguientes capas:

- *Capa física.* Administra la transmisión de la información estructurada en celdas dependiente del medio físico de transmisión.
- *Capa ATM.* Es responsable de establecer conexiones y pasar celdas a través de la red ATM. Para realizar esta función, utiliza la información del encabezado de cada celda ATM.
- *Capa AAL (Adaptation ATM Layer).* Es responsable de aislar los protocolos de capas superiores de los detalles de los procesos de ATM.

Las capas que residen arriba de la capa AAL, aceptan datos del usuario, los conforman en paquetes y los entregan a la AAL. La figura 4.12 muestra el modelo de referencia ATM.

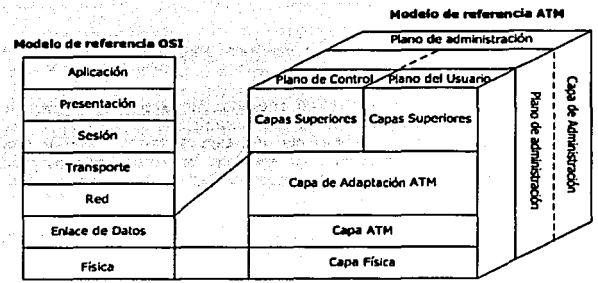


Fig 4.12. Modelo de referencia ATM

4.3.5.1. Capa física

Esta capa tiene cuatro funciones: convertir los bits en celdas; controlar la transmisión y recepción de bits en el medio físico; supervisar los límites de las celdas de ATM; empaquetar las celdas en un tipo de trama adecuado para enviarlas a través del medio físico.

Esta capa se divide en dos subcapas: subcapa PMD (Dependiente del Medio Físico) y TC (Convergencia de Transmisión).

La subcapa PMD presenta dos funciones básicas. Primero, sincroniza la transmisión y la recepción a través del envío y recepción de un flujo continuo de bits con la información de temporización asociada. Segundo, especifica el medio físico para el medio de transmisión que se va a utilizar, incluyendo los tipos de conector y cable. Algunos ejemplos de estándares de medios de transmisión para ATM son la SONET/SDH (Red Óptica Síncrona / Jerarquía Digital Síncrona), DS3/E3, 155 Mbps a través de MMF (Fibra Óptica Multimodo) utilizando el esquema de codificación 8B/10B y 155 Mbps 8B/10B, a través de cableado STP. El aspecto más importante del nivel físico de ATM es que no define ningún tipo de medio específico. Soporta muchos tipos de medios, inclusive aquellos existentes y utilizados en otros sistemas de comunicaciones. Varias especificaciones de interoperabilidad aún se encuentran bajo desarrollo.

La subcapa TC tiene cuatro funciones: delineamiento de celdas, generación y verificación de la secuencia HEC, desacoplamiento de la tasa de celdas y adaptación de la trama de transmisión. La función de delineación de celdas conserva los límites de las celdas ATM, y permite así que los dispositivos puedan ubicar celdas dentro de una ráfaga de bits. La generación y verificación de la secuencia HEC crea y verifica el código de control de errores del encabezado para asegurar la validez de los datos. El desacoplamiento de la tasa de celdas conserva la sincronización e inserta o suprime celdas ATM libres (no asignadas) para adaptar la tasa de celdas ATM válidas a la capacidad de carga útil del sistema de transmisión. La adaptación de la trama de transmisión empaqueta las celdas ATM en tramas aceptables para la implementación de la capa física particular.

Tipo de medio en redes ATM

Entre las capas físicas propuestas para las redes ATM, pueden señalarse:

- ATM sobre SDH: STM-1 (155,52 Mbps) y STM-4 (622,08 Mbps)

- ATM sobre PDH: E1 (2,048 Mbps), DS1 (1,548 Mbps), Ds2 (6,312 Mbps), E3 (34,368 Mbps), E4 (139,264 Mbps) y DS3 (44,736 Mbps).
- ATM a 100 Mbps sobre FDDI (TAXI).
- ATM a 25,6 Mbps. (Solución propuesta por IBM en el ATM Forum para llevar ATM a la estación de trabajo).

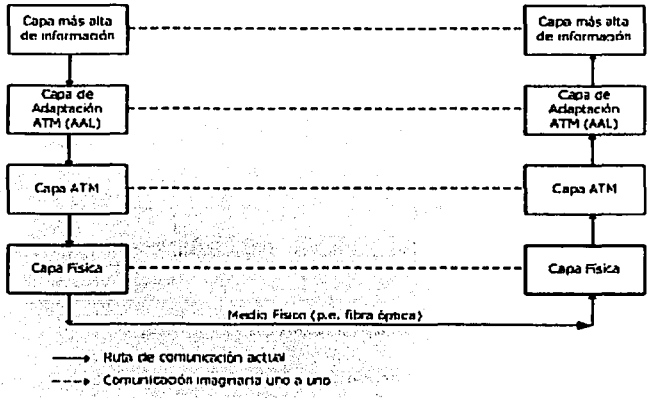
4.3.5.2. Capa ATM

La misión principal de la capa ATM es la transferencia del flujo de celdas a través de la red. En esta capa reside el control de tráfico, congestión, admisión de conexión y parámetros de uso y de red incluyéndose algunos mecanismos que se describen en el apartado Control de tráfico y congestión.

También se añade el campo de cabecera para establecer los mecanismos de ruteo, control de flujo y corrección de errores. Para ello, la capa ATM realiza un conjunto de funciones que describimos a continuación:

4.3.5.3. Capa AAL

La capa de adaptación ATM (figura 4.13) como su nombre lo indica es la responsable de desarrollar el mapeo necesario entre la capa ATM y los protocolos de capas superiores. Es decir, esta capa es donde ATM encapsula el tráfico de las aplicaciones superiores del usuario dentro del formato de ATM. Proporciona la conversión de información dentro de un formato que pueda viajar a lo largo de la red ATM. Conversión de un teléfono, datos o bien otras señales de comunicación dentro del formato de celda ATM. Para la recepción final, AAL invierte la conversión, regresando las celdas dentro de la señal original.



4.13. Modelo de referencia de Protocolo de la Capa de Adaptación (AAL)

Como se puede observar, la red ATM es independiente del tipo de tráfico que está lleva, esto es debido a que ATM no conoce la estructura de la información que acarrea y no lleva a cabo ningún proceso de reconocimiento de está; además de que la red ATM es de cierta forma independiente del tiempo, es decir, no existe relación entre la coordinación del tiempo de la aplicación origen y el tiempo de reloj de la red.

4.3.6. Multiplexaje Estadístico y Cell Relay Switching

ATM se basa en una técnica de multiplexaje estadístico llamada *conmutación de retransmisión de celdas* (cell relay switching). El multiplexaje estadístico es una forma de multiplicar la capacidad efectiva de una red o línea de transmisión, al tomar ventaja de la naturaleza estadística de las ocasiones en que se necesita transportar información. Con este método, es posible suprimir los periodos de silencio para que no se transmitan por la línea. Mientras tanto, las palabras de otras conversaciones pueden transmitirse en esos espacios. Este concepto se aplica también a la transmisión de datos, y de hecho se hace de una manera más eficiente, ya que se pueden entrelazar los caracteres separados de diferentes textos, o bien transmitir diferentes archivos de datos rápidamente uno detrás de otro.

En la figura 4.14, se ilustra la técnica del multiplexaje estadístico. Tres usuarios separados (representados por A, B y C) se comunican a través de la misma línea de transmisión. Los tres diferentes circuitos fuentes se conectan al multiplexor y este a su vez a un demultiplexor al otro extremo de la línea.

Lo único que hace este multiplexor es enviar todo lo que recibe de cualquiera de los circuitos directamente a la línea de transmisión. La razón por la que se le llama *estadístico* es porque depende de la probabilidad estadística de que los tres circuitos no quieran transmitir al mismo tiempo. De hecho, el multiplexor está diseñado para poder atender transmisiones simultáneas de todas las fuentes, por períodos cortos de tiempo. Si el tiempo es largo, los espacios de almacenamiento temporal (buffers) se llenan y se desbordan.

Para prevenir la pérdida de información, el sistema debe planearse para que la suma de los *promedios* de flujo de cada canal sea menor que la capacidad máxima de la línea de transmisión. En realidad, la capacidad de la línea debe ser de 1.5 a 2 veces la suma de los flujos (A+B+C) para que el multiplexaje estadístico funcione de manera confiable. De otro modo, se presentan congestionamientos, seguidos algunas veces de largos períodos de holganza del sistema.

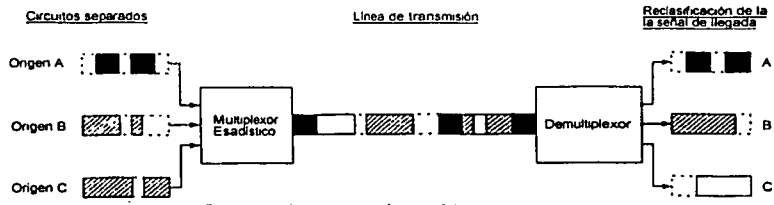


Fig. 4.14. Multiplexaje Estadístico y Cell Relay Switching

Las redes públicas de voz, a diferencia de las redes de datos, no utilizan este multiplexaje, sino que utilizan la conmutación de circuitos.

Cell relay es una forma de multiplexaje estadístico similar en varios aspectos a la conmutación de paquetes, sólo que en lugar de *paquetes* se les llama *celdas* a las unidades básicas

de información. Debido a las velocidades que maneja ATM y el corto tamaño de la celda, la duración de la transmisión de la celda también es muy pequeño, lo que permite aplicar un esquema de prioridades para que las aplicaciones muy sensibles a los retrasos (como el video o la voz) tengan acceso a la siguiente ranura de celda disponible. En cambio, las aplicaciones en las cuales no importan las variaciones en el retraso de propagación de la señal, se les puede asignar únicamente las ranuras de celda de baja prioridad.

- *Expansión de las capacidades de direccionamiento.* IPv6 incrementa el tamaño de direcciones de 32 bits (2^{32}; 4,294,967,296) a 128 bits (2^{128} direcciones; 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456), para soportar mas niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables y un sistema de autoconfiguración de direcciones. Significa que si la población mundial fuera de 10 billones habría $3.4 * 10^{27}$ direcciones por persona. O visto de otra forma habría un promedio de $2.2 * 10^{20}$ direcciones por centímetro cuadrado. Siendo así muy pequeña la posibilidad de que se agoten las nuevas direcciones. Se añade un nuevo tipo de dirección, la llamada ANYCAST, de forma que es posible enviar un paquete a cualquier nodo entre un grupo de ellos, UNICAST y MUTLICAST.
- *Simplificación de la cabecera.* Algunos campos de la cabecera de IPv4 son eliminados o son opcionales, tanto para reducir el costo de procesamiento como el tamaño de la cabecera.
- *Mayor flexibilidad para extensiones y nuevas opciones.* En IPv6 no existe un campo opciones. La gestión de opciones se realiza por un campo siguiente, cabecera (next header). Eliminando así las limitaciones de tamaño en la cabecera, e introduciendo una gran flexibilidad en el desarrollo de nuevas opciones.
- *Capacidades de control de flujo.* Se añaden capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o por servicios de tiempo real.
- *Capacidades de autenticación y privacidad de datos.* IPv6 provee extensiones para soportar autenticación, integridad y confidencialidad de datos.
- Permite la autoconfiguración de equipos.
- Facilita la computación móvil.
- Proporciona QoS.

En cuestión de seguridad IPv6 integra mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata de algo obligatorio y no añadido como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación, "Autenticación Header") y ESP (encriptación, "Encapsulation Security payload"), que permiten básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y se pueden de manera conjunto o por separado, con túneles o sin ellos. Se aplica en ruteadores, hosts y firewalls. Este tema esta descrito mediante las normas RFC2401, RFC2402, RFC2406, RFC2412 y RFC2451.

Por otro lado las únicas barreras que se pueden citar:
- El problema de multi-homing.
- La gente a favor del direccionamiento ajustable en longitud.
- El propio IPv4, de alguna forma, con los parches como NAT.
- La falta de soporte real por parte de fabricantes de routers y software "dominantes".
- La complejidad de la migración/transición.
- Los usuarios necesitan razones comerciales "FORZADAS" para migrar a IPv6.

5.2. Formato de celda

El formato general del datagrama de IPv4 es como se indica en la figura 5.1.

Encabezado del datagrama	Área de datos del datagrama

Fig. 5.1. Formato general del datagrama de IPv4

Aunque el espacio de direccionamiento de IPv6 es bastante más grande que en la versión 4, la cabecera es solamente dos veces la de dicha versión. En la figura 5.2 se muestra la cabecera de IPv4.

Bits: 4	8	16	32
Versión	Cabecera	TOS	Longitud Total
Identificación		Indicador	Desplazamiento de Fragmentación
TTL	Protocolo		Checksum
Dirección Fuente de 32 bits			
Dirección Destino de 32 bits			
Opciones			

Fig. 5.2. Cabecera de IPv4

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

A continuación se describe la nomenclatura de cada campo:

- Versión. Es la versión del protocolo (4 bits).
- Header. Cabecera (4 bits).
- TOS, Type of Service. Tipo de servicio (1 byte).
- Total Length. Longitud total (2 bytes).
- Identification. Identificación (2 bytes).
- Flag. Indicador (4 bits).
- Fragment Offset. Desplazamiento de fragmentación (12 bits – 1.5 bytes).
- TTL, Time To Live. Tiempo de vida (1 byte).
- Protocol. Protocolo (1 byte).
- Checksum. Código de verificación (2 bytes).
- Source Address. Dirección Origen de 32 bits (4 bytes).
- Destination Address. Dirección destino de 32 bits (4 bytes).

En la tabla 5.2 se ha marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el esquema 5.3.

Campo Modificado
Campo que desaparece

Fig. 5.3. Estado de campos para IPv6

En IPv6 cambia completamente el formato de datagrama. Como se muestra en la figura 5.4, un datagrama IPv6 tiene un *encabezado base* de tamaño fijo, seguido por ceros o más *encabezados de extensión*, seguidos a su vez por datos.

	opcional			
Encabezado base	**Extensión 1 de Encabezado**	. . .	**Extensión N de Encabezado**	**Datos**

Fig. 5.4. Formato general del datagrama de IPv6

Se ha paso de tener 12 campos a tan solo 8 para IPv6. El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4, se esta facilitando la misma información de varias formas. Un caso muy evidente es el Checksum o verificación de la integridad

de la cabecera: otros mecanismos de encapsulado ya realizan esta función (IEEE 802, MAC, framing PPP, capa de adaptación de ATM, etc.). El caso de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los ruteadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Es interesante que, aun cuando debe adaptarse a direcciones extensas, un encabezado base IPv6 contiene menos información que un encabezado de datagrama IPv4. Las opciones y algunos de los campos fijos que aparecen en un encabezado de datagrama de IPv4 se han cambiado por encabezados de extensión en el IPv6. En general, el cambio en los encabezados en los datagramas refleja los cambios en el protocolo. Algunos de los campos son renombrados:

- Type of service → Etiqueta de flujo (Flow Level).
- Longitud total → Longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65,536 bytes. Tiene una longitud de 16 bits (2 bytes).
- Protocolo → Siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los routers, sino tan solo de extremo a extremo. Tiene una longitud de 1 byte.
- Tiempo de vida → Límite de datos (Hop limit). Tiene una longitud de 1 byte.
- La alineación se ha cambiado de múltiplos de 32 bits a múltiplos de 64 bits.
- El tamaño de los campos de dirección origen y destino se ha incrementado en 16 octetos cada uno.
- La información de fragmentación se ha movido de los campos fijos en el encabezado base, hacia un encabezado de extensión.

En la figura 5.5 se muestra el contenido y el formato de un encabezado base de IPv6. Varios campos corresponden directamente a los campos de un encabezado IPv4.

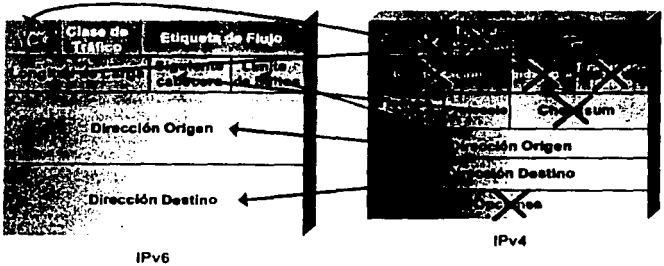


Fig. 5.5. Formato de gatagrama IPv6

A continuación se describe cada uno de los campos de este datagrama:

- *Versión.* Este campo ocupa 4 bits e indica la versión de IP. Para el formato descrito, la versión es numero 6.
- *Prioridad.* Este campo ocupa 4 bits e indica la prioridad que el remitente desea para los paquetes enviados, respecto a los demás paquetes enviados por el mismo. Los valores

de prioridad se dividen en dos rangos de 0 a 7 y de 8 a 15. Los primeros son para transmisiones capaces de reducir su velocidad en caso de un congestionamiento.
Los valores de 8 al 15 se usan para tráfico en tiempo real cuya tasa de envío es constante aún si se están perdiendo todos los paquetes mandados, por ejemplo video de alta calidad. Y el valor mas alto (15), cuando el remitente esta muy poco dispuesto a algún paquete sea descartado, por ejemplo audio de baja calidad. Dentro de cada grupo, los paquetes de número más bajo son menos importantes que los paquetes de número alto.

