33
24.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS ARAGON

ANALISIS COMPARATIVO ENTRE RUTEADORES Y LAN SWITCHES PARA APLICACIONES LAN/WAN.

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICISTA
P R E S E N T A N :

JORGE ESPINOZA DE LOS MONTEROS REBOLLEDO
JORGE VILLEDA CHAVERO

ASESOR: ING. DAVID ESTOPIER B.

EDO. DE MEXICO. OCTUBRE 97

Agradecimientos

Nos encontramos rodeados con muchas personas que han contribuido de una u otra forma en la realización de estos apuntes.

A Dios que le debemos el ser y el estar aquí ... Gracias.

A nuestros padres que sin ellos no solo no hubiéramos terminado, sino que ni siquiera hubiéramos empezado, por ello y por todos los esfuerzos que han hecho para poder terminar nuestros estudios... Gracias.

A los Ingenieros de PEMEX Ing. Carlos Acevedo Z. Ing. Víctor Pérez. Act. Alfonso R. Ing. Rosendo Palma. Ing Miguel Aguayo. Tec. Rafael Crespo. Tec. Alberto Carreno. Tec. Antonio Becerra. Ing Daniel Aguilera. y a todas las personas que laboran en el depto de transmisión de datos: Por su atención para recabar todas nuestras dudas en la realización de estos apuntes... Gracias.

Al Ing. Daniel Estrépin B., por su paciencia, orientación, asesoría y revisión de estos apuntes... Gracias.

A los profesores Ing. Raúl Barrón V., Ing Narciso Acevedo H., Ing.Juan Garibaldi P., y al Ing. Daniel Tenda P. por la revisión de los apuntes... Gracias.

A nuestros amigos Adrián. Edgar. Ulises. Ismael. Chacobo. Raul. Juan Carlos y Ernesto. porque juntos hemos pasado los momentos más felices en la Universidad.

A la Universidad Nacional Autónoma de México. con la que siempre estaremos en deuda... Gracias.

Jorge & George.

Dedico este trabajo:

A Alberto, mi Papá
Por ser el mejor ejemplo que puedo seguir en todos los sentidos. Además de haberme dado lo que soy. Te quiero.

A Concepción, mi Mamá
Todos los días me enseñaron los caminos, pero tu me enseñaste a caminar. Te quiero.

A La Familia Espinoza de los Monteros Rodríguez, Verónica y Alfonso
Ya que han sido un ejemplo, además de que siempre me han apoyado incondicionalmente y sobre todo por la confianza que siempre han mostrado para conmigo.

A La Familia Doctores Manuel Espinoza de los Monteros, Laura, Julio y Doctor
Por que siempre han estado ahí, cuando necesito hablar, además del apoyo que siempre me han brindado.

A mis Hermanos Gerardo y Alberto
Porque sin darse cuenta también han sido un ejemplo para mí.

A Luisa
Por toda la Comprensión, Apoyo y Amor que siempre me has brindado incondicionalmente.

A Jorge Villada Chavez
Por el buen compañero y sobre todo, buen amigo que puede ser.

A mis Amigos
Guille, Sonia, Toño, Adriana, Bony, Willy y muy especialmente a Lovy
Por ser los mejores amigos que alguien puede tener.

A mis tíos Sergio y Gumaro, Pedro y Ma. Elena, Benito y Beatriz
Por ser una familia con la que se puede contar de una forma bastante especial

A mis Primos Paty, Mayra, Erika, Pastor, Mono, Angélica y Paco y muy especialmente a Claudia, Diana, Edith, Estéb, Angel y Alan a quienes espero sirva en un buen ejemplo.

Jorge Espinoza

Dedico esta tesis:

A mis Padres
Con respeto y cariño por su apoyo y confianza.

A mis hermanos
Felix, Juan Carlos, Graciela, Martha, Lourdes y Patricia.
Gracias por haber estado conmigo en todo momento y que de una u otra forma colaboraron para lograr esta meta, esperando corresponderles de la misma manera.

A la familia Ruiz Villada. Margarita, Tacho y con mucho cariño a mi sobrino Daniel esperando poder ser un buen ejemplo.

A mi compañero de tesis Jorge Espinoza
Con quien he formado un buen equipo de trabajo mostrando dedicación y empeño.