- *Flow label.* Este campo ocupa 24 bits, es usado por el remitente para indicar que sus paquetes sean tratados de forma especial por los routers, como en servicios de alta calidad o en tiempo real. En este punto, se entiende el flujo como un conjunto de paquetes que requieren un tratamiento especial. Todos los paquetes pertenecientes al mismo flujo deben tener valores similares en los campos dirección origen, destino, prioridad y etiqueta de flujo.
- *Longitud de carga (payload).* Este campo ocupa 16 bits, indicando el resto del paquete que sigue a la cabecera. La máxima longitud de carga útil que puede tenerse es de 64 Kbytes. Cuando se necesite que esta longitud sea mayor, se incluye un valor de cero en este campo y con ello se agrega una extensión del encabezado con el campo Jumbo Payload que permite realizar transferencia de datos con longitudes mayores en los paquetes.
- *Siguiente encabezado.* Este campo ocupa 8 bits e identifica el tipo de cabecera que sigue a la cabecera IPv6 y se representa mediante valores decimales en la tabla 5.6.

Valor decimal	Siglas	Descripción
0		Reservado (IPv4)
1	HBH	Opción Salto por salto (IPv6)
2	ICMP	Protocolo Internet de Mensajes de Control (IPv4)
3	GGP	Protocolo Gateway a Gateway
4	IP	IP en IP (encapsulación IPv4)
5	ST	Trama
6	TCP	Protocolo de Control de Transmisión
8	EGP	Protocolo de Gateway a Exterior
17	UDP	Protocolo de Datagrama de Usuario
43	RH	Encabezado de ruteo (IPv6)
44	FH	Encabezado de fragmentación (IPv6)
46	RSVP	Protocolo de Reservación
51	AH	Encabezado de autenticación
58	CMP	Protocolo Internet de Mensajes de Control (IPv6)
59	Null	Sin encabezado siguiente (IPv6)
60	DOH	Encabezado de Opciones Destino (IPv6)

Tabla. 5.6. Valores para el campo Siguiente Cabecera

- *Limite de saltos.* Ocupa un octeto. Tiene un valor numérico que puede ser como máximo 255. Es decrementado en una unidad por cada nodo que redirige el paquete hacia su destino. El paquete es descartado si el valor del campo llega a cero.
- *Dirección origen y destino.* Cada uno ocupa 128 bits y deben incluir las direcciones de los puntos extremos para la entrega de paquetes.

5.3. Fragmentación

Como en IPv4, IPv6 prepara el destino final para realizar el reensamblaje de datagramas. Sin embargo, los diseñadores tomaron una decisión poco usual respecto a la fragmentación. Recordemos que IPv4 requiere un ruteador intermedio para fragmentar cualquier

datagrama que sea demasiado largo para el MTU (Maximum Transmisión Unit) de la red en el que viaja. En IPv6, la fragmentación está restringida a la fuente original. Antes de enviar tráfico de información, un origen debe realizar una técnica de *Path MTU Discovery (descubrir el MTU de la ruta)* para identificar el MTU mínima a lo largo de la trayectoria hasta el destino. Antes de enviar un datagrama, el origen fragmenta el datagrama de manera que cada fragmento sea menor que el Path MTU. Así la fragmentación es de extremo a extremo; no son necesarias fragmentaciones adicionales en ruteadores intermedios.

Para cada paquete que deba ser fragmentado, el origen le asigna un identificador, este identificador debe ser diferente de cualquier otro paquete enviado recientemente con las mismas direcciones origen y destino.

El paquete original se diferencia en dos partes, fragmentable y no fragmentable. La parte no fragmentable consiste en la cabecera IPv6 y las cabeceras extendidas que deban ser procesadas por los nodos intermedios en el camino del paquete. La parte fragmentable consta del resto de cabeceras extendidas, de la cabecera del nivel superior y de la carga.

El paquete original se descompone en fragmentos cuya longitud debe estar alineada a 8 octetos (excepto el último). La parte no fragmentable del paquete original se copia a todos sus fragmentos, cambiando el campo longitud de la carga a la longitud de cada fragmento y el campo siguiente cabecera a 44 (valor que identifica a una cabecera de fragmento).

Cada cabecera de fragmento esta descompuesta por:

- La parte no fragmentable del paquete original.
- La cabecera del fragmento.
- El fragmento propiamente dicho.

En destino, el paquete original es construido según las siguientes normas:

- Los fragmentos del paquete original deben contener los mismos valores en los campos Dirección Origen, Dirección Destino e Identificador del paquete.
- El campo siguiente cabecera, de la cabecera IPv6 se obtiene del campo: siguiente cabecera de fragmento del primer fragmento.
- El campo tamaño de la carga del datagrama original se calcula en base al tamaño de la parte no fragmentable y al tamaño y offset del fragmento del último fragmento.

En el proceso de reensamblado, pueden producirse los siguientes errores:

- Si se ha recibido un número de fragmentos insuficientes para recomponer el paquete original pasados 60 segundos desde el primer fragmento recibido, se abandona el proceso y se descartan todos los fragmentos recibidos. Si se recibió el primer fragmento (offset de fragmento=0), se envía un mensaje ICMP de error al origen.
- Si la longitud de un fragmento en octetos no es múltiplo de 8 y no es el último fragmento, se descarta el fragmento y se envía un mensaje de ICMP de error al origen.
- Si la longitud y el offset de fragmento de un fragmento determinan que la longitud de la carga del paquete original es mayor de 65535 octetos, se descarta el fragmento y se envía un mensaje de ICMP de error.

5.4. Direccionamiento

Para IPv4, cuando se comunican a los usuarios, ya sea en documentos técnicos o a través de programas de aplicación, las direcciones IP se escriben como cuatro enteros decimales separados por puntos, en donde cada entero proporciona el valor de un octeto de la dirección IP. Por lo tanto, la dirección de 32 bits es:

10000000 00001010 00000010 00011110

se escribe

128.10.2.30

De hecho, la mayor parte del software TCP/IP que muestra una dirección IP o que requiere que una persona la introduzca, utiliza notación decimal con puntos. En la tabla 5.7 se resumen el rango de valores para cada clase.

Clase	Dirección más baja	Dirección más alta
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tabla. 5.7. Clases de direcciones IPv4

Con IPv6 se resuelve el problema de tener una capacidad insuficiente, el gran tamaño de direcciones plantea un problema nuevo: los usuarios que manejan redes deben leer, introducir y manipular estas direcciones. Obviamente, la notación binaria no es práctica. Sin embargo, la notación decimal con puntos utilizada por el IPv4 tampoco hace las direcciones lo suficientemente compactas. Para entender porqué, consideremos el ejemplo de un número de 128 bits expresado en notación decimal con puntos:

104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255

Para ayudar a hacer la dirección ligeramente más compacta y fácil de introducir, los diseñadores del IPv6 proponen utilizar una notación hexadecimal con dos puntos (abreviado *colon hex*) en la cual el valor de cada cantidad o bloque de 16 bits de la dirección se representa en hexadecimal separado por dos puntos. Existen tres formas para representar direcciones IPv6 mediante cadenas de texto:

1. Por ejemplo, cuando el valor mostrado arriba en notación decimal se traduce a la notación hexadecimal con dos puntos e impresa (con la estructura x:x:x:x:x:x:x:x), utilizando el mismo espaciado, se convierte en:

   68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF

2. La notación con dos puntos tiene la ventaja obvia de requerir menos dígitos y menos caracteres separadores que la notación decimal con puntos. Además, la notación hexadecimal con dos puntos incluye dos técnicas que la hacen muy útil. En la primera, la notación hexadecimal con dos puntos permite la *compresión a 0* mediante la cual una cadena de ceros repetidos se reemplaza por un par de dos puntos. Por ejemplo la dirección:

   FF05:0:0:0:0:0:0:B3

   Puede escribirse:

   FF05::B3

   Para asegurar que la compresión cero produce una interpretación sin ambigüedades, la propuesta especifica que puede aplicarse sólo una vez en cualquier dirección. La compresión cero es especialmente útil cuando se emplea el esquema de asignación de direcciones propuesto ya que muchas direcciones contendrán cadenas contiguas de ceros
3. La segunda técnica, la notación hexadecimal con dos puntos incorpora sufijos decimales con punto; esta combinación tiene como propósito de utilizarse durante la transición de IPv4 a IPv6. por ejmeplo, la siguiente cadena es una notación hexadecimal con dos puntos válida:

0:0:0:0:0:0:128.10.2.1 y,
0:0:0:0:HF:129.144.52.38

Aún cuando los numeros están separados por dos puntos, cada uno especifica el valor de una cantidad de 16 bits, los números en la porción decimal con puntos especifican el valor de un octeto. Por supuesto, la compresión a cero puede utilizarse con el número de arriba para producir una cadena hexadecimal con dos puntos equivalente que se vería muy similar a una dirección IPv4:

::128.10.2.1 y,
::HF:129.144.52.38

Por otra parte, como ya hemos mencionado las direcciones son identificadores de 128 bits para un dispositivo o un conjunto de ellos. Como en IPv4, IPv6 asocia una dirección con una conexión de red específica, no con una computadora específica. Así, la asignación de direcciones es similar para IPv4: un ruteador IPv6 tiene dos o más direcciones y un dispositivo IPv6, con una conexión de red, necesita sólo una dirección. En IPv6 también conserva la jerarquía de direcciones de IPv4 en la que una red física es asignada a un prefijo. Sin embargo, para hacer la asignación de direcciones y la modificación es más fácil, IPv6 permite que varios prefijos sean asignados a una red dada y que una computadora tenga varias direcciones simultáneas asignadas hacia una interfaz determinada.

Además de permitir varias direcciones simultáneas por conexión de red, el IPv6 expande y en algunos casos, unifica las direcciones especiales de IPv4. En general, una dirección de destino en un datagrama cae dentro de una de tres categorías:

- *Unicast.* Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales. El datagrama deberá rutearse hacia el destino a lo largo de la trayectoria más corta.
- *Anycast.* Identificador para un conjunto de interfaces en el que todas comparten un solo prefijo de dirección (por ejemplo, si están conectadas a la misma red física). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de ruteo).
- *Multicast.* Identificador para un conjunto de inetrfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. Se emplea para aplicaciones de retranmisión múltiple.

Existen algunas diferencias importantes en el direccionamiento de IPv6 respecto de IPv4:

- No hay direcciones broadcast (su función es sustituida por las direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominados "prefijo" a la parte de la dirección hasta el nombre indicado (incluyéndolo).
- Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de encaminamiento.
- Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo puede ser empleado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast).

- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de Internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

5.4.1. Direcciones unicast locales

Las direcciones unicast son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura como se indica en la figura 5.8.

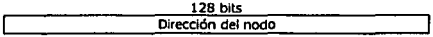


Fig. 5.8. Dirección completa de IPv6

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que esta conectado, de manera general (figura 5.9).

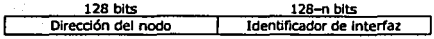


Fig. 5.9. Identificación de prefijos en dirección IPv6

Dispositivos específicos pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El "identificador de interfaz" se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace

Se han definido dos tipos de direcciones unicast de uso local: Local de Enlace (Link-Local) y Local de Sitio (Site-Local).

Las direcciones locales de enlace han sido direccionadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario o situaciones en las que no hay routers. Por tanto, los routers no permiten retransmitir ningún paquete con direcciones de origen o destino que no sean locales de enlace (su ámbito está limitado a la red local). Tienen el formato de la figura 5.10.

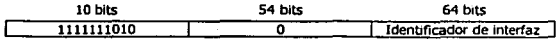


Fig. 5.10. Direcciones locales IPv6

Se trata de direcciones:

FE80::<ID de interfaz>/10

Las direcciones locales de sitio (figura 5.11) permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo local. Se configuran mediante un identificador de subred de 16 bits. Los routers no deben retransmitir *fuera del sitio* ningún paquete cuya dirección fuente o destino sea "local de sitio" (su ámbito esta limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111010	0	ID de subred	Identificador de interfaz

Fig. 5.11. Direcciones locales de sitio IPv6

Se trata de direcciones,

FEC0::<ID de subred>:<ID de interfaz>/10

5.4.1.1. Direcciones Aggregatable Global Unicast

Las direcciones aggregatable global unicast son identificadas por el prefijo de formato (FP) 001, equivalen a las direcciones IPv4 públicas y son globalmente ruteables.

El concepto de direccionamiento "aggregatable" es indispensable para una mejor organización jerárquica de del ruteo en las redes globales. Este formato de direcciones esta diseñado para soportar el tipo de "agregation" que se utiliza hoy en día, *provider-based* (basados en proveedores). Y un nuevo tipo de agregación *exchange-based* (basado en intercambios). La combinación de ambos permite un ruteo mas eficiente.

En este tipo de direcciones, los 64 bits mas altos identifican la red, y los mas bajos el nodo.

Existen tres tipos de direcciones aggregatable global unicast:

- De prueba 6Bone: comienzan con 3ffe.
- 6to4: comienzan con 2002.
- Asignadas por un proveedor: comienzan con 2001.

Están organizados en tres niveles de jerarquía:

- Topología pública (Public Topology). Es el conjunto de proveedores e intercambios que proveen servicios públicos de tránsito Internet.
- Topología de sitio (Site Topology). Es local a un sitio específico u organización que no provee servicio público a nodos fuera del sitio.
- Identificador de Interfaz (*Interface identifier*). Un número único, al menos en el segmento local de la LAN; de 64 bits usualmente generado automáticamente, identifica las interfaces en los enlaces.

En la figura 5.12 se muestra el formato de las direcciones Aggregatable Global Unicast.

3	13	8	24	16	64
FP	TLA ID	RES	NLA ID	SLA ID	ID de interfaz

Topología Pública — Topología de Sitio — Identificador de interfaz

Fig. 5.12. Formato de direcciones Aggregatable Global Unicast

PREFIJO DE FORMATO (FP FORMAT PREFIX): se utiliza para identificar direcciones aggregatable global unicast, su valor es 001.

TOP-LEVEL AGREGATION IDENTIFIER (TLA ID): se encuentra en el nivel superior de la jerarquía de ruteo. Los routers situados en este nivel tienen en la tabla de ruteo una entrada para cada TLA ID activo y probablemente tendrán entradas adicionales que proveerán información de ruteo del TLA ID en el cual se encuentren.

Podrían tener otras entradas, para optimizar el ruteo, dependiendo de su topología, pero siempre minimizar el número de entradas adicionales de la tabla de ruteo.

Este formato de direccionamiento soporta 8,192 (2^{13}) identificadores TLA. Pudiéndose incrementar este número, aumentando el número de bits del campo reservado o usando este formato para prefijos de formato adicionales.

Al día de hoy hay dos tipos de prefijos TLA:

- El de 6bone, cuyos primeros 16 bits son 3ffe::/16. aquí los top-level aggregators son llamados pseudo-TLA o pTLA, los cuales son asignados a través de un proceso definido por la comunidad 6bone.
- El de asignación de producción temprana cuyos primeros 16 bits son 2001::/16. Aquí los top level aggregators son llamados sub-TLA, los cuales son asignados a través del Internacional Regional Internet Registry (RIR) Process.

RESERVADO (RES): este campo se reserva para uso futuro y debe ser cero. Este campo permite un crecimiento futuro de los campos TLA ID y NLA ID.

IDENTIFICADOR DE NEXT-LEVEL AGREGATION IDENTIFIER (NLA): es usado por organizaciones a las que se les asignó un TLA, para crear una estructura jerárquica de direccionamiento, acorde con su propia red, y para identificar los sitios u organizaciones que dependen de ella.

Cada organización puede manejar el NLA que le fue asignado, de forma que, reserve una porción para un nuevo NLA1 (figura 5.13) y crear así una jerarquía de direccionamiento a su red. El resto de los bits se utilizan para los sitios a los cuales desea dar servicio. Esto se muestra en el siguiente esquema.

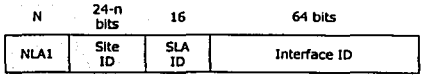


Fig. 5.13. Jerarquía de direccionamiento empleando NLA

Las organizaciones a las que se les asigna un TLA ID reciben 24 bits para uso del NLA ID. Permitiendo a cada organización proveer servicio a tantas organizaciones como el número total de direcciones como el número total de direcciones IPv4 soportadas actualmente.

Las organizaciones que tienen asigando TLA ID pueden soportar varios NLA ID en su propio espacio de Site ID. Asimismo, las organizaciones que reciben un NLA ID pueden usar su SITE ID para soportar otros NLA's ID. Esto se demuestra en el esquema 5.14.

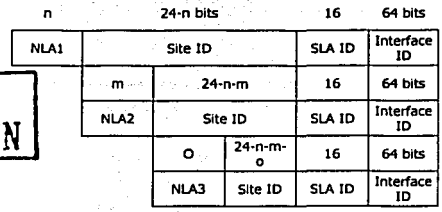


Fig. 5.14. Manejo de Site ID para soportar múltiples NLA ID's

El diseño del espacio del NLA ID para un TLA específico, es dejado a la organización responsable de ese TLA ID. Mientras que el diseño del siguiente NLA ID es responsabilidad del NLA ID del nivel previo.

IDENTIFICADOR DE SITE-LEVEL AGREGATION IDENTIFIER (SLA): es usado por organizaciones finales para crear su propia jerarquía local de direccionamiento e identificar subredes. Es análogo al concepto de subred de IPv4 excepto que cada organización tiene un número mayor de subredes. Este campo soporta 65,355 subredes individuales.

La forma en que se maneje el campo SLA ID es responsabilidad de cada organización. El número de subredes soportadas en este formato de direccionamiento debería ser suficiente, salvo para organizaciones muy grandes. Las organizaciones que necesiten subredes adicionales podrán solicitar otros identificadores SLA. El formato es como se indica en la figura 5.15.

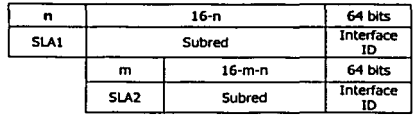


Fig. 5.15. Formato del campo SLA

IDENTIFICADOR DE INTERFASE (INTERFACE ID): Los identificadores de interfaz son empleados para identificar interfaces en un enlace. Se requiere que sean únicos para un enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz (MAC). El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se requiere que tengan una longitud de 64 bits y ser construido en el formato IEEE EUI-64 (EUI-64). Estos identificadores pueden tener un rango global cuando un token global (dirección MAC de 48 bits de IEEE) se encuentre disponible o tenga un rango local cuando un token global no se encuentre disponible (enlaces, puntos finales de un túnel). El bit "u" (bit universal/local en la terminología EUI-64 de IEEE), en el identificador EUI-64 debe ser configurado correctamente para especificar un ámbito global o local.

5.4.2. Direcciones anycast (RFC2526)

Las direcciones anycast tienen el mismo rango de direcciones que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero (figura 5.16).

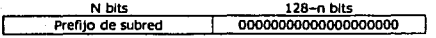


Fig. 5.16. Dirección anycast del router de la subred

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del router de la subred", serán enviados a un router de la subred.

Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz estan reservados para su asignación como direcciones anycast de la subred.

La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/local" igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen como en la figura 5.17.

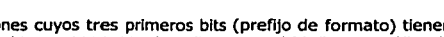


Fig. 5.17. Construcción de dirección anycast del router de la subred

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según la figura 5.18.

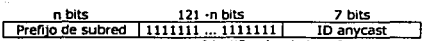


Fig. 5.18. Dirección anycast del router de la subred de longitud diferente

5.4.3. Direcciones multicast (RFC2375)

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast. Las direcciones multicast tienen formato de la figura 5.19.

8 bits	4 bits	4 bits	112 bits
11111111	000T	ámbito	Identificador de Grupo

Fig. 5.19. Formato dirección multicast

El bit T indica, si su valor es cero, es una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits ámbito tienen significados de la tabla 5.20.

0	Reservado
1	Ámbito local de nodo
2	Ámbito local de enlace
3	No asignado
4	No asignado
5	Ámbito local de sitio
6	No asignado
7	No asignado
8	Ámbito local de organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito global
F	Reservado

Tabla 5.20. Bits ámbito

El "Identificador de Grupo", identifica como cabe esperar, el grupo de multicast concreto al que se refiere, bien sea permanente o temporal, dentro de un determinado ámbito.

5.4.4. Formato para la representación en URL's (RFC2732)

Cuando se ocupa algun explrador de Internet se emplean URLs, en muchas ocasiones sin conocer el significado de esta abreviatura.

La especificación original (RFC2396), que data del año 1988, nos dice que Uniform Resource Locator (Localizador de Recurso Uniforme), es un medio simple para identificar un recurso a través de su localización en la red.

De la misma forma que se usa direcciones en formato IPv4 para describir un URL, se han descrito normas para realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.

El motivo por el que ha sido preciso realizar esta definición es simple. Con la anterior especificación no estaba permitido emplear el carácter ":" en una dirección, sino como separador de puerto. Por tanto, si sea facilitar operaciones tipo "cortar" y "pegar", para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de las direcciones IPv6.

La solución es sencilla: el empleo de los corchetes ("[","]) para encerrar la dirección IPv6, dentro de la estructura habitual del URL. Algunos ejemplos son como sigue:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417A
- ::192.9.5.5
- ::FFFF:129.144.52.38
- 2010:836B:4179::836B4179

Serían representadas como:

- http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
- http://[1080:0:0:0:8:800:200C:4171]/index.html
- http://[3ffe:2a00:100:7031::1]
- http://[1080::8:800:200C:417A]/foo
- http://[::192.9.5.5]/ipng
- http://[::FFFF:129.144.52.38]:80/index.html
- http://[2010:836B:4179::836B4179]

5.5. Autoconfiguración (RFC 2462)

La autoconfiguración es el conjunto de pasos por las cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play".

El proceso incluye la creación de una dirección de enlace local, verificación de que no sea duplicada en dicho enlace y determinación de la información que ha de ser configurada (direcciones y otra información)

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración "stateless", no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un "identificador de interfaz", que identifica de forma única la interfaz en la subred. La dirección se compone por la composición de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración stateful, el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

Ambos tipos de configuración (stateless y stateful), se complementan. Un host puede usar autoconfiguración stateless, para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración stateless se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan solo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de la red.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que aprobar el algoritmo de detección de direcciones duplicadas.

5.6. IPv6 sobre Ethernet (RFC2464)

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, etc.), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full duplex basadas ISO/IEC8802-3).

Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet (figura 5.21). La cabecera Ethernet contiene las direcciones origen y destino Ethernet, y el código de tipo Ethernet.

El campo de datos contiene la cabecera IPv6 seguida por los propios octetos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

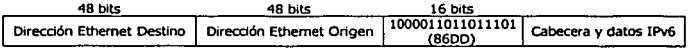


Fig. 5.21. Trama Ethernet normalizada

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, se basa en la dirección MAC de 48 bits (IEEE 802). Se toman los tres primeros bytes (los de mayor orden), y se les agrega "FFFE" (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo de EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte EUI-64 (el 2° bit por la derecha, el 2° bit de menor peso). Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz (figura 5.22), pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

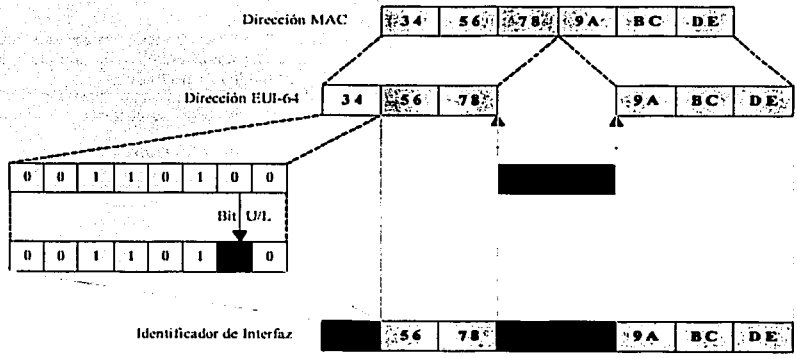


Fig. 5.22. Construcción de dirección IPv6 para interfaz

5.7. Estrategias de transición

Uno de los caminos de transición es el uso simultáneo de ambos protocolos. Los dispositivos con ambos protocolos también se denominan "nodos IPv6/IPv4". De esta forma, el dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que solo soportan uno de los dos protocolos.

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión). El DNS podrá resolver la dirección IPv4, la dirección IPv6 o ambas.

Se puede emplear la dirección IPv4, anteponiendo 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 "mapeada desde IPv4".

5.7.1. Túneles IPv6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete(s) IPv6 en IPv4. La figura 5.23 muestra el paquete de encapsulación.

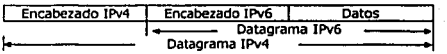


Fig. 5.23. Paquete IPv6 encapsulado en IPv4

Estos túneles pueden ser utilizados de formas diferentes:

- Router a router. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
- Host a router. Hosts con doble pila se conectan a router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
- Host a host. Hosts con doble pila interconectados por una infraestructura IPv4. el túnel comprende la ruta completa que siguen los paquetes.
- Router a host. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la pila.

Los túneles se clasifican según el mecanismo por el que el nodo realiza el encapsulado:

- *Túneles configurados.* En los dos primeros casos (router a router y host a router), el paquete es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Se llama configurado porque la dirección del nodo destino se configura manualmente y desde el nodo que se encarga de encapsular; solo se emplea en conexiones punto a punto.
- *Túneles automáticos.* En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv6 está contenida en la dirección IPv4. El "desencapsulado", en el extremo final del túnel, realiza la función opuesta. En la figura 5.24 se muestra este túnel.

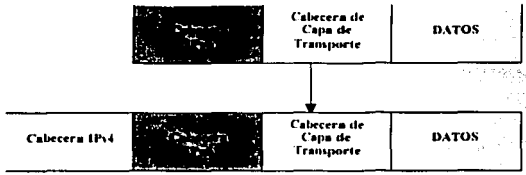


Fig. 5.24. Túnel automático

5.7.2. Conexión de dominios IPv6 sobre redes IPv4

Es un mecanismo comúnmente denominado 6to4, para asignar un prefijo de dirección IPv6 de cualquier sitio que tenga al menos una dirección IPv4 pública. De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP's.

5.7.3. "Tunnel Server" y "Tunnel Broker"

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y DNS permanentes.

La diferencia con el mecanismo 6to4 es que el "Tunnel Broker" no requiere la configuración de un router.

Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que cuentan con conectividad IPv4.

El "Tunnel Broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" administra (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El "Tunnel Server" es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo ordenes del "broker" crea, modifica o borra los servicios asociados a un determinado tunel/usuario.

El mecanismo para su con figuración es tan sencillo como indicar, en un formulario Web, datos relativos al Sistema Operativo, la dirección IPv4, un "apodo" para máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

CAPÍTULO 6
Administración y mantenimiento de redes

6.1 Administración de redes

6.1.1. Conceptos

Sistema de Administración de red:

Un sistema de administración de red es un conjunto de herramientas (software y hardware) que proporcionan monitoreo y control sobre un red. Su función principal es auxiliar al administrador de red a resolver cualquier tipo de problema que se le presente, para dar una solución rápida de una manera ordenada y secuencial.

La plataforma más utilizada para implementar un sistema de administración de red, son las estaciones de trabajo corriendo UNIX, LINUX, Windows NT Server, Windows 2000 Server o Windows 2003 Server como sistema operativo con una interfaz gráfica de ventanas.

Un sistema de administración de red debe tener las siguientes características:

- Una interfaz gráfica que pueda producir una estructura jerárquica de la red y permitir conexiones lógicas entre los diferentes niveles de la jerarquía, esto puede lograrse con un mapa que plasme la topología actual de la red (p.e. What's up Gold).
- La interfaz deberá contar con un conjunto de comandos amigables, pero poderosos para realizar las tareas de administración de red.
- El sistema deberá proveer una base de datos confiable que pueda almacenar y poner a disposición cualquier información requerida.
- El sistema deberá ser fácil de construir y expandir. Es decir deberá ser adaptable a cualquier tipo de red que se tenga, e igualmente si la red tiene o no la misma plataforma operativa, además de facilitar la adición de aplicaciones y desarrollos requeridos por el administrador.
- Un mínimo de equipo adicional, es decir la mayoría del equipo tanto en hardware y software requerido por el sistema de administración deberá ser encontrado en el equipo existente.
- El sistema deberá ser capaz de manejar protocolos de administración actuales.
- El sistema deberá contar con herramientas de análisis de datos y graficación de los mismos.

6.1.2. Áreas a cubrir en un sistema de administración

La Organización Internacional de Estandarizaciones (OSI) ha decretado las áreas que un sistema de administración debe cubrir.

6.1.2.1. Administración de acceso

Es el seguimiento de la utilización de los recursos de red por los usuarios. Este tipo de administración es totalmente necesaria ya que con ello el administrador puede observar:

- Del abuso de los privilegios en los accesos a usuarios.
- El uso ineficiente de la red.

- Asegurarse que el usuario este obteniendo exactamente los recursos necesarios.
- Planear un crecimiento en base a un conocimiento preciso de la actividad de los usuarios (procesamiento, uso de periféricos, espacio de almacenamiento, por mencionar algunos.)

6.1.2.2. Administración de desempeño

El proceso de medición del desempeño de los dispositivos que conforman a una red. Los factores que reflejan el desempeño pueden ser:

- Porcentaje de utilización
- Capacidad disponible
- Tiempo de respuesta
- Tráfico
- Cantidad de errores

Los administradores emplean esta información para planear crecimientos de la red, cambios de la misma o bien para mantener o incrementar su funcionalidad.

6.1.2.3. Administración de fallas

El objetivo es determinar lo más rápido posible el punto de la red donde se presenta una falla para que ésta se corrija lo antes posible. El proceso de localización de un problema o falla en la red, envuelve los siguientes pasos:

a. Determinar exactamente donde esta la falla
b. Separar el sitio donde esta ocurriendo la falla del resto de la red, para que pueda seguir funcionando sin interferencia.
c. Determinar la causa o causas de la falla
d. Reparar el problema si es posible.

También se logra detectar problemas que puedan generar posteriormente una falla. Los usuarios esperan una solución rápida y real de cualquier problema que se presente en la red. Si una falla ocurre, los usuarios desean ser notificados y que la falla sea corregida inmediatamente. Para tener este nivel de respuesta a fallas en la red, se requiere una muy rápida y confiable detección de fallas provistas por el sistema de administración.

6.1.2.4. Administración de configuración

Es el proceso de configurar a los elementos de la red, desde una terminal remota. La administración de configuración involucra los procesos de inicialización, mantenimiento y cuando deja de funcionar algún dispositivo de la red sea lógicos (contadores de retransmisión del protocolo de transporte) o físicos (servidores, dispositivos de interconexiones) y estados de los mismos.

6.1.2.5. Administración de seguridad

Es el proceso de monitoreo y control sobre los accesos a la información dentro de la red. Alguna información almacenada en ciertas computadoras no puede ser vista por todos los usuarios, esta llamada es la información confidencial o crucial. Se debe ser cuidadoso con ella y mantener un constante control sobre los accesos a la misma y determinar cuales fueron válidos.

Los archivos log son una herramienta muy útil para realizar esta tarea.

6.1.3. Arquitectura de un sistema de administración de red

6.1.3.1. Tipos de arquitectura

Existen tres posibles arquitecturas para construir un sistema de administración de red:

Arquitectura centralizada. Significa tener una sola maquina en toda la red que se encargue de correr las aplicaciones del sistema y allí se almacenen también los datos que requieran estas aplicaciones.

Arquitectura distribuida. Llamada así ya que se tienen varios sistemas de administración corriendo simultáneamente en varias máquinas distribuidas a través de la red. Bajo esta arquitectura cada sistema puede administrar por ejemplo una parte especifica de la red llamada región, tal es el caso de una subred, un edificio o un conjunto de ellos.

Arquitectura mixta. Esta arquitectura combina las dos anteriores (centralizada y distribuida) en una arquitectura jerárquica. En este tipo existirá un sistema principal que almacenará toda la información esencial de la red y a su vez se delegarán tareas de administración especificas a otros sistemas en al red.

6.1.3.2. Elementos de un sistema de administración de red

Llamaremos a cada elemento de una red administrada nodo. Habrá nodos que estén capacitados para administrar, es decir ejecutar tareas que lleven a detectar fallas, medir desempeño, observar el acceso a recursos, por mencionar algunos. Estos nodos son llamados nodos administradores. También existirán nodos que estén capacitados para ser administrados, éstos reciben el nombre se nodos administrados.

Los nodos administrados y administradores son los elementos primarios de un sistema de administración. Dentro de cada uno de estos nodos se encuentran otros elementos del sistema que permiten que la interacción entre los elementos primarios se lleve a cabo.

En el siguiente esquema se muestra a un nodo administrador y uno administrado, dentro de ambos se pueden apreciar los elementos citados en el párrafo anterior. Ambos nodos contienen un elemento llamado agente.

Un agente es una colección de software dedicado a las tareas de administración. Los nodos administradores requieren de un elemento llamado: software de administración de red (SAR).

Cada agente realiza las siguientes tareas:

- Obtiene información sobre el estado y actividades del nodo en que reside.
- Almacena localmente los datos recopilados
- Responde a las peticiones que un nodo administrador le envía como:
    - Cambiar un parámetro en el nodo
    - Transferir datos del estado y de las actividades del nodo.

Los agentes se encuentran presentes en diversos nodos de la red como son PC´s, Estaciones de trabajo, concentradores, puentes, switches, enrutadores, por mencionar algunos.

El software de administración de red, permite realizar las tareas de administración sobre los nodos administrados y administradores, incluyendo el nodo en el que reside.

Además de los agentes y el SAR, todos los nodos y dispositivos de interconexión pueden contar con sistema operativo (SO), software de aplicación (Apl) y software de comunicación (Com).

6.1.3.3. Arquitectura del software de administración de red (SAR)

El software de un sistema de administración de red, generalmente se divide en tres categorías:

Software de aplicación

La interacción entre un usuario y el software de administración de red es provista por el software de presentación que es una interfase gráfica. Dicha interfase es necesaria en cualquier sistema de administración con el fin de permitir al usuario administrar y controlar la red, por una vía sencilla que le provea de comandos para ejecutar acciones de administración y analizar los datos que estas acciones generen. La llave para lograr un efectivo sistema de administración de red es una interfase unificada, es decir, la interfase deberá ser capaz de concentrar a todos los dispositivos de la red en un mapa o esquema que represente su topología, esto permitirá al usuario tener una administración heterogénea de su red.

Software de tareas de administración

En general el software que realiza las tareas de administración de red organizado en tres capas.

En la capa más alta encontramos una colección de aplicaciones que se encargan de las tareas de administración sobre las diferentes áreas (fallas de acceso, configuración, desempeño y seguridad).

En el nivel medio encontramos módulos que implementan funciones primitivas y de propósito general, como son: la generación de alarmas o resúmenes de datos, éstas funciones son utilizadas por las tres capas.

En el nivel más bajo es donde se encuentra el servicio de transporte de datos, este servicio lo constituye un protocolo de administración de red, usado para intercambiar información de administración entre nodos administradores y agentes.