Y en especial a Abigail Pardo Díaz
Por su Amor y Apoyo incondicional.

Jorge Villada.

ÍNDICE Pag.

Índice.

OBJETIVO:

Con esta tesis se pretende dar a conocer un estudio acerca de las técnicas de conectar redes de datos a altas velocidades las cuales son por medio de LAN Switches y Ruteadores , este estudio se va a enfocar a hacer una comparación entre ellas, tratando de obtener información suficientemente confiable que nos permita instalar lo que más convenga a las necesidades de la red y al presupuesto que se tenga destinado para hacer nuestra red más rápida y más confiable en la transmisión de información.

INTRODUCCIÓN.

Los logros tecnológicos dentro de la industria de las comunicaciones han sido significativos, en la mayoría de los complejos industriales, universidades e instituciones financieras, existe la necesidad de intercambiar una amplia gama de servicios disponibles hoy en día, tales como audio, imagen y sobre todo la transmisión de datos, estas necesidades obligan a inversiones cada vez mayores en equipos y sistemas que procesen la información lo mas rápido posible no importando cual sea el origen y destino de ésta.

Ésta tendencia a crecer rápidamente ha forzado a crear infraestructuras confiables para consolidar y permitir el adecuado intercambio de información entre los usuarios, que harán uso de esa infraestructura, por lo que las empresas o lugares donde existe ésta demanda de servicios, buscan diferentes ofertas en equipos que satisfagan adecuadamente las necesidades de comunicación, considerando, por supuesto, que el producto se seleccione de acuerdo a los objetivos de la empresa, buscando que el rendimiento sea el adecuado, así como el costo y la posibilidad de crecimiento en el futuro.

La fabricación de equipos de comunicaciones es una industria dinámica, lo que significa que día a día esta innovando con tecnología cada vez más avanzada y que a su vez presenta una mayor calidad en sus productos, lo que ha generado una gran competencia entre productores, con nuevas ideas y diseños tecnológicos, en el gran mercado de las telecomunicaciones.

Aun cuando existen muchos elementos que constituyen una red de comunicación de datos, en este trabajo nos enfocaremos a estudiar solo dos componentes que son el Ruteador y el LAN Switch (Conmutadores informáticos) que en esencia su función dentro de una red es la misma, pero como lo vamos a ver a lo largo de el trabajo cada uno tiene su características que lo hacen más conveniente que el otro para algunas aplicaciones y menos para otras, por ejemplo, debemos hacer notar que uno

OBJETIVO:

Con esta tesis se pretende dar a conocer un estudio acerca de las técnicas de conectar redes de datos a altas velocidades las cuales son por medio de LAN Switches y Ruteadores , este estudio se va a enfocar a hacer una comparación entre ellas, tratando de obtener información suficientemente confiable que nos permita instalar lo que más convenga a las necesidades de la red y al presupuesto que se tenga destinado para hacer nuestra red más rápida y más confiable en la transmisión de información.

INTRODUCCIÓN.

Los logros tecnológicos dentro de la industria de las comunicaciones han sido significativos, en la mayoría de los complejos industriales, universidades e instituciones financieras, existe la necesidad de intercambiar una amplia gama de servicios disponibles hoy en día, tales como audio, imagen y sobre todo la transmisión de datos, estas necesidades obligan a inversiones cada vez mayores en equipos y sistemas que procesen la información lo mas rápido posible no importando cual sea el origen y destino de ésta.

Ésta tendencia a crecer rápidamente ha forzado a crear infraestructuras confiables para consolidar y permitir el adecuado intercambio de información entre los usuarios, que harán uso de esa infraestructura, por lo que las empresas o lugares donde existe ésta demanda de servicios, buscan diferentes ofertas en equipos que satisfagan adecuadamente las necesidades de comunicación, considerando, por supuesto, que el producto se seleccione de acuerdo a los objetivos de la empresa, buscando que el rendimiento sea el adecuado, así como el costo y la posibilidad de crecimiento en el futuro.

La fabricación de equipos de comunicaciones es una industria dinámica, lo que significa que día a día esta innovando con tecnología cada vez más avanzada y que a su vez presenta una mayor calidad en sus productos, lo que ha generado una gran competencia entre productores, con nuevas ideas y diseños tecnológicos, en el gran mercado de las telecomunicaciones.