Software de soporte de administración de red

Para realizar sus funciones, el software que realiza las tareas de administración de red necesita tener acceso a una base de información de administración local conocida como MIB (Management Information Base).

El MIB local de cada agente contiene información que refleja la configuración, el comportamiento del nodo en que reside y parámetros que pueden ser usados para controlar la operación del mismo.

El manejo del MIB es ejercido por cada agente, el cual puede extraer información de la MIB y ponerla a disposición. Toda la información contenida en una MIB es conocida como información administrativa.

6.3.3.4. Proxy

Hasta este momento hemos considerado que cada elemento dentro de una red tiene un agente y todos se comunican con el mismo protocolo de administración.

Esto no es siempre posible en la realidad ya que en una red que será administrada no puede contar entre sus elementos equipos muy viejos que no soportan los estándares de administración que se desean usar o bien componentes como modems y multiplexores que no soportan software adicional.Para manejar estos casos es común tener un agente sirviendo como Proxy o delegado.

Cuando un agente desempeña un rol de delegado, éste actúa como mediador entre un nodo y el nodo administrador. Si se cuenta en la red con elementos que no sean capaces de comunicarse con el mismo estándar de administración, es necesario utilizar un delegado.

El nodo administrador enviará su petición sea de información o de control a un delegado, para que éste la transfiera en forma apropiada al elemento deseado. Cuando la petición es resuelta, el elemento deberá transmitir su respuesta en el mismo camino en que la petición llego.

El monitoreo de red es una acción de lectura, cuya función es obtener información acerca del estado y comportamiento de los elementos de la red. Abarca las tres primeras áreas funcionales de administración de red (fallas, desempeño y acceso). El control de red es una acción de escritura, cuya función es alterar los parámetros de los componentes de la red para realizar funciones específicas. Este comprende las dos últimas funciones de administración que son: configuración y seguridad.

6.2. Protocolos de administración y seguridad en redes

6.2.1. Normas para la administración de la red

El Comité Asesor de Internet (Internet Advisory Board, IAB) ha elaborado o adoptado varias normas para la administración de la red. En su mayoría, éstas se han diseñado específicamente para ajustarse a los requerimientos del TCP/IP, aunque, cuando es posible, cumplen con la arquitectura OSI. Un grupo de trabajo Internet, responsable de las normas para la administración de la red, adoptó un enfoque de dos pasos para cubrir las necesidades actuales y futuras.

El primer paso comprende el uso del Protocolo Simple para Administración de la Red (Simple Network Management Protocol, SNMP), el cual fue diseñado y aplicado por el grupo de trabajo. SNMP se utiliza actualmente en muchas redes Internet, y está integrado dentro de muchos de los, productos comerciales que están disponibles. Conforme se ha mejorado la tecnología, SNMP ha evolucionado y se ha vuelto más completo.

El segundo paso comprende las normas OSI para administración de la red, llamados Servicios Comunes de Información sobre la Administración (Common Management Information Services, CMIS), y al Protocolo Común de Información sobre la Administración (Common Management Information Protocol, CMIP), los cuales se utilizarán en las futuras aplicaciones de TCP/IP

IAB ha publicado Common Management Information Services and protocol over TCP/IP(CMOT) como una norma para TCP/IP y para la administración OSI.

Tanto SNMP como CMOT utilizan el concepto de los administradores de red que intercambian información con los procesos que se encuentran dentro de los dispositivos de la red, como las estaciones de trabajo, los puentes, los rutadores y los multiplexores.

La arquitectura tanto de SNMP como de CMOT es tal, que la información recopilada se almacena de una forma que permita a otros protocolos leerla.

6.2.2. Protocolos de Administración

Los administradores de red necesitan un método consistente para obtener información de todos los componentes de su red. Muchas veces los administradores se basan en las herramientas genéricas de sus sistemas (ping, arp, ipconfig, disk, printer) para realizar tareas de monitoreo y en base en al información obtenida realizar acciones de control sobre la red.

Estas herramientas son generalmente fáciles de usar y no necesitan implementaciones anexas para su funcionamiento, generalmente están integradas a los sistemas operativos. Sin embargo estas herramientas no fueron diseñadas propiamente para la administración de una red, generalmente basan sus funciones en un intercambio de paquetes a nivel capa de red y no pueden manejar la cantidad adecuada de información para proporcionar una información administrativa confiable.

Para conseguir la información que necesitan los elementos de la red, utilizan la técnica de polling y no son capaces de generar reportes de eventos por si mismos, además de no proveer abundante información acerca de los sucesos que están ocurriendo en la red, esta información en muchos casos no es suficiente para tomar las decisiones más acertadas para la administración de la red. Por esta razón surgió la necesidad de desarrollar tecnologías específicas para la administración de red y es así como se originan los protocolos de administración de red.

Los protocolos de administración de red son una colección de especificaciones de comunicación capaces de manipular información administrativa a través de los elementos de una arquitectura de administración de red.

Los sistemas de administración de red, ejercen sus funciones y tareas basados en la manipulación y comunicación de información que proveen dichos protocolos.

Existen dos grandes familias de protocolos de administración SNMP (Simple Network Management Protocolo) y CMIS/CMIP (Common Management Information Services / Common Management Information Protocol). Ambos protocolos proveen un camino uniforme para acceder a cada elemento de una red con el objeto de obtener información administrativa y proporcionar control.

SNMP no es un solo protocolo, sino tres protocolos que juntos forman una familia; todos diseñados para trabajar en pro de las metas de la administración. Los protocolos que conforman la familia SNMP son:

- Simple Network Management Protocol (SNMP).
- Base de información de la administración MIB.
- Estructura e identificación de la información sobre la administración (SMI).

6.2.2.1. SNMP

Introducción

El origen de SNMP (Protocolo Simple de administración de Red) fue provocado por el desarrollo descomunal de Aparnet hoy internet. El creciente número de subredes que se unían a Aparnet hizo imposible que solo unos cuantos expertos en la red pudiesen resolver diversos problemas presentados en las diferentes subredes existentes, es así como los desarrolladores de

TCP/IP pensaron en la creación de un protocolo estándar que proporcionara un camino para el monitoreo y control de toda la red, facilidad de interactuar con el, además de proporcionar una solución a los problemas existentes.

Arquitectura de SNMP

En la arquitectura de SNMP esta una colección de nodos administradores y elementos administrados. SNMP es el encargado de comunicar la información administrativa entre los nodos administradores y los agentes en los nodos administrados.

La disposición de estos elementos pueden adoptar cualquiera de las arquitecturas fundamentales de un sistema de administración; centralizada, descentralizada o mixta.

En los nodos administradores, nodos administrados, agentes, el protocolo de comunicación y la base de datos donde se almacena la información de administración están implícitos en la arquitectura SNMP.
El nodo administrador deberá tener como mínimo los siguientes elementos:

- Una interfaz donde al administrador de red puede monitorear y controlar la red.
- Un conjunto de aplicaciones para análisis de datos.
- La capacidad de llevar los requerimientos de monitoreo y control a los elementos de la red.
- Una base de datos que almacene la información extraída de los elementos administrados.

SNMP esta a cargo solamente de los dos últimos.

Los agentes deben estar en los nodos administrados y en el nodo administrador si se desea que este sea autocontrolable y automonitoreable. A través del agente, el nodo administrador se puede obtener información y ejercer acciones de control sobre los elementos de la red. SNMP deberá ser integrado en cada elemento administrado en forma de agente, con el cual el nodo administrador podrá establecer un vínculo de control y monitoreo con cada uno de estos elementos.

Toda la información de los elementos administrados se almacena en una base de datos llamada MIB, SNMP proporciona una sintaxis específica para almacenar la información dentro de la MIB, de esta manera un nodo administrador puede entender la información proveída por otros agentes SNMP.

El nodo administrador y los nodos administrados son comunicados a través de un protocolo de administración de red. El protocolo de administración de red usado para redes basadas en TCP/IP es SNMP (Simple Network Management Protocol), el cual tiene las siguientes habilidades:

- Habilita los nodos administradores para recaudar información de un objeto administrado.
- Habilita los nodos administradores para establecer o modificar valores o parámetros en los agentes de los nodos administrados.
- Habilita a uno o más agentes para notificar eventos significativos a el nodo administrador.

6.2.2.2. SNMP dentro del modelo de capas del protocolo TCP/IP

SNMP es parte del grupo de protocolos TCP/IP y fue diseñado para ser de capa de aplicación.

El protocolo de capa de transporte en el que esta basado SNMP es UDP. Para el enrutamiento de paquetes usa IP, para capas inferiores puede basarse en una amplia variedad de protocolos (CSMA/CD, X.25)

SNMP requiere el uso de un servicio de transporte para la entrega de sus mensajes, SNMP no sabe si el protocolo de la capa de transporte es o no orientado a conexión. En el caso de TCP/IP, UDP provee el servicio de entrega de paquetes para SNMP, este protocolo de transporte no es orientado a la conexión.

Los puertos UDP que han sido asignados para la transferencia de paquetes SNMP son dos: los agentes escuchan peticiones, por el puerto 161, los nodos administradores escuchan peticiones cualquier entrega o petición de información por el puerto 162.

Como UDP es un protocolo sin reconocimiento de paquetes, es posible que un mensaje SNMP pueda perderse, SNMP fue desarrollo para ser usado sobre un protocolo de transporte no orientado a conexión, la razón para ello es que un protocolo con estas características no incrementa la carga de paquetes sobre la red, aminorando de esta manera la eficiencia con la que los paquetes SNMP son recibidos por cualquier elemento dentro de la configuración administrada. SNMP por si mismo no provee reconocimiento de paquetes.

El gráfico 6.1 muestra la dependencia entre los principales protocolos, entre ellos SNMP. Cada polígono cerrado corresponde a un protocolo y esta colocado directamente arriba de los protocolos que utiliza. Por ejemplo, SNMP depende del TCP que a su vez depende del IP.

La capa inferior representa todos los protocolos que proporciona el hardware. La segunda capa esta integrada por las listas inferiores de ARP y RARP. La tercera capa de la capa inferior contiene IP. Este es el único protocolo que ocupa toda la capa, los protocolos de más bajo nivel entregan información que llega del IP y los de más alto nivel deben utilizar IP para enviar datagramas.

SNMP depende de la Abstract Syntax Notation (ANSI).

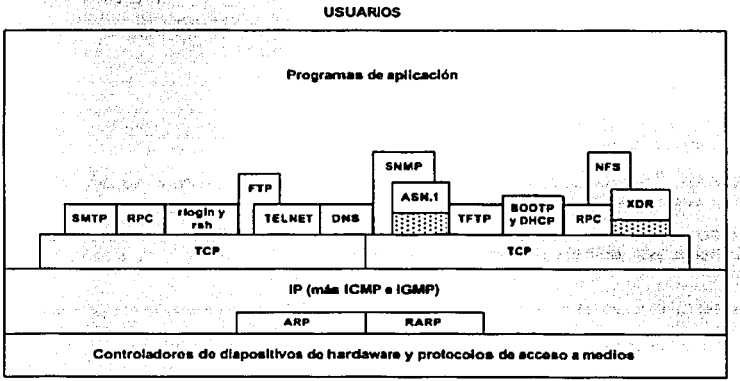


Fig. 6.1. Dependencia de protocolos

En los periféricos que tienen integradas las capacidades para SNMP corre un paquete de software agente para administración, cargado como parte de un ciclo de arranque o incrustado en la memoria fija (firmware) del dispositivo. Estos dispositivos que tienen agentes SNMP se dice que se trata de dispositivos administrados.

Los dispositivos administrados por SNMP se comunican con el software servidor SNMP que está localizado en cualquier parte de la red. El dispositivo habla con el servidor de tres formas:

POR SONDEO. Un dispositivo sondeado hace que el servidor se comunique con el dispositivo, preguntándole sobre su condición o sobre sus estadísticas actuales. El sondeo en ocasiones se hace en intervalos regulares, teniendo al servidor conectado a todos los dispositivos administrados de la red.

POR INTERRUPCIÓN. Un sistema SNMP basado en la interrupción hace que el dispositivo administrado envíe mensajes al servidor cuando algunas condiciones lo garanticen. De esta forma, el servidor conoce inmediatamente cualquier problema (a menos que el dispositivo falle , en cuyo caso la notificación debe hacerse desde otro dispositivo que haya tratado de comunicarse con el dispositivo que falló).

Sondeo dirigido por trampa

Es una combinación de sondeo y de interrupción para sobreponerse a todos estos problemas. Esta implica que el servidor haga un sondeo de las estadísticas a intervalos regulares o cada vez que lo ordene el administrador del sistema.

6.2.2.3. Base de datos de información administrativa (MIB)

El estándar especifica los elementos de los datos que un anfitrión o un ruteador deben conservar y las operaciones permitidas en cada uno. Cada dispositivo administrado por SNMP mantiene una base de datos que contiene estadísticas y otro tipo de información. Estas bases de datos se llaman Base de información sobre administración o MIB.

Las entradas de MIB tienen cuatro datos:

UN TIPO DE OBJETO. El tipo de objeto es el nombre de la entrada específica, generalmente a manera de un simple nombre.

UNA SINTAXIS. La sintaxis es el tipo de valor, como una cadena o un entero. No todas las entradas una MIB tienen un valor.

UN CAMPO DE ACCESO. El campo de acceso se utiliza para definir el nivel de acceso de la entrada, comúnmente está definida por los valores de sólo lectura, lectura-escritura, sólo escritura y no accesible.

UN CAMPO DE ESTADO. El campo de estado contiene una indicación de que la entrada de la MIB es obligatoria (lo que significa que el dispositivo administrado debe aplicar la entrada), opcional (el dispositivo administrado puede aplicar la entrada) u obsoleta (que no se utiliza).

Las entradas MIB generalmente las estandarizan protocolos y siguen reglas estrictas para el formateo, definidas por la Notación para Sintaxis Abstracta Uno (Abstract Syntax Notation One, ASN. I).

Definición de relaciones administrativas

La administración de red involucra la interacción de varias entidades de aplicación soportadas por un protocolo en este caso SNMP. Los elementos de la red administrada que se comunican con otros a través de SNMP son llamados entidades de protocolo o entidades de SNMP. Dichas entidades son: las aplicaciones de administración dentro del nodo administrador y el agente en el nodo administrado.

La interacción entre las entidades SNMP se puede definir como una relación uno a mucho entre el nodo administrador y un conjunto de agentes en varios nodos administrados, varios nodos administradores pueden existir en una configuración, y estos a su vez sostiene relaciones con varios conjuntos de nodos administrados.

Cada agente controla su propia, MIB, proporcionando la información requerida y realizando las modificaciones que los nodos administradores requieran. Por otro lado los nodos administradores tienen el derecho de hacer consultas y modificaciones a las MIB del conjunto de elementos que ellos administran. Con estas condiciones surge la necesidad de contar con alguna táctica que permita a los agentes protegerse así mismos y a sus MIBs de accesos no autorizados. De este hecho nace el concepto de comunidades SNMP y nombres de comunidad.

Una comunidad SNMP es una relación entre un agente SNMP y un conjunto arbitrario de nodos administradores, la cual define reglas especificas que hace valida el acceso al agente y a su MIB.

El concepto de comunidad es local y se define en el agente, este establece una comunidad por cada combinación con un nodo administrador. A cada comunidad le es asignado un nombre llamado nombre de comunidad el cual es único dentro del agente. Como los nombres de comunidad son definidos en el agente, el mismo nombre puede ser usado por diferentes agentes. La definición de los nombres es irrelevante y no indica ninguna similitud entre las diferentes comunidades.

Al ser definidas las comunidades y los nombres de las mismas, el agente puede ejercer control sobre los accesos que los nodos administradores realizan a su MIB en tres aspectos:

- Autenticación. Es el proceso mediante el cual se asegura que una comunicación entre el agente y el nodo administrador es auténtica.
- Política de acceso. Un agente puede limitar el acceso a su MIB a un selecto grupo de nodos administradores.
- Servicio de Proxies. El concepto de comunidad es también utilizable cuando se cuenta con proxies, recordemos que un proxy es un agente que actúa como intermediario con otros dispositivos.

6.2.3. Protocolos de seguridad, SNMP

SNMP proporciona múltiples ventajas referentes a su fácil Implementación y su gran funcionalidad, pero desafortunadamente no provee elementos de seguridad. SNMP no es capaz de autentificar la fuente de un mensaje de administración, el uso de un nombre de comunidad puede no proveer seguridad ya que un agresor puede observar un mensaje y averiguar dicho nombre y usarlo para su beneficio.

Los protocolos de seguridad no son totalmente compatibles con SNMP, los formatos de los encabezados de los mensajes son diferentes y muchos de los procedimientos que SNMP aplica fueron modificados, sin embargo el formato de los PDU es el mismo.

6.2.3.1. Servicios de seguridad que proveen los protocolos de seguridad SNMP

En general los protocolos de seguridad proveen los siguientes servicios que incrementan la seguridad en un esquema de administración y monitoreo de red.

- Integridad en los datos. Asegura que todo mensaje sea recibido o enviado, sin duplicación, interrupción, intersección o modificado.
- Autenticación del origen de los datos. Reconoce el origen de cualquier mensaje enviado.
- Confidencialidad en los datos. Asegura que la información no este disponible para entidades o procesos no autorizados.

La integridad en los datos y la autenticación del origen de los mismos, son proporcionados por un mismo mecanismo, la confidencialidad en los datos es un servicio opcional que puede ser adicionado a los otros dos servicios en la misma implementación.

6.2.3.2. Mecanismos de seguridad

Para proveer los servicios de seguridad listados anteriormente, los protocolos de seguridad deberán incluir los siguientes mecanismos.

- Para garantizar la integridad de los datos, un algoritmo de resumen de mensaje es requerido. Dicho algoritmo es usado para calcular un resumen de 128 bits de un porción apropiada del mensaje. Este resumen es incluido como parte del mensaje enviado a la maquina receptora, para asegurar que dicho mensaje no sufrió modificación. El algoritmo de resumen de mensajes que los protocolos de seguridad SNMP usan es el MD51. Una marca de tiempo es incluida en cada mensaje generado, el valor de la marca de tiempo esta basado en los relojes de sincronización de los nodos administradores y los agentes. Un receptor de mensaje evalúa la marca de tiempo para determinar si dicho mensaje es reciente, o si el mensaje esta relacionado con otros que el mismo recipiente ha recibido. En conjunción con otra información disponible en el mensaje (por ejemplo: el identificador de petición), la marca de tiempo también indica si el mensaje es una respuesta de un mensaje previo.
- Para garantizar la integridad de los datos y la autenticación del origen de los mismos, la porción del mensaje que es resumida es primero reconstruida con un valor secreto compartido por la maquina originadora del mensaje y el recipiente
- Para garantizar la confiabilidad de los datos, un algoritmo simétrico de encriptación es requerido. Una porción apropiada del mensaje es encriptada. Los protocolos de seguridad usan el algoritmo de encriptación DES2.

6.2.3.3. Especificaciones de los protocolos

Como mencionamos anteriormente, los protocolos de seguridad SNMP utilizan dos métodos para proveer sus servicios de seguridad: un algoritmo de resumen de mensajes MD[5] y un esquema de encriptación DES. Para que un servicio de seguridad sea brindado, estos métodos deben interactuar con dos diferentes protocolos: El protocolo de *autenticación-resumen y el protocolo simétrico de privada.*

La conjunción de estos dos protocolos y los respectivos métodos ofrecen los mecanismos que a su vez proporcionan todos los servicios de seguridad mencionados.

Cuando se brinda el servicio de autenticación del origen de los datos, por ende se brinda el servicio de integridad de los mismos. El servicio de confidencialidad puede ser incluido en la implementación. De esta manera una arquitectura de administración de red basada en estos protocolos puede proveer varios niveles de seguridad, es decir los datos pueden ser enviados sin

ningún servicio de seguridad o bien solo con el servicio de autenticación (incluyendo el servicio de integridad de los datos), o solo con el servicio de confidencialidad, o finalmente con todos los servicios.

6.2.3.4. Protocolos de seguridad

Protocolo de autenticación – resumen. Este protocolo junto con el algoritmo MD[5] proporciona el mecanismo para la autenticación del origen e integridad de los datos. En esencia el proceso de autenticación es el siguiente: Un resumen de mensaje es ejercido sobre el mensaje que será enviado, usando el algoritmo MD[5]. Dicho mensaje mas el resumen es transmitido, cuando el mensaje llega a la entidad receptora, de nueva cuenta se realiza un resumen del mensaje recibido y si este resumen es igual al resumen que esta incluido en el mensaje, entonces el mensaje recibido es declarado autentico e integro

Protocolo simétrico de privada. Este protocolo provee protección a los datos de tal forma que solo la entidad fuente y la entidad destino puedan leer el mensaje. El método para proveer dicha protección es la encriptación, la cual requiere que el destino y la fuente compartan la misma llave de encriptación. El algoritmo usado para la encriptación es DES.

6.3 Mantenimiento de redes

6.3.1. Monitoreo de red

El monitoreo de red consiste en observar y analizar el estado y comportamiento de cada elemento de la red administrada.

6.3.1.1. Clasificación de la información obtenida por el monitoreo

El propósito de monitoreo es obtener información y ésta puede ser dividida en:

Información estática

Información referida a la configuración de cada elemento en la red. Por ejemplo el número de identificación de los puertos en un concentrador, los nombres de los archivos de dispositivo asociados a una partición de disco, por mencionar algunos.

La información estática es usualmente generada por el elemento involucrado, por ejemplo un concentrador contiene su propia información de configuración. Esta información puede estar disponible al sistema de monitoreo directamente desde el elemento si este tiene un agente apropiado.

Información dinámica

Información relacionada con eventos en la red, como un cambio en el estado de un protocolo o la transmisión de un paquete en la red.

La información dinámica es recolectada y guardada por el nodo de red que la genera sin embargo, mucha de esta actividad puede ser observada y almacenada por otro nodo conectado a la misma red. El término monitor de red o nodo monitor es usado para referirse a un dispositivo en al red que observa las actividades de los demás nodos conectados, así como el tráfico de paquetes depositados en la red.

Información estadística

Información que es derivada de la información dinámica, como el promedio del número de paquetes por unidad de tiempo por computadora.

La información estadística puede ser obtenida por cualquier sistema que tenga acceso a una fuente de información dinámica. La información estadística es usualmente generada por un monitoreo de red. Para ello será necesaria la transmisión de la información dinámica hacia el monitor, donde la procesará y analizará. Si el monitor no tiene acceso a la información dinámica de un nodo, entonces el nodo mismo tendrá que procesar y analizar su información para posteriormente enviar el resultado de los cálculos del monitor.

6.3.1.2. Elementos y configuración de un sistema de Monitoreo

Los elementos en términos funcionales que componen a un sistema de monitoreo de red son:

- Objetos administrados. Son objetos que representa recursos tanto de software como de hardware en la red.
- Agente. Es un conjunto de software dedicado a tareas de administración, el cual manipula la información administrativa contenida en una MIB y comunica esta información a un nodo monitor.
- El incluir un agente a un nodo lo hace monitoreable.
- Aplicaciones del monitoreo. Son programas de aplicación que realizan tareas sobre los datos recaudados y que presentan sus resultados a los usuarios.
- Elementos de monitoreo en un nodo monitor. El nodo monitor es por si mismo un elemento de la red y por lo tanto un objeto administrado monitoreable, dicho nodo generalmente incluye un agente. Es de vital importancia monitorear un estado y comportamiento del nodo monitor para garantizar que este siga realizando de una manera eficiente sus funciones.
- Elementos de monitoreo en un nodo monitoreado. En un nodo monitoreado comúnmente solo incluye dos elementos de monitoreo: el agente y los objetos administrados.
- Configuración básica de un sistema de monitoreo. Existen varias configuraciones que un sistema de monitoreo puede adoptar. La configuración más simple es la más común, dicha configuración requiere que el nodo monitor y el nodo monitoreado compartan el mismo protocolo de administración y la misma sintaxis y semántica de MIB.
- Configuración con un monitor externo. Un sistema de monitoreo pueden también incluir uno o más agentes que monitorean las actividades en la red desde fuera del o los nodos monitores, estos agentes son conocidos como monitores externos o monitores remotos.

6.3.1.3. Polling y Reporte de eventos

La información que es útil para propósitos de monitoreo es recolectada y guardada por los agentes y transferida al módulo administrador en un nodo monitor.

Dos técnicas son usadas para poner disponible la información del agente al módulo administrador: El polling (encuesta) y el reporte de eventos.

El polling es una interacción petición / respuesta entre el módulo administrador y el agente. El módulo administrador puede realizar una petición de información a cualquier agente (siempre y cuando este autorizado) y el agente responderá con la información de su MIB.

Un sistema de monitoreo puede utilizar el polling entre sus elementos para diversos fines como son: obtener condiciones que periódicamente se actualizan o para investigar un área en detalle después de que ha sido descubierto un problema en ella.

En el reporte de eventos, la iniciativa de transferencia es del agente y el módulo administrador esta actuando como receptor esperando por información.
Un agente puede generar un reporte periódicamente para dar al sistema de administración el estado actual de cualquier elemento, también puede generar un reporte cuando haga un evento significativo por ejemplo un cambio de estado.

El periodo de reporte o sea, el tiempo que debe esperar el agente para enviar la información al módulo administrador, es definido por el agente, este puede ser modificado por el nodo monitor.

El reporte de eventos es muy útil para detectar problemas tan rápidamente como estos ocurran. Es más eficiente que el polling para monitorear objetos cuyos estados o valores cambien con poca frecuencia.

Las dos técnicas son muy utilizadas, un sistema de monitoreo regularmente emplea ambos métodos.

6.3.1.4. Monitoreo de fallas

El objetivo de este es identificar fallas lo más rápido posible, después de que éstas ocurran, además de ayudar a determinar sus causas así como la acción correctiva que puede ser tomada.

Funciones de monitoreo de fallas

El monitoreo de fallas, básicamente deberá detectar y reportar fallas. Como mínimo, el agente deberá mantener un archivo log o archivo resumen que contenga los eventos significativos y errores que se generen, la información de estos archivos deberá estar disponible para los nodos monitores autorizados. Si el monitoreo de fallas puede implementar un método polling o un método reporte de eventos, estos archivos log serán muchos más confiables.

El agente envuelto en este tipo de monitoreo deberá tener la capacidad de reportar fallas a uno o más sistemas de administración.

Un buen monitor de fallas, debe anticiparse a las mismas, esto puede lograrse definiendo valores de umbral o frontera. Estos valores son límites preestablecidos que están cerca de ser una falla, cuando los resultados de un evento rebasan los valores de umbral definidos, se genera una alarma, de esta manera se detectan situaciones que puedan terminar en una falla para dispositivos de interconexión de red, servidores.

El monitoreo de fallas deberá también asistir en el aislamiento y diagnóstico de la falla. En una situación compleja, las fallas serán diagnosticadas, aisladas y finalmente corregidas por el esfuerzo del administrador y programas de monitoreo.

En la detección de fallas, es necesario que el sistema de monitoreo cuente con una eficiente interfaz, que permita interactuar de manera sencilla y rápida al administrador humano con los programas de monitoreo. Algunas de las pruebas que una interfaz debe tener disponible es forma de comandos son:

- Prueba de conectividad
- Prueba de integridad de datos

- Prueba de integridad de protocolos
- Prueba de saturación de datos
- Prueba de saturación de conexión
- Prueba de tiempo de respuesta
- Prueba de funcionalidad del protocolo de monitoreo

Monitoreo de desempeño

Un requisito absoluto para la administración de una red es la posibilidad de medir el desempeño de la misma. Nosotros no podemos esperar administrar y controlar una red sin antes monitorear el desempeño.

Indicadores de desempeño

Una de las dificultades a las que se enfrenta un administrador de red es la selección y el uso de los indicadores apropiados para medir el desempeño de su red. Existen un gran número de indicadores. Existen dos categorías de indicadores: los orientados a servicios y orientados a eficiencia.

Monitoreo de desempeño orientado a servicios

Los indicadores orientados a servicios son los que se relacionan con la satisfacción de las necesidades de los usuarios por medio de los servicios que proporciona la red por ejemplo: almacenamiento de datos, correo electrónico, impresión.

La disponibilidad es el porcentaje de tiempo que una red, un elemento o una aplicación esta disponible para un usuario. Dependiendo de la circunstancia de una red, una alta disponibilidad puede ser muy importante. La confiabilidad de ésta depende de los componentes individuales de una red. La confiabilidad es al probabilidad de que un componente desempeñe una función especifica por un tiempo determinado, bajo condiciones señaladas.

El tiempo de respuesta aparece en la terminal de un usuario después de que éste realizó una petición. Es decir el tiempo entre la última tecla oprimida por el usuario y el principio del despliegue del resultado del monitor. Un tiempo rápido de respuesta es la llave de la productividad cuando se trabaja con aplicaciones de cómputo. Cuando un usuario y una computadora interactúan de modo que ninguno tenga que esperar al otro, la productividad se incrementa notablemente y la calidad se mejora. Con el tiempo de respuesta podemos identificar cuellos de botella o lugares donde sea posible que se formen.

Precisión es el porcentaje de tiempo en el cual no ocurren errores en la transmisión ni en la entrega de información. Sobre la precisión generalmente el administrador no tiene control, ya que depende directamente de las capas de protocolo inferiores. Sin embargo este indicador puede ser muy útil al advertir posibles fallas, si la precisión es muy baja, dicho indicador puede advertirnos fallas como: posible falla en la línea de transmisión o posibles interferencias o ruido que deben ser corregidos.

Monitoreo de desempeño orientado a eficiencia

El rendimiento es la velocidad en la cual un evento de una aplicación (transferencia de archivos, mensajes) ocurre. Este puede verse afectado por un mal funcionamiento de los elementos de la red a los cuales la aplicación este asociada, por ejemplo si una transferencia de archivos es lenta, probablemente la velocidad del canal de comunicación ya no sea la adecuada o bien, puede existir un cuello de botella en algún lugar.

La utilización es el porcentaje de tiempo que un recurso esta en uso sobre un periodo de tiempo dado. El uso más importante de éste es la búsqueda de cuellos de botella potenciales y

áreas de congestión, además de que usualmente el tiempo de respuesta se incrementa exponencialmente a razón del incremento en la utilización de un recurso.

Funciones del monitoreo de desempeño

El monitoreo de desempeño tiene dos funciones básicas:

- Medición del desempeño: el cual obtiene estadísticas acerca de los elementos en la red.
- Análisis del desempeño: es el análisis de datos estadísticos. La medición del desempeño es casi siempre llevada a cabo por los agentes dentro de los dispositivos en la red. Estos agentes están en posición de observar la cantidad de tráfico de paquetes dentro y fuera de un elemento, el número de conexiones en las capas del protocolo, el tráfico por conexión y otras mediciones que provee un detallado esquema del comportamiento de un elemento de la red.

Monitoreo de acceso

Es el seguimiento del uso de los recursos de la red por los usuarios. Es necesario conocer con precisión toda la información relacionada con los accesos a los recursos de la red, para así poder tener un control más efectivo sobre los mismos y poder planear el crecimiento de la red con datos reales.

Algunos de los accesos a recursos que pueden ser observados son:

- Acceso a equipos de computo y cualquier periférico.
- Acceso a sistemas y programas: aplicaciones y programas dentro de los servidores, base de datos.
- Acceso a servicios: esto incluye todos los servicios de comunicación y servicios de información disponibles para los usuarios de la red.
- Acceso a líneas de comunicación.

La información que deberá obtenerse de cada usuario estará basada en los requerimientos del administrador y tipo de recurso que sea monitoreado. Los siguientes son ejemplos de algunos datos que pueden ser recopilados:

Identificación

- Máquina donde se realiza la conexión
- Número de paquetes por acceso
- Tiempo de inicio y fin del acceso
- Recursos usados

6.3.2. Control de red

El control de red es la acción de modificar parámetros establecidos en los elementos de la red con el fin de realizar tareas de administración.

Existen dos áreas funcionales que la administración de red debe cubrir, en las cuales el control se desarrolla de una manera amplia y son: configuración y seguridad.

6.3.3. Control de configuración

La administración de configuración se fundamenta en el siguiente principio básico: el nodo administrador tiene acceso a los elementos de la red, sean físicos o lógicos, para poder ejercer

sobre ellos funciones como: iniciar, detener, configuración de parámetros y estados. Estas acciones no son más que acciones de control también referidas como control de configuración.

Mientras la red esta en operación, la administración de configuración es responsable de realizar cambios en las configuraciones de los elementos de la red, en respuesta a otras funciones de administración de red o bien por petición del administrador. Por ejemplo si a través del monitoreo de fallas se detecta y aísla una falla, por medio del control de configuración se puede alterar la configuración de uno o varios elementos para eludir la falla mientras se repara.

Funciones del control de configuración

La función de configuración describe la naturaleza y el estado de los recursos que son de interés para ser administrados. Es decir la información de configuración incluye una especificación de los recursos bajo la administración y sus atributos. Los recursos pueden ser físicos o lógicos. Los atributos incluyen nombre del elemento, dirección, características de operación, versiones de software.

La información de configuración puede ser estructurada de las siguientes formas:

- Una simple lista de campos.
- Una base de datos orientada a objetos. Cada elemento de interés es representado por uno o más objetos. Cada objeto contiene atributos cuyos valores reflejan las características de cada elemento representado.
- Una base de datos relacional. Cada campo dentro de la base contiene valores que reflejan características de los elementos de la red.

Esta información debe ser accesible al nodo administrador, generalmente, la información es almacenada cerca del recurso administrado en cuestión, donde se encuentre el agente, si dicho agente se encuentra dentro del elemento administrado entonces ahí también se almacenará la información.

Configuración y modificación de atributos

El control de configuración deberá habilitar al nodo administrador para que remotamente pueda configurar y modificar los atributos.

Existe una limitante a esta capacidad: algunos de los atributos reflejan la realidad en un recurso y no pueden , por su naturaleza ser modificados remotamente. Por ejemplo, un atributo puede ser el número de puertos en un concentrador, el número de puertos puede ser únicamente cambiado por una acción física en el concentrador, no por una acción remota; no obstante se puede remotamente habilitar puertos en cualquier tiempo.

Una modificación a un atributo será una modificación a la información de configuración en la base del agente. En general las modificaciones pueden clasificadas como:

ACTUALIZACIÓN DE LA BASE ÚNICAMENTE. Cuando un administrador ejecuta un comando dentro del sistema de administración hacia un nodo administrado y este comando repercute en un cambio de valor en los atributos de la base, pero no cambia atributos de configuración ni de operación del nodo. Por ejemplo: cuando es cambiado el nombre y la dirección del administrador de red.

ACTUALIZACIÓN DE LA BASE MÁS LA MODIFICACIÓN DEL RECURSO. En adición a la actualización de la base de datos en el agente, un comando puede tener un efecto en los atributos de configuración y operación del recurso administrado. Por ejemplo, si el estado del atributo de un puerto físico en un concentrador es configurado como deshabilitado, entonces el agente no solo actualiza el atributo en la base de datos, si no también deshabilita el puerto.