Aun cuando existen muchos elementos que constituyen una red de comunicación de datos, en este trabajo nos enfocaremos a estudiar solo dos componentes que son el Ruteador y el LAN Switch (Conmutadores informáticos) que en esencia su función dentro de una red es la misma, pero como lo vamos a ver a lo largo de el trabajo cada uno tiene su características que lo hacen más conveniente que el otro para algunas aplicaciones y menos para otras, por ejemplo, debemos hacer notar que uno

OBJETIVO:

Con esta tesis se pretende dar a conocer un estudio acerca de las técnicas de conectar redes de datos a altas velocidades las cuales son por medio de LAN Switches y Ruteadores , este estudio se va a enfocar a hacer una comparación entre ellas, tratando de obtener información suficientemente confiable que nos permita instalar lo que más convenga a las necesidades de la red y al presupuesto que se tenga destinado para hacer nuestra red más rápida y más confiable en la transmisión de información.

INTRODUCCIÓN.

Los logros tecnológicos dentro de la industria de las comunicaciones han sido significativos, en la mayoría de los complejos industriales, universidades e instituciones financieras, existe la necesidad de intercambiar una amplia gama de servicios disponibles hoy en día, tales como audio, imagen y sobre todo la transmisión de datos, estas necesidades obligan a inversiones cada vez mayores en equipos y sistemas que procesen la información lo mas rápido posible no importando cual sea el origen y destino de ésta.

Ésta tendencia a crecer rápidamente ha forzado a crear infraestructuras confiables para consolidar y permitir el adecuado intercambio de información entre los usuarios, que harán uso de esa infraestructura, por lo que las empresas o lugares donde existe ésta demanda de servicios, buscan diferentes ofertas en equipos que satisfagan adecuadamente las necesidades de comunicación, considerando, por supuesto, que el producto se seleccione de acuerdo a los objetivos de la empresa, buscando que el rendimiento sea el adecuado, así como el costo y la posibilidad de crecimiento en el futuro.

La fabricación de equipos de comunicaciones es una industria dinámica, lo que significa que día a día esta innovando con tecnología cada vez más avanzada y que a su vez presenta una mayor calidad en sus productos, lo que ha generado una gran competencia entre productores, con nuevas ideas y diseños tecnológicos, en el gran mercado de las telecomunicaciones.

Aun cuando existen muchos elementos que constituyen una red de comunicación de datos, en este trabajo nos enfocaremos a estudiar solo dos componentes que son el Ruteador y el LAN Switch (Conmutadores informáticos) que en esencia su función dentro de una red es la misma, pero como lo vamos a ver a lo largo de el trabajo cada uno tiene su características que lo hacen más conveniente que el otro para algunas aplicaciones y menos para otras, por ejemplo, debemos hacer notar que uno

Ruteador, de hecho el concepto de "internetworking" (conexión de redes con otras redes) no existiría sin los Ruteadores, ya que era la única forma de interconectar redes LAN (Local Área Network) con otras redes que estuvieran en sitios alejados.

Aun cuando los Ruteadores son una de las bases para interconectar redes estos han comenzado a ser desplazados por los Switches ya que los Ruteadores presentan en principio una desventaja muy notoria en relación a los switches y es que los Ruteadores son muy susceptibles al tiempo, como se puede notar en las video conferencias que el movimiento de la boca de la persona, no corresponde al sonido que escuchamos, otra de las desventajas es que los Ruteadores no pueden trabajar a las velocidades que en la actualidad se están manejando por ejemplo en aplicaciones ATM o FDDI, además los Ruteadores trabajan en la capa tres del modelo OSI y los Switches en capa dos (OSI) lo que significa que ahora con los Switches se pueden ignorar los headers (encabezados) de la capa tres.

Aunque existen muchas desventajas que tienen los Ruteadores en relación a los Switches, también existen muchas funciones que los Ruteadores realizan aun mejor que los Switches como por ejemplo es el manejo del tráfico de información que existe cuando las redes ya se conectan de tal forma que se consideran WAN (Wide Área Network)

Por el otro lado los LAN Switches pueden manejar un ancho de banda para la transmisión de 10 Mbps en una canal dedicado, aun cuando realmente sean medios compartidos, pero esto es transparente para el usuario Para que un Ruteador pueda manejar estas velocidades el administrador de la red tendrá que utilizar VLANS (LAN virtuales) lo cual ayuda a que si la configuración de la red requiera de algún cambio se pueda hacer por medio de un clic del mouse.