ACTUALIZACIÓN DE LA BASE MÁS LA ACCIÓN. En algunos sistemas de administración no existen comandos de acción directa disponibles para los administradores, sin embargo existen parámetros en la base de datos que cuando son configurados, producen una cierta acción. Por ejemplo, un puente puede mantener definido un parámetro de reinicialización en su base de datos, si éste parámetro es configurado como verdadero por un administrador autorizado, el puente realizará el proceso de reinicialización, cuando este proceso esté terminado el parámetro regresará a su estado original es decir falso.

El control de configuración deberá permitir la configuración y modificación de los atributos de los recursos administrados sin que toda la red o parte de ella sean dados de baja.

Los vínculos describen una asociación o conexión entre elementos de la red. Por ejemplo: una topología, estructura jerárquica de los componentes, conexión física o lógica. El administrador deberá tener el control sobre estos vínculos en el sistema de administración y en cualquier momento podrá modificarlos.

El administrador de red podrá a través de su sistema de administración, terminar o iniciar la operación de toda la red o bien de alguna subred. El proceso de inicialización incluye la verificación de que todos los recursos se hayan levantado correctamente, así como los vínculos y la notificación a los usuarios y al mismo administrador. Para el proceso de terminación deberá incluir la capacidad de notificar a los usuarios antes de que este proceso sea terminado.

Un administrador puede requerir información acerca de los atributos existentes en la base de datos de cualquier agente, además explorar las relaciones entre los objetos administrados, esta no es una acción de control si no de monitoreo, pero el control de configuración deberá proveer esta facilidad al administrador basado en las funciones de monitoreo.

6.3.4. Control de seguridad

El recurso más valioso dentro de una compañía o institución es la información. Las computadoras se han convertido en una fuente de almacenamiento y proceso de dicha información, por lo que se ha generado la necesidad de salvaguardar a los sistemas de cómputo de posibles ataques. Al parecer los esquemas de cómputo distribuido y la utilización de redes para la comunicación de datos han producido un gran cambio en la concepción de seguridad de cómputo, por lo que se ha pensado en la seguridad de los datos que viajan por la red y se delinearon acciones para proteger dichos datos. El nombre genérico del grupo de herramientas y estrategias diseñadas para proteger información dentro de un sistema de cómputo, esté o no en red, se le conoce como seguridad en cómputo.

La administración de seguridad o control de seguridad, tendrá que ver con todos los aspectos de la seguridad en cómputo y deberá ejercerse sobre los recursos que son administrados, incluyendo al propio sistema de administración.

El control de seguridad en cómputo define dos requerimientos básicos:

- Información confidencial. La información y los parámetros de configuración en todos los elementos de la red debe estar disponible solo para usuarios autorizados.
- Integridad. La información y los parámetros de configuración en todos los elementos de la red, pueden ser modificados únicamente por usuarios autorizados.

Ataques a la seguridad

Los ataques a los sistemas de cómputo son muy variados y para tomar medidas sobre ellos es necesario catalogarlos:

- Interrupción. Un valor en la red es destruido, no utilizable o no disponible. Como ejemplo podemos citar: la destrucción de una pieza de hardware o bien la deshabilitación de un elemento lógico como un sistema de archivos.
- Intercepción. Un individuo no autorizado obtiene acceso a un valor dentro de la red. El individuo puede ser una persona, un programa o una computadora. Por ejemplo la intervención de una transmisión de archivos para realizar una copia ilícita.
- Modificación. Un individuo que no solo obtiene acceso a un valor de la red si no también modifica la información. Por ejemplo el cambio de datos de un archivo, la modificación de un programa, la modificación de un mensaje enviado por la red.

Los ataques al hardware son aquellos para causar un daño físico pueden ser accidentales o intencionales.

Los ataques al software incluyen ataques al sistema operativo, utilerías y programas de aplicación. El software en especial los programas de aplicación son fáciles de borrar, además existe la posibilidad de alterar o dañar al software dejándolo no utilizable o en el peor de los casos sigue funcionando realizando tareas que no están autorizadas, con la opción a dañar los datos con los que se trabaja por ejemplo los virus.

Los datos son una parte muy vulnerable dentro de un sistema de computo. Los ataques a los datos los podemos dividir en dos:

- accesos no autorizados
- modificación de datos

En el tipo de ataques a las líneas de comunicación tiene que ver con la manipulación de los datos que viajan por la red. Por ejemplo el agresor puede intervenir los paquetes que son transmitidos para modificar los datos en ellos o bien, modificar el flujo de paquetes incrementando estos para causar un daño en la comunicación de la red. También el agresor puede tomar una dirección asignada de la red y utilizarla para sus propios fines. Estos tipos de ataques son muy difíciles de detectar debido a su naturaleza.

Como un sistema de administración involucra un conjunto de programas de aplicación, elementos de hardware y bases de datos, los ataques citados anteriormente pueden ser considerados como ataques al sistema de administración de red, además de dichos ataques podemos definir ataques específicos a un sistema de administración

- Usuario enmascarado. Es un usuario no autorizado, que trata de realizar tareas de administración de red. Puede tener acceso a las aplicaciones de administración y a la información de los objetos administrados.
- Sistema enmascarado. Es una computadora que trata de obtener los derechos del nodo administrador sobre los elementos administrados.
- Interferencia con el intercambio de información e instrucciones entre el nodo administrador y los agentes. Un ataque grave es la observación del tráfico del protocolo de administración por un extraño para extraer información. Más dañina es al modificación de este tráfico para romper la operación del agente con los recursos o el nodo administrador.

Funciones de control sobre la seguridad

En el control de seguridad de un sistema de administración de red existen tres funciones básicas a cubrir:

- Mantenimiento de la seguridad de la información. Un sistema de administración de red deberá proveer medidas para limitar y validar el acceso a la información que éste maneja, por ejemplo: derechos de accesos a la información, contraseñas, validación de la información.

- Seguridad de actividades. Se debe dar seguimiento a toda actividad realizada, a través del registro de eventos, monitoreo del uso de recursos, reporte de violaciones a la seguridad del sistema.
- Control de acceso a recursos. Un importante servicio que un sistema de administración deberá proveer es el control de los accesos a los recursos, este proceso involucra la validación y autenticación de cualquier usuario, maquina o programa antes de permitir dicho acceso. Ya que se haya realizado la validación, un usuario podrá crear o borrar objetos administrados, tener acceso a las fuentes de información, cambiar los atributos.

CAPÍTULO 7
Desarrollo e implementación

7.1. Descripción

Como se ha visto, la red local se basa en una arquitectura cliente/servidor que se apoya en el protocolo TCP/IP, pues las aplicaciones que emplean los clientes ocupan un conjunto de protocolos de la estructura TCP/IP para la comunicación entre dispositivos. Algunos servicios palpables que utilizan estos protocolos son el correo electrónico, SMTP (Simple Mail Transport Protocol); la emulación de terminales, Telnet; transferencia de archivos, FTP (File Transfer Protocol) y para fines de monitoreo, SNMP (Simple Network Management Protocol).

La red esta compuesta con el estándar Ethernet debido a que el cableado tiene una combinación entre categoría 3 y categoría 5. En base a que ya se tiene una topología en estrella y en base a la tabla 7.1 que contiene la comparativa entre tecnologías LAN.

	Fast Ethernet	Token Ring	100 VG-AnyLan
Método de Acceso	CSMA/CD	Token Passing	Prioridad bajo demanda
Manejo de problemas	Los problemas son identificados por series procedimientos aislados	Los procedimientos de prueba son invocados cada vez que un nodo accesa en la red, si uno de los procedimientos falla, se generan mensajes que indican las posibles causas, incluyendo direcciones sospechosas	La prueba de enlace se efectúa cada vez que se establece un enlace, como al encender el equipo y al conectar el cable o cuando ocurren algunos errores
Costo de dispositivos	Muy baratos	Más caros que Fast Ethernet en un 80%	Mas caros que Fast Ethernet en un 50%, apoyada por pocos fabricantes (principalmente HP)
Velocidad de tranmsión	100 Mbps	4 ó 16 Mbps. Todos los equipos deben configurarse en la misma velocidad	100 Mpbs
Instalación	Instalación sencilla debido a la posibilidad de conexión en estrella o árbol, se pueden incluir nuevos nodos sin interrumpir el tráfico de la red	Requiere de un concentrador donde las conexiones son hechas a un MAU principal con algún otro sistema o concentrador, si se daña un equipo de la red se interrumpe la continuidad de la red	Igual que Fast Ethernet
Tráfico	Se satura más rápido que Token Ring debido a la gran cantidad de colisiones que causa una transmisión de gran volumen de información	No existen colisiones por lo que aprovecha al máximo su ancho de banda	El protocolo de Prioridad bajo Demanda es un método de acceso simple y determinista, que maximiza la eficiencia de red eliminando las colisiones de Fast Ethernet y los retardos de rotación de Token Ring

Tabla 7.1 Comparativa de tecnologías LAN

Algunos de los concentradores tienen la función de Autonegociación. Tienen la posibilidad de poder comunicar a los dispositivos las capacidades de transmisión sobre un segmento determinado de la red: Primeramente si lo permiten las características del cable con que estén comunicados los dispositivos, y por otra parte las tarjetas de red. De esta forma tanto el concentrador como las tarjetas de red (NIC), pueden aumentar la velocidad de transmisión de datos inclusive cambiar a una transición Full-duplex.

Debido a que el backbone de la red se sustenta en concentradores, provoca numerosas "caídas" en la red, es decir, las computadoras dejan de tener conexión con el servidor causado por el concentrador; puesto que éste se puede considerar que comparte todo el ancho de banda, es decir, el total de este ancho de banda se divide en el total de todos los puertos, es así donde se forman dichos cuellos de botella y son tantas las peticiones de transmisión de datos que el concentrador no puede con este trabajo y deja de funcionar temporalmente por periodos pequeños.

Las tarjetas de red de esas máquinas tienen una dirección IP por medio de un servidor DHCP, es decir, solicitan al servidor una dirección IP. Cuando pierde dicha conexión con el servidor, se necesita la ayuda de algún comando como winipcfg (para Windows 9x), cerrar la sesión y volverse a firmar en la red para poder restaurar la conexión, o en casos extremos reiniciar el equipo. De esta forma las personas de soporte o help desk resuelven este problema. Cabe señalar que todos los clientes tienen el sistema operativo Windows 95 o Windows 98.

En la figura 7.2 se muestra la organización de la red de forma general, nombrando cada concentrador de acuerdo al departamento donde se encuentren. Esto con la finalidad de administrar los concentradores de una forma más franca y clara. Con esta descripción es más sencilla la explicación para personas cuyos departamentos son superiores a la Subdirección de Informática (departamento encargado de todo el cómputo de la delegación).

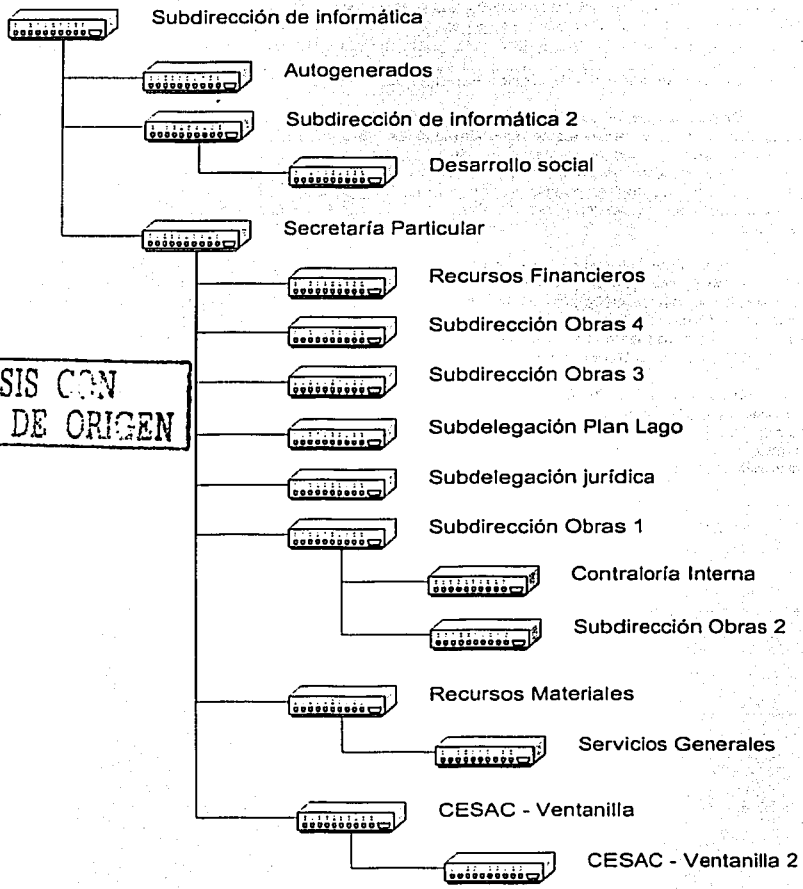


Fig. 7.2. Organización de concentradores de la red actual

De acuerdo a la figura 7.2, la estructura en cascada de los concentradores es uno de los factores que hace que el performance de la red sea deficiente y los tiempos de respuesta sean largos a causa de la división de ancho de banda por cada puerto ocupado dentro de la red. De esta forma si existen 120 equipos conectados de manera simultanea, los problemas de conexión son evidentes.

En cuánto a cableado, la mayoría de los Jacks (donde se introduce el conector RJ-45), el cable esta mal rematado inclusive dentro del panel de parcheo; por lo que puede tener falsos contactos, esto se comprobó por un simple comando de MS-DOS (ping) lo que nos muestra cortes de comunicación al mostrarnos el mensaje de "Tiempo de espera agotado" y subsecuentemente los datos de la dirección al que se manda la petición de respuesta, la cantidad de bytes que se envían, el tiempo de respuesta y el tiempo de vida. La elaboración de cables para la conexión desde la roseta a la computadora (patch cord), es elaborado por parte del personal que labora en la subdirección de Informática, sin ningún estándar en la organización de los pines en el conector; además que en muchos de los casos el aislante sale de este conector, inclusive se observa que algunos hilos no hacen contacto con el metal de los conectores (no están bien rematados).

Para poder transmitir datos de alta importancia como son las bases de datos a oficinas de Centro Histórico y acceso a Internet emplean un solo enlace por lo que se necesita separar estos dos servicios, además de aumentar la velocidad en cada uno de estos servicios. Esto se refleja en el tiempo que tarda en transmitir dicha información y por otra parte cuando se acceda a alguna página de World Wide Web.

7.2. Requerimientos de red

Como se ha mostrado en el apartado anterior, las necesidades son:

- **Mayor número de direcciones:** direccionamiento y configuración IPv6 de equipo.
- **Cableado estructurado**, bien delimitado y correctamente instalado.
  - Cableado para tres concentradores más (Departamentos: Alumbrado público, Tenencia de la tierra y Pagos).
- **Enlaces dedicados:** un enlace para Internet e independientemente, un enlace dedicado con el D.D.F. para datos.
- **Hardware y software:** mejores dispositivos de red, es decir, switches para mejorar el desempeño de la red local y PC's actuales con sistema operativo que tengan soporte para el protocolo IPv6.

7.2.1. Aumento de número de direcciones

Es un hecho que el número de direcciones aumenta y aumentará porque cada vez existen mas aplicaciones que se basan en comunicación por medio de redes. Por otra parte, cualquier tipo de institución la tendencia es crecer en su infraestructura y personal, por lo que se necesitará una mayor cantidad de direcciones IP.

En cuanto a la configuración de IPv6 necesitamos planear el direccionamiento. Existen tres organizaciones que tienen prefijos sTLA, es decir, tienen asignados rangos de direcciones lo suficientemente considerables, nos sólo para sí mismos, si no para asignar a bastantes organismos: UNAM, AVANTEL y ITESM.

Se ha elegido que el proveedor de este servicio sea nuestra casa, la UNAM, por tener experiencia en el ramo, solidez en su backbone y la mejor atención por parte de soporte.

Para obtener un rango se necesita enviar una solicitud de direcciones IPv6, solicitud de dominio inverso y solicitud de nombres IPv6 para pertenecer a la RedUNAM.

Solamente los responsables de la red local de alguna institución o empresa pueden solicitar delegación del espacio de direcciones para un bloque pNLA /48 a partir del prefijo pTLA 3ffe:8070::/28. Todo esto solo para servicio de pruebas, sin costo.

Si se requiere servicio de Producción se solicita direcciones y delegación de espacio de direcciones IPv6 a partir del prefijo sTLA 2001:0448::/35 de la UNAM obteniendo un prefijo que no se define si no hasta que el organismo de la UNAM que regula la asignación, apruebe conforme a sus políticas.

Como se dijo, la UNAM tiene un prefijo sTLA (2001:0448::/35) para la parte de producción. Para la red CUDI (Corporación Universitaria para el Desarrollo de Internet) se ha asignado un prefijo sNLA 2001:0448:0003::/48 (para producción) y pNLA (pruebas) 3ff3:8070:1060::/48.

Partiendo de que se ha asignado a los asociados académicos el prefijo sSLA, 2001:0448:0003:XYYZ:/64, podemos afirmar que puede ser aprobado algún tipo de direcciones donde:

- X identifica las regiones (16 regiones posibles):
  X=0, backbone
  X=1, Internacional
  X=2, Internacional
  X=3, Tijuana
  X=4, Monterrey
  X=5, México D.F.
  X=6, Guadalajara
  X=7, Cd. Juárez
- YY identifica las redes de los asociados (256 redes posibles), inicialmente se asignan 2 redes a cada asociado, pudiendo asignar mas si así lo requieren.
  X=5, México D.F.
  YY=00, IPN 2001:0448:0003:5*00*Z::/64
  YY=01, IPN 2001:0448:0003:5*01*Z::/64
  YY=02, UAM 2001:0448:0003:5*02*Z::/64
  YY=03, UAM 2001:0448:0003:5*03*Z::/64
  YY=04, UDLA 2001:0448:0003:5*04*Z::/64
  YY=05, UDLA 2001:0448:0003:5*05*Z::/64
  YY=06, UNAM 2001:0448:0003:5*06*Z::/64
  YY=07, UNAM 2001:0448:0003:5*07*Z::/64
- Z identifica las subredes para los asociados (16 subredes posibles). Cada organismo tiene 2 redes con 16 subredes y 2^{64} hosts cada una.

Entonces nuestro rango de direcciones según este esquema podría ser el siguiente:

Desde 2001:0448:003:5080::/64 hasta 2001:0448:003:509F::/64

y los 64 bits restantes, pertenecen a la dirección del host según aparece el modelo de direcciones unicast del apartado 5.5.1.1 del capitulo anterior.

Al establecer conexiones con CUDI, esta organización recomienda utilizar filtros con el fin de anunciar únicamente los prefijos delegados:

2001:0448:003:508Z::/60
2001:0448:003:509Z::/60

Obteniendo un prefijo de direccionamiento, posteriormente se:

- configuran ruteadores y PC's que soporten IPv6.
- configuran túneles de IPv6 sobre IPv4 o conexiones nativas de IPv6 /ATM desde la red UNAM hasta uno o mas sitios remotos
- instalan herramientas de monitoreo para IPv6.
- Instalan aplicaciones para IPv6:
  - HTTP
  - FTP
  - Correo
  - DNS
  - Seguridad (IPsec)

El requisito principal es contar con una dirección IPv4 válida globalmente y algún equipo que soporte IPv6 para la conexión extrema del túnel.

En cuanto al costo, no se tiene un precio para soporte, delegación de dominios y direcciones pues se debe enviar el registro vía World Wide Web.

Si se elige la opción de la configuración IPv6 no se necesitaría contratar un enlace a Internet, puesto que los servicios de RedUNAM pueden incluir Internet. De esta forma también se pueden aceptar conexiones del protocolo IPv4.

Para la parte del enlace a la delegación Xochimilco, se tendría que hacer una configuración 6to4 como la que se menciona en el apartado 5.10.3.

7.2.2. Cableado estructurado

Se necesita tener un estándar para el tipo de cable, conectores, jacks, rosetas y sobretodo una canaleta para la protección del cable de posibles campos magnéticos, golpes, rasguños, jalones, etc. Se recomienda cableado Categoría 6 que recientemente se liberó en su estándar y además conectores RJ-45 para este tipo de cable pues es diferente a la categoría anterior (Cat 5E).

La administración de la delegación afirma que se tiene contemplado la posibilidad de cablear tres oficinas mas, con 5 o más computadoras por cada una, por lo que se necesita la compra o arrendamiento de este equipo además de switches.

El cableado se encontrará en el rack de aluminio que ya posee la institución. Los paneles de parcheo contendrán las conexiones hacia los switches o computadoras, según sea el caso.

Este cableado tiene 4 pares sin recubrimiento metálico. Es empleado para transmisiones LAN de alta velocidad. Este producto proporciona máxima seguridad en el sistema de cableado estructurado.

Soporta los siguientes estándares: IEEE 802.3 Gigabit, IEEE 802.5 Token Ring, ATM 155, entre otros. Supera los requerimientos de compatibilidad electromagnética exigidos por la Normativa EN 55022 para sistemas de cableado estructurado y especificaciones de los últimos borradores (5688.2-1), para sistemas de cableado UTP Cat. 6/Clase E.

Especificación:

- ANSI / EIA / TIA 568A (Borrador Abril 1998).
- UL 444, 444 (13), EN 50173, EN 50167 (LSZH).
- UL 1581 (CM), UL 1666 (CMR), UL 910 (CMP).

Aplicaciones, supera todos los requerimientos de rendimiento para las aplicaciones existentes y las propuestas de redes de alta velocidad:

- Gigabit Ethernet, aprobada por el comité de la IEEE 802.3ab (1000BASE-T).
- 622 Mbps y 1.2 Gbps ATM.
- Video de banda ancha análogo y digital.
- Internet/Intranet.
- High-End multimedia.
- Requerimientos de ancho de banda muy altos de CAD/CAM, aplicaciones médicas, financieras/banca y aeroespaciales.

Estándar EIA/TIA568

Es un conjunto de informes técnicos donde se define los componentes a utilizar:

- TSB36A: Cables con pares trenzados 100 ohms UTP y FTP.
- TSB40A: Conector RJ45.
- TSB 53: Cables Blindados 150 ohms.

En la tabla 7.3 se describe algunas de las normas y categorías por medición de diferentes parámetros como impedancia, velocidad.

CAT 3	Hasta 16 MHz. Ethernet 10 Mbps, Token Ring 4 Mbps, Localtalk, Telefonía.
CAT 4	Hasta 20 MHz. Ethernet 10 Mbps, Token Ring 4 y 16 Mbps, Localtalk, Telefonía.
CAT 5	Hasta 100 MHz. Ethernet 10 y 100 Mbps, Token Ring 4 y 16 Mbps, ATM 155 Mbps
CAT 6	Hasta 200 MHz
CAT 7	Hasta 700 MHz.

Tabla 7.3. Categorías de cableado de par trenzado

Norma 568

Esta norma define la forma de conexión y distribución de los pines dentro de jacks y plugs para el cableado. En la figura 7.4 se muestra la numeración de los pines.

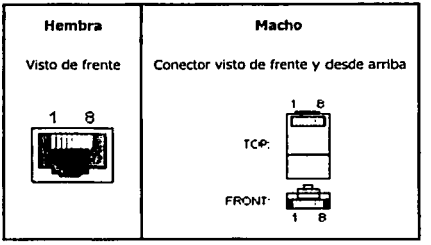


Fig. 7.4. Numeración de pines para plug RJ-45

Norma EIA 568A

Esta norma muestra como deben de organizarse los hilos del cable par trenzado dentro del plug RJ-45, según se muestra en la tabla 7.5.

1	T3-Blanco Verde	5	T1- Blanco Azul
2	R3- Verde	6	R2-Naranja
3	T2- Blanco- Naranja	7	T4-Blanco Naranja
4	R1- Azul	8	R4-Marrón

Tabla 7.5. Norma EIA 568A

Norma EIA 568B (258A)

Norma que define la distribución de hilos dentro el plug RJ-45 (tabla 7.6).

1	T2-Blanco Naranja	5	T1- Blanco Azul
2	R2-Naranja	6	R3- Verde
3	T3-Blanco Verde	7	T4- Blanco Marrón
4	R1-Azul	8	R4- Marrón

Tabla 7.6. Norma EIA 568B

Cableado ISO/IEC 11801

Norma que define una instalación, sus componentes y conexiones por parte de cableado estructurado. La tabla 7.7 define tipo de aplicaciones.

Clases	Aplicaciones
Class A	Aplicaciones de baja frecuencia y/o voz, hasta 100 Khz.
Class B	Aplicaciones de Datos a baja velocidad, hasta 1 Mhz
Class C	Aplicaciones de Datos de Alta velocidad hasta 16 Mhz.
Class D	Aplicaciones Datos Alta velocidad hasta 100 Mhz
Class E	Aplicaciones Datos Alta velocidad hasta 200 Mhz.
Class F	Aplicaciones Datos Alta velocidad hasta 700 Mhz.
Optical	Todas según longitud de onda.

Tabla 7.7. Aplicaciones para cableado

Partiendo de las cotizaciones hechas por las empresas, se presenta una tabla comparativa (tabla 7.8) de los honorarios de éstas.

Compañía	Descripción de servicio	Costo Unitario	Incluye
Cableado A	Cambio de cableado por nodo	464 pesos	• Cable cat. 5, el necesario • Parcheo en la terminal del usuario • Parcheo en el rack de datos • Cableado por ductos locales • Identificación de nodos
	Orden de servicio 1 hora	800 pesos	• Cambio de lugar de nodos de voz o datos ó • Levantamiento de instalación de materiales requeridos ó • Reparaciones de nodos instalados de voz y datos ó • Instalación de ductos • No incluye tapas, cable, paneles, jacks, conectores, etc. • En paquete de nodos a instalar 30% de descuento
Cableado B	Cambio de cableado por nodo	980 pesos	• Instalación de nodo sin materiales • Prueba de buen funcionamiento de nodos • Activación y desactivación del nodo • Cambio de nodo de la red • Reubicación del nodo
Cableado C	Cambio de cableado por evento	880 pesos	No incluye materiales
Cableado D	Cableado estructurado por nodo	1000 pesos	• Cable cat. 6 • Material, accesorios, canalización • Memoria técnica • Prueba de scanner
Costos + IVA			

Tabla 7.8. Comparación de proveedores

Todas las empresas tienen condiciones de pago propias. Se debe considerar que toda cotización tiene una vigencia. Al igual que en las propuestas de enlaces y hardware.

En definitiva, la mejor opción es la empresa D porque incluye la categoría 6 en el cableado y memoria técnica que ninguna otra compañía lo ofrece, recalcando que es un material demasiado importante para futuras revisiones, o bien, nuevas instalaciones.

7.2.3. Enlaces dedicados

Si no se desea contratar el servicio de Internet con RedUNAM, se debe realizar una configuración 6to4 y así contratar el enlace a Internet con algún otro ISP pues solo se cuenta con 64 Kbps, se aconseja para el número de usuarios, que se amplíe por lo menos a 512 Mbps puesto que solo se ocupa para servicios de navegación por http y correo (smtp).

Para el enlace dedicado al Centro Histórico se aconseja se aumente a 512 Mbps, como mínimo, puesto que la información que más tiene valor es el que se transmite por este enlace.

En la tabla 7.9 se encuentran los costos del enlace dedicado a oficinas de Centro Histórico y de acceso a Internet a través de diferentes compañías. Cabe señalar que en aquellas compañías que no aparece el precio del descanalizador, significa que la señal se entrega descanalizada. En la compañía 2 el costo de este equipo puede ser por arrendamiento por 75 USD mensuales.

ENLACE DEDICADO CON COMINICACION CON DDF (Centro Histórico) 512 Kbps		COMPAÑÍA -- ENLACE 1	COMPAÑÍA -- ENLACE 2	COMPAÑÍA -- ENLACE 3	COMPAÑÍA -- ENLACE 4	COMPAÑÍA -- ENLACE 5
CONCEPTO	PAGO A 60 MESES	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL
Internet corporativo 256	Mensual	$ 14,152.00	$ 14,025.00	$ 16,830.00	$ 13,260.00	$ 12,750.00
Gastos de instalación	Único	$ 43,000.00	$ 40,000.00	$ 38,000.00	$ 45,000.00	$ 45,000.00
	Total	$ 19,548.00	$ 21,945.00	$ 11,939.00	$ 9,434.00	$ 20,440.00

ENLACE DEDICADO CON SALIDA A INTERNET 512 Kbps		COMPAÑÍA 1	COMPAÑÍA 2	COMPAÑÍA 3	COMPAÑÍA 4	COMPAÑÍA 5
CONCEPTO	PAGO A 60 MESES	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL
Internet corporativo 512	Mensual	$ 15,791.60	$ 14,430.00	$ 17,371.00	$ 14,498.00	$ 13,000.00
Descanalizador	Único	$ 9,631.00	$ 11,150.00	$ -	$ -	$ 9,700.00
	Total	$ 25,422.60	$ 25,580.00	$ 17,371.00	$ 14,498.00	$ 22,700.00

Tabla 7.9. Costos para instalación de enlaces dedicados

Si se desea cambiar de proveedor, las compañías 3 y 4 absorberían los gastos de penalización por cancelación de contrato antes de la fecha de terminación del contrato. Esta última compañía, su fuerte es la ingeniería de software por lo que no se recomienda. La compañía 5 tiene muy poca infraestructura y la gente de este departamento solo va a sus labores 3 veces a la semana, por tanto, no se recomienda contratar el servicio con esta empresa. Así, la decisión se inclina por la primera pues es menor el costo del descanalizador.

7.2.4. Hardware y software

Para cuestión de un mejor performance de la red es importante cambiar la mayoría de los concentradores por switches, de preferencia cambiar los concentradores que tengan mas de 8 puertos conectados a los clientes y como caso ideal, cambiar los cables mas cortos al switch principal por fibra óptica, además de realizar una reorganización de las conexiones para los switches.

Es importante cambiar el sistema operativo tanto de clientes como de los servidores, pues Windows 95 (clientes) no fue diseñado para trabajar con redes (no incluye soporte IPv6), para poder trabajar con más comodidad en redes se necesita migrar a Windows 2003 Server como controlador primario; se necesita Windows XP Professional para los clientes pues este último tiene el soporte necesario para la configuración de IPv6, además de incluir mejores comandos y herramientas para la administración y monitoreo de los equipos.

El proceso que se tiene que seguir para la compra de equipo es por medio de una licitación pública, es decir, se anuncia públicamente que la dependencia del gobierno va a adquirir equipo, invitando a las empresas en el ramo a participar en un concurso para la adjudicación del contrato de compra venta de bienes y servicios. Las organizaciones se dan por enterados comprando las bases del concurso y de este modo concursan tratando de cumplir con los requerimientos del contrato que lleva las especificaciones técnicas y detalles de lo que se requiere.

Se recomienda un arrendamiento puro pues consiste, a grandes rasgos, en una renta mensual más baja que en el arrendamiento financiero. En este último no conviene comprar el equipo pues al final del contrato se vende el equipo mas caro que en el arrendamiento financiero.

Por lo tanto, solo se puede hacer una sugerencia del equipo que se debe arrendar tratando de aprovechar el contrato que anteriormente se tenía:

- PC x86:
  - Disco duro 40 GB.
  - Memoria de 256 MB.
  - Procesador x86 a 2 GHz.
  - Windows XP Professional.
- Switch:
  - CISCO Catalyst 2950 G.
- 3 Licencias Windows 2003 server.

7.3. Diseño de red

En el punto anterior se mencionó que es importante una reorganización para las conexiones de los nuevos switches puesto que tienen un concentrador – hijo o porque su información es prioritaria a transmitirse. Por lo que se recomienda cambiar los concentradores por switches CISCO Catalyst 2950 G de los siguientes departamentos como mínimo:

- CESAC – Ventanilla 1.
- CESAC – Ventanilla 2.
- Contraloría Interna.
- Pagos.
- Recursos Financieros.
- Recursos Materiales.
- Subdirección Obras 1.

Además se nos solicitó de manera temporal que se reestructura la red con dos switches 3Com SUPERSTACK 3 4400 de 24 puertos cada uno, que adquirieron recientemente pero no saben como distribuir y organizar los concentradores en cascada con estos dispositivos (para balancear la carga de transferencia de información). Todo esto hasta que se aprobara con todo el proyecto y se reemplazaran concentradores por switches. No se recomienda comprar los switches a reemplazar pues los switches CISCO arriba mencionados tienen mejores características que el modelo 3Com SUPERSTACK 3 4400. Algunas de sus debilidades son las siguientes:

- Esta plataforma esta limitada en apilar hasta ocho unidades y no soporta switch clustering, por lo que cada dispositivo debe ser administrado individualmente.
- La implantación del QoS del SuperStack no permite a los administradores la prioridad dentro del tráfico además de asignar el ancho de banda, particularmente en redes que soportan la telefonía IP.
- Los productos de la familia SuperStack proveen limitada protección a la inversión hecha, puesto que estos modelos no pueden conectarse con los modelos 3300/4300 empleando interfases de stacking. Por lo que los módulos 1000BASE-T y SX no pueden ser compartidos entre switches.
- Sin filtro de seguridad, notificación de direcciones MAC, y Secure Shell (SSH), los modelos SuperStack no entrega la seguridad de la red LAN necesaria para prevenir amenazas internas.

En la figura 7.10 se muestra la reestructuración que se necesita para tener un mejor desempeño de la red. Los switches que ya se contaban se pueden instalar en los departamentos de

Secretaría Particular y en la Subdirección de Informática como backbone de toda la red pero la solución es cambiar todos los concentradores por switches. Los cables que van a cada departamento no rebasan los 100 metros, por lo que no se está pasando por alto las restricciones de la norma de este tipo de cable.