Es prácticamente imposible que nos podamos poner de acuerdo en cual de los dos es mejor para implementar en nuestra red, ya que cada uno ofrece ventajas, a la vez que presenta limitaciones, además la información que se ha obtenido acerca de los Ruteadores y de los LAN Switches ha sido precisamente de los mismos fabricantes, que por lógica y mercadotecnia va a hablar maravillas de sus productos, pero la finalidad de este trabajo es solo dar a conocer esas ventajas y desventajas de uno con respecto del otro solo para que el administrador o la persona que vaya a diseñar una red tenga la información necesaria y real para que él mismo tome la decisión de la forma en que se va a conectar su red ya sea mediante LAN Switches o Ruteadores, claro tomando en cuanta las necesidades, capacidad y presupuesto para implementar su red.[1]

[1] Cabe mencionar que algunos conceptos todavía no se alcancen a comprender en la introduccion pero en el capitulo 1 de Conceptos Generales trataremos de explicar los términos mas usados, pero que se iran entendiendo mejor a lo largo del documento.

CAPÍTULO 1

CONCEPTOS GENERALES.

1.- INTRODUCCION.

En este primer capitulo se darán a conocer algunos conceptos necesarios para entender todo lo referente a la interconexión de redes. Debido a que son muchos los conceptos que engloba todo el mundo de las redes, en este capítulo solo se ofrecerán los principales o al menos los más relevantes para el entendimiento de este trabajo. (Existen más términos que se conocerán al ir avanzando en este trabajo y de igual forma trataremos de explicarlos de tal forma que no se necesite ser un experto en el tema para comprenderlos).

1.1.- ARQUITECTURAS PARA LA INTERCONEXIÓN DE REDES.

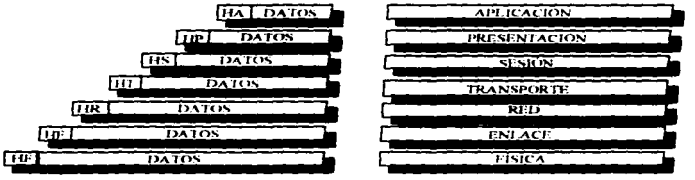
Cuando se desea interconectar computadoras en redes, se debe seguir algún modelo que nos diga como hacerlo. Existen dos modelos a seguir para la interconexión de redes, los cuales son el Modelo OSI y el Modelo DARPA.

1.1.1.- MODELO OSI.

La Organización Internacional de Estandarización (ISO) creó el modelo OSI para romper con los enormes problemas que se generaban al querer interconectar redes pequeñas con otras redes. Esto lo hizo diseñando diferentes capas y asignando responsabilidades a cada capa del modelo.

El modelo OSI esta dividido en siete capas o niveles que es tienen comunicación únicamente con sus capas contiguas para recibir o para enviar información, pero cada nivel es funcionalmente independiente de los demás.

En el siguiente diagrama se pueden ver las siete capas del modelo OSI.



LAS SIETE CAPAS DEL MODELO OSI

Las capas del modelo OSI se pueden agrupar en cuanto a su funcionalidad en tres categorías las cuales son las siguientes:

* **Servicios.-** (Son las capas de Sesión, Presentación y Aplicación). Estas capas son las que proveen los servicios de la red, al usuario , algunos de estos servicios son por ejemplo, E-Mail, Emulación de terminal, Transportación de archivos.

* **Comunicaciones.-** (Son las capas de Red y de Transporte). Juntas estas capas se encargan de hacer segura la transportación de datos ya sea recibiendo o enviando la información sin importar el nivel físico.

* **Conexión Física.-** (Son las capas Física y de Enlace). Estas capas se encargan de la conexión física entre los componentes de la red como conectores y cables con las capas superiores del modelo, y su responsabilidad es mover los datos fuera de la red y recibir los que vengan de afuera.

Estas son las funciones generales que engloban las siete capas, pero cada capa se encarga de una función específica dentro de la red. Ahora se mostrará de una forma un poco más detallada cada capa del modelo para conocer la función que desempeña.

1.1.1.1.- CAPA DE APLICACIÓN.

La capa de aplicación provee al usuario los servicios de la red. Algunos de los servicios más comunes son, como ya se mencionaron E-Mail, Emulación de terminal, Aplicaciones para la administración de la red, etc.

Contrario a la creencia popular, los protocolos de la capa de aplicación no son usados por el usuario, sino que el usuario necesita unas interfaces (software) para poder accesar a la red, lo que quiere decir que la capa de aplicación es el lugar donde se encuentra el software que utiliza el usuario y luego lo codifica en el protocolo conocido por la red.

1.1.1.2.- CAPA DE PRESENTACIÓN.

La capa de presentación es la capa que se encarga de la forma en que se va a presentar la información a la aplicación, se podría decir que es el recipiente o la envoltura en donde va la información hacia la capa de aplicación.

1.1.1.3.- CAPA DE SESIÓN.

La capa de sesión se encarga de la estabilidad de la conexión, además coordina la sincronización del dialogo entre envío y recepción de mensajes y también provee un control de la sesión de usuario.

1.1.1.4.- CAPA DE TRANSPORTE.

La capa de transporte en la responsable de la integridad de los datos, de que estos se reciban y se envíen correctamente.

1.1.1.5.- CAPA DE RED.

La capa de red es la encargada de que los paquetes de datos o tramas viajen a través de la red y sepan cual es su destino y también cual es el camino más óptimo para llegar a el, basándose en direcciones IP o mejor dicho por direcciones que se conocen por medio del software y que el administrador de la red es quien las asigna a cada usuario.

1.1.1.6.- CAPA DE ENLACE.

La capa de enlace de datos es la capa que se encarga de organizar las cadenas de bits con el número MAC (Media Access Control) en una sola trama para que la información contenga una dirección física hacia donde dirigirse, y al hacer la conexión, también provee de: sincronización entre la red y las interfaces, detección de error, "Media Access Managment and Bridging". Esta capa es el enlace entre las capas superiores que contienen los protocolos y software de la red con el medio físico de la misma red (hardware).

1.1.1.7.- CAPA FÍSICA.

La capa física describe las especificaciones físicas del medio, lo cual incluye: tipo de cable, propiedades eléctricas, capacidad para transmitir y recibir señales o propiamente dicho el ancho de banda para transmitir y recibir tramas de datos.

1.1.2.- MODELO DARPA (TCP/IP).

Este modelo esta organizado en cuatro capas conceptuales:

4.- Aplicación
3.- Transporte
2.- Internet
1.- Interfaz de red

1.1.2.1.- CAPA DE APLICACIÓN.

En esta capa se proveen aplicaciones tales como: TELNET, FTP (File Transfer Protocol) y MTP (Mail Transfer Protocol).

1.1.2.2.- CAPA DE TRANSPORTE.

Esta capa es la responsable de proporcionar comunicación entre aplicaciones residentes de diferentes HOST colocando un identificador en los bloques de la información, esta capa también permite procesar la información.

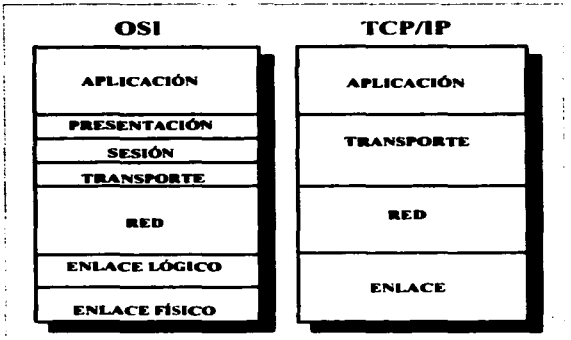
1.1.2.3.- CAPA DE INTERNET.

Esta capa corresponde a la capa de red del modelo OSI. Esta capa es la responsable de proveer la comunicación entre HOST Y HOST, es aquí donde se encapsulan los paquetes dentro de los bloques para transmitirlos dentro de la capa de Interfaz de red hacia la red que se esta conectando.

1.1.2.4.- CAPA DE INTERFAZ DE RED.