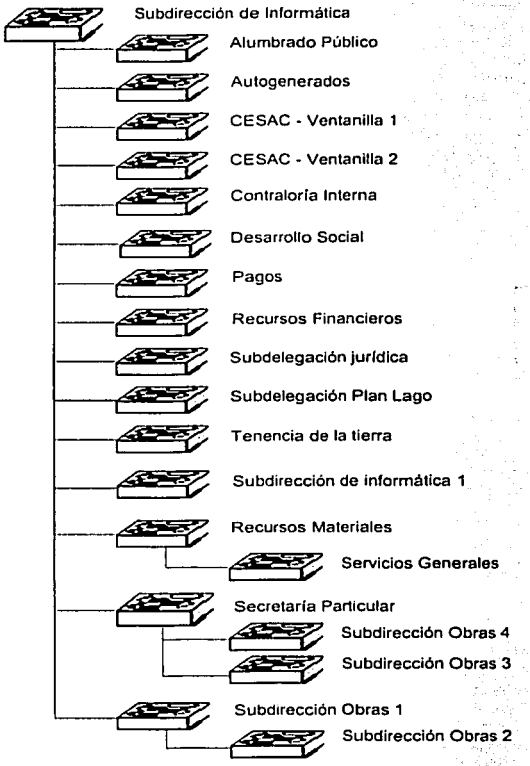


Fig. 7.10. Organización de switches para red de la delegación Xochimilco

7.4. Características de la red

Conforme a lo anteriormente mencionado en los puntos anteriores, las características de la red propuesta son:

- Red Fast Ethernet, estándar 802.3 de IEEE:
  - Velocidad de 100 Mbps.
  - Topología de bus conectado en estrella.
  - 200 PC's y sistema operativo Windows XP Professional para el mejor funcionamiento de las aplicaciones y direccionamiento con las siguientes características:
    - Disco duro 40 GB.
    - Memoria de 256 MB.
    - Procesador x86 a 2 GHz.
    - Windows XP Professional.
  - 18 Switches CISCO Catalyst 2950 G de 24 puertos para mejorar el rendimiento de la red. Características:
    - Tecnología EtherChannel que agrupa lógicamente grupos de puertos para incrementar el ancho de banda.
    - La seguridad de cada puerto previene, a usuarios no autorizados, el acceso a red limitando el número de direcciones MAC permitidas por puerto. La notificación de direcciones MAC comunica al administrador la adición de nuevos usuarios o eliminación de ellos.
      La limitación de la velocidad asegura la apropiada cantidad de ancho de banda para cada usuario, permitiendo a los administradores priorizar el tráfico a ciertos usuarios.
      Mejores caracteritcas en la administración con el software CMS: mapas de topología, gráficos de enlaces y reportes de actualizaciones en tiempo real, plantillas de configuración para evitar el entrenamiento. Este software esta incluido en el switch, no necesita ser instalado. Se consulta desde un navegador Web

- Cableado categoría 6,
  - plugs y jacks categoría 6,
  - Cableado listos para entrar a velocidades de 1 Gbps.
  - Además de memoria técnica para futuras modificaciones y nuevas instalaciones.
  - Estándares:
    - IEEE 802.3ab (1000BASE-T).
    - IEEE 802.5 Token Ring.
    - ANSI / EIA / TIA 568A (Borrador Abril 1998) entre otras.
- Direccionamiento IPv6:
  - Mayor número de direcciones.
  - Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
  - Proporciona una infraestructura segura sobre la cual se pueden realizar transacciones usando cualquier aplicación.
  - Autoconfiguración.
  - Calidad de Servicio.
  - Multicast y Anycast.
  - Aplicaciones de telefonía IP, Videoconferencia de mejor calidad.
- Enlaces dedicados de 512 Mbps para enlace a Internet y a Centro Histórico mejorando la velocidad de transmisión de datos.
- Tres servidores con sistema operativo Windows 2003 Server.

En la figura 7.11 plano se muestra la ubicación de los nodos en un plano general de la delegación Xochimilco.

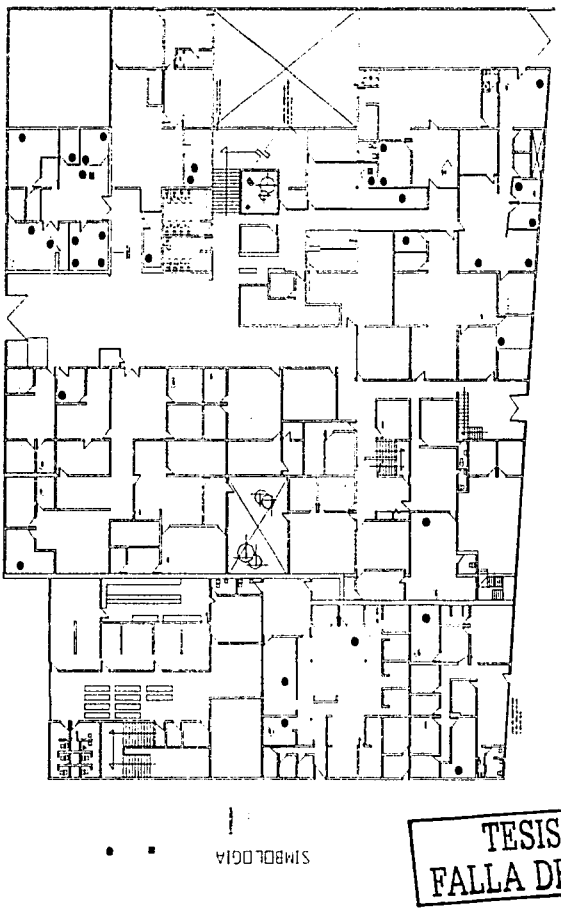


Fig. 7.11. Ubicación de nodos dentro de las instalaciones de la delegación Xochimilco

7.5. Servicios de la red local

Si bien se han expuesto las características de la red, ahora se listarán servicios que se incluyen en la red:

- Políticas de seguridad, ejecución e instalación de programas, instalación de hardware, de tal forma que se administre adecuadamente los clientes, estos, relacionadas con las cuentas de usuario.
- Administración de equipos y usuarios.
- Correo electrónico (cuentas relacionadas con las cuentas de usuarios para una mejor administración).
- Administración remota, conectándose directamente a la computadora y resolver problemas tomando el control de la computadora empleando programas específicos incluidos en el sistema operativo de los clientes, simplificando las tareas al área de soporte.
- Ejecución de programas en la autentificación de la red para instalar agentes como: antivirus, o control remoto.
- Compartimiento de recursos: unidades de CD, unidades de almacenamiento ZIP, impresoras, discos duros, scanners.
- Servicios de impresión, si se cuenta con tarjetas de red para las impresoras.

7.6. Costos

Los costos de acuerdo a las necesidades se presentan en la tabla 7.12.

Empresa	Descripción	Cantidad	Costo Unitario	Características	Total
Compañía enlace 5	Enlace dedicado con comunicación con DDF (Centro Histórico)	1	12,750 pesos pago mensual + 45,000 pesos por gastos de instalación	Incluye soporte los 365 días del año y configuración	57,750 pesos
Compañía enlace 1 (si no se contrata con RedUNAM)	Enlace dedicado con salida a Internet a 256 Mbps	1	9,631 pesos + pago mensual de 9,917 pesos	Incluye soporte los 365 días del año y configuración	19,548 pesos
Cableado D	Cableado Estructurado	200 nodos	1000 pesos	Incluye: • Cable cat. 6 • Material, accesorios, canalización • Memoria técnica • Prueba de scanner	200,000 pesos
PROVEEDOR	PC	200 computadoras	6,000 pesos	Modelo Inspiron: • Procesador x86 a 2 GHz • 256 MB en memoria • Monitor • CD-ROM • Tarjeta de video y sonido integradas • Windows XP Professional • 1 año de garantía	1,200,000 pesos
Microsoft	Licencia de	3	11,000 pesos		33,000 pesos

	Windows 2003 Server con 5 clientes				
Microsoft	Licencia para cliente de Windows 2003 Server	185	2000 pesos		370,000 pesos
PROVEEDOR	Switch CISCO Catalyst 2950 G	18	15,675 pesos		282,150 pesos
Gustavo Rodrigo Sánchez Vélez	Honorarios		30,000 pesos	Supervisión de la instalación de todo el proyecto con debida documentación	40,000 pesos
				Total	**2,202,448 pesos**

Tabla 7.12. Costos del proyecto

Todo lo anterior depende, como se dijo, de la licitación, aquí se muestra una propuesta pero la decisión tal vez no dependa de la Subdirección de Informática.

Del costo total falta aumentar los correspondientes al direccionamiento por medio del grupo de IPv6 de DGSCA, de los cuales no se obtuvo respuesta para ser incluidos en esta propuesta.

7.6.1. Plan de trabajo

En esta sección se expone un procedimiento en el cual se detalla las actividades que se llevarán a cabo para la transición de equipo, software, configuración e instalación de cableado:

A. Instalación de canaletas y tubería para el cableado para toda la delegación Xochimilco.
B. Instalación de cableado dentro de las canaletas y tubería.
C. Instalación de rosetas, conexión de cableado con jacks.
D. Parcheo del cableado en el panel de parcheo.
E. Comprobación de cableado con patch cords (escaneo de cableado) en computadoras, concentradores, switches y servidores.
F. Instalación y configuración de computadoras nuevas.
G. Respaldo de información de servidores y pruebas de recuperación de dicha información desde este respaldo.
H. Configuración con IPv6 de ruteadores, Firewall, servidores y clientes, incluyendo comprobación de conexiones, considerando que se contrate el servicio de Internet con RedUNAM.
I. Configuración del enlace dedicado con Centro Histórico y/o enlace de Internet, incluyendo pruebas.

En la tabla 7.13 muestra el esquema Trabajo – tiempo especificando cuanto tiempo se cada una de las actividades mencionadas anteriormente.

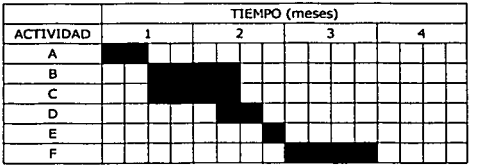


Tabla 7.13 Esquema Trabajo -- Tiempo

CONCLUSIONES

De acuerdo a la investigación con el personal de la Subdirección de Informática de la delegación Xochimilco, las necesidades de comunicación y de velocidad de transmisión de datos son bastantes, mejor performance de la red, "caídas" en el servicio de conexión con los concentradores y por consiguiente con el servidor, tiempos de respuesta grandes, combinación de categorías dentro el cableado y falta de un estándar para la instalación de éste, sistemas operativos que han dejado de ser funcionales para aplicaciones basados en comunicación dentro de redes, etc. Como consecuencia de toda la anterior problemática se justifica el gran cambio en la infraestructura (cableado, equipo de cómputo y comunicaciones), configuración (IPv6) y la velocidad de transmisión de información por medio del enlace privado y de Internet.

El avance de la tecnología es significante a medida que pasa el tiempo y más rápido en la última década. Existen nuevas necesidades de comunicación y por tanto se necesitan el cambio de equipos para estos requerimientos.

Aunque la categoría 5E del cableado de par trenzado soporta la configuración 1000BASE–T con velocidades de 1 Gbps, el cableado categoría 6 también la soporta, además que se desarrollarán aplicaciones que aprovecharán su performance. Por tanto, el cableado, es en gran parte un factor indispensable para tener una estabilidad en el performance de la red.

Desafortunadamente el costo de esta tecnología es elevado, pero se tiene la seguridad que puede servir, por parte del cableado, tal vez 10 años. Las computadoras es el equipo que mas deprecia año tras año pero de la misma forma se puede conseguir un buen equipo a bajo costo. En cuanto al equipo de comunicaciones (ruteadores, switches) tardan en ser obsoletos pero cada día soportan nuevas tecnologías de transmisión.

IPv6 es el futuro próximo de las comunicaciones, ya existen IP phones, se esta trabajando en el desarrollo de VoIPv6, Videoconferencia, QoS, Firewalls, entre otras muchas aplicaciones que harán de las Telecomunicaciones una herramienta mas estable. Además de tener mejor calidad en todos estos servicios gracias a las simplificaciones que se han hecho al nuevo protocolo.

Un enlace de mayor velocidad ayudará a tener mejor tiempo de respuesta, traducido para el personal administrativo en menor tiempo para recolectar datos y procesarlos rápidamente en el Centro Histórico.

El camino es largo en cuestión de aplicaciones, pero una vez que se establezca un estándar en las organizaciones se podrá correr en el desarrollo de las mismas.

La integración de switches como backbone de la red local tiene un significado de estabilidad en la comunicación entre los diferentes dispositivos que la conforman. En este tiempo, los diseñadores de redes recomiendan integrar switching en las redes locales, como solución para ampliar en ancho de banda de forma económica y con una migración relativamente sencilla, sin considerar el cableado y el costo. De esta forma se reduce la congestión en el tráfico de transmisión de datos y mejorando por mucho el tiempo de respuesta, el desarrollo de las nuevas aplicaciones cliente – servidor ya mencionadas, aprovechar el incremento de la velocidad en las estaciones de trabajo, utilización de redes virtuales, acceso remoto a computadoras, instalaciones de software programadas, etc.

En cuanto a la administración, el sistema operativo propuesto mantiene a cuentas de usuarios que pueden ser separadas por grupos con políticas bien definidas como: la ejecución de

ciertos programas, permisos para instalación de paquetes, opciones para la configuración de estaciones de trabajos así como permisos para acceso a los recursos de las computadoras. Así mismo se puede delimitar el horario y días en los que puede trabajar una cuenta dentro del dominio, si se encuentra dentro de los límites de horario, simplemente no accederá a los recursos de la computadora, o bien, puede destinarse cierta cuenta a un solo equipo.

Desafortunadamente como toda la familia de Microsoft tiene y tendrá huecos de seguridad, para resolver este problema el administrador de la red tendrá que estar al tanto de las actualizaciones y parches que se liberen. Este sistema operativo contiene la administración de protocolos como DNS como servicio de nombres de dominio, DHCP para asignación dinámica de direcciones IP y para SNMP para comunicar información administrativa entre los agentes de nodos administrados y nodos administradores. También se puede monitorear cada computadora que se encuentre dentro del dominio de red: Desactivar, eliminar o restringir una computadora del dominio son algunas de las acciones que pueden aplicar con el fin tener cierta seguridad en la información contenida en los equipos de cómputo.

Con la separación de transmisión de datos al Departamento del Distrito Federal al Centro Histórico, y el acceso a Internet cambiará notablemente el rendimiento de la red gracias a la velocidad de 512 Kbps por cada enlace y el tráfico se divide por dos canales diferentes, es aquí donde el ruteador realiza su labor de encaminamiento de información.

En cuanto a la transición de actividades, es decir, a la migración en las actividades referidas en el esquema trabajo – tiempo, es posible hacerlas gradualmente, se expuso en un tiempo de 3 meses y una semana para cambiar radicalmente la infraestructura, configuración, etc., de toda la delegación. Pero puede retrasarse si la disposición del personal de la Subdirección de Informática planea actividades dentro de este plan.

Es una propuesta integral que no se necesita llevar a cabo en este periodo de tiempo, sin embargo se debe tomar en cuenta como una solución real. Las aplicaciones cliente – servidor y la tecnología que se va presentando día a día, son cada vez mas orientadas a Internet y por consiguiente se necesitará una reestructuración en el direccionamiento IPv6.

En cuánto al mantenimiento de la red, es necesario hacer respaldos periódicos, revisar rutinariamente el espacio en disco de todos los servidores, el espacio que se mantiene en los buzones de usuarios del servidor de correo, probar todos los cables de red por lo menos dos veces al año con un probador.

Por lo que a clientes se refiere, mantener actualizados los clientes con los parches y service packs del sistema operativo, revisar el tamaño de los archivos personales de correo (PST) cada tres meses, hacer una limpieza cada tres meses del equipo físicamente, depurar archivos temporales de aplicaciones.

BIBLIOGRAFÍA

- Jenkins, Neil; Schatt, Stan. "Redes de área local (Lan)". Prentice Hall Hispanoamericana. México, 1996.
- Derfler, Frank. "Descubre redes LAN & WAN". Prentice may. México, 1998.
- Hadrón, Thomas. "Redes de área local: La siguiente generación". Megabyte: Noriega. México, 1992
- Parrilla Peláez, Juan Carlos; Rubio Carretero, Juan José. Redes de área local. Síntesis. Madrid, 1996.
- Rodríguez, Jorge. "Introducción a las redes de área local". McGraw-Hill. México, 1996.
- López Rubio, Gustavo; Piñeiro Noguera, Jesús. "Redes de área local: fundamentos, implementación (hardware y software), conectividad y administración". Ciencia 3. Madrid, 1998.
- Estevez Domingo, Manuel; Guerra Cebollada, Juan Carlos; Palua Salvador, Carlos. Universidad Politécnica de Valencia. Valencia, Italia, 1999
- Huidobro Moya, José; Blanco Solsona, Antonio. "Redes de área local". Paraninfo. Madrid, 2001.
- Nunemacher, Greg. "Introducción a las redes de área local". Paraninfo. Madrid, 1999.
- Loshin, Peter. "IPv6 clearly explained". Boston, 1999.
- Huitema, Christian. "IPv6: The New Internet Protocolo Protocol". Prentice Hall, 1998.
- Raya Cabrera, José Luis; Raya Pérez, Cristina. "Redes locales y TCP/IP". Alfaomega. México, 1997
- Martin, James. "TCP/IP networking: architecture, administration, and programming". Prentice-Hall. Englewood Cliffs, New Jersey, 1994
- Cacique Valadez, Agustín; Velázquez Arellano, Jorge Alberto. "Aprendiendo TCP/IP en 14 días". Prentice-Hall. México, 1997
- Raya Cabrera, José Luis; Raya Pérez, Cristina. "Redes locales y TCP/IP". Ra-Ma. Madrid, 1995.

REFERENCIAS WEB.

- CISCO SYSTEMS. http://www.cisco.com. Consultado Febrero 2003.
- Equipo 3com. http://www.3com.com. Consultado Mayo 2003.
- Cableado Panduit. http://www.panduit.com. Consultado Febrero 2003.
- Foro Internacional IPv6. http://www.ipv6forum.com. Consultado Septiembre 2003.
- Empresa privada con Ipv6 nativo. http://www.renater.fr. Consultado Septiembre 2003.
- Empresa de telecomunicaciones. http://www.consulintel.es. Consultado Septiembre 2003.
- Organización para los estándares en tecnologías de comunicación. http://www.ietf.org. Consultado Febrero 2003.
- Página de especificaciones de estándares RFC. http://www.rfc-editor.org. Consultado Febrero 2003.