Esta capa es la responsable de transmitir los datos sobre el medio físico hasta su destino final. Esta capa correspondería a las capas de enlace y física del modelo OSI.

En la siguiente figura podemos ver las capas del modelo OSI que corresponderían a las capas del modelo DARPA.



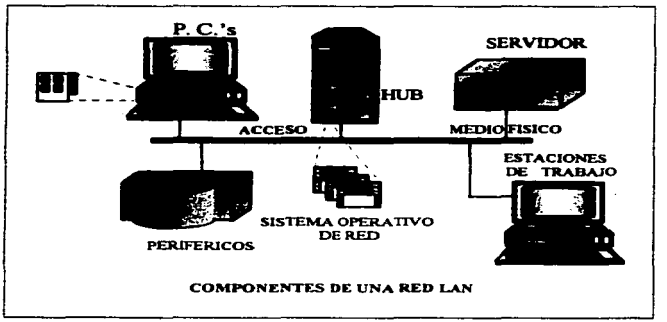
COMPARACIÓN DEL MODELO "OSI" CON "TCP/IP"

1.2 REDES LAN.

El mundo LAN nació de la necesidad de compartir recursos entre las computadoras y sus usuarios para hacer más eficiente, económico y administrable un sistema de cómputo.

La expansión de la industria de las redes locales durante los últimos seis años ha sido explosiva. Se estima que sólo en Estados Unidos existen 90 fabricantes, los cuales producen más de 100 sistemas de red local. Además de estos fabricantes de sistemas completos, otras empresas ofrecen componentes de red individuales. Son más de 250 las empresas dedicadas al negocio de redes locales y sus componentes.

La idea básica de una red local es facilitar el acceso a todos y desde todos los ETD (Equipo Terminal de Datos) de la oficina, entre los que se encuentran no sólo las computadoras, sino también otros dispositivos presentes en casi todas las oficinas: impresoras, trazadores gráficos, archivos electrónicos, base de datos, así como compartir recursos disponibles dentro de la red. La red local se configura de modo que proporcione los canales y protocolos de comunicación necesarios para el intercambio de datos entre computadoras y terminales.



COMPONENTES DE UNA RED LAN

1.2.1 ¿CÓMO DIFIERE UNA LAN DE OTRAS REDES?.

a) Tiene una configuración geográfica limitada, normalmente las distancias son menores a 3 Km., y tipicamente enlazando computadoras dentro de un edificio ú oficina.

b) Operan en ella protocolos por encima del nivel tres del modelo OSI.

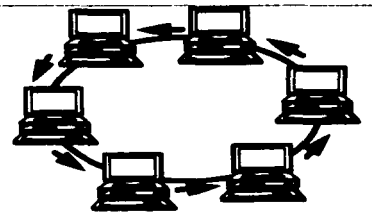
c) La operación es controlada por un sistema operativo que reside en un equipo de la red, el sistema operativo maneja la seguridad y además controla los servicios del servidor como son: Archivos (File Server), Impresión (Print Server) y Aplicaciones (Aplication Server).

Dentro de los sistemas operativos de red mas comunes se encuentran:
- NOS (Network Operating System).
- UNIX : protocolo TCP/IP.
- Novell Netware: Protocolo SPX/IPX, migrando a TCP/IP.
- Microsoft Windows NT Server: Protocolo TCP/IP o NetBEUI.
- Banyan Vines.
- Sistemas Peer to Peer: Windows for Workgroups, Lantastic.

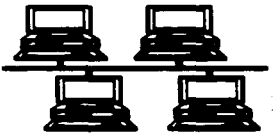
d) El medio de transmisión es compartido por todas las estaciones.

e) La transmisión es en banda base, es decir, es la transmisión de una señal analógica o digital en su frecuencia original, sin modificarla por modulación.

Ejemplos de redes LAN.



TOPOLOGÍA DE ANILLO



TOPOLOGÍA DE BUS

1.2.2 MÉTODOS DE ACCESO AL MEDIO.

Los métodos de acceso al medio donde se trabaja, forman una parte muy importante en el diseño de una red, pero cuando se trabaja en grupos hay que elegir un método que se debe de seleccionar de los demás métodos, en base a criterios que se discutieron al diseñar en un principio la red.

En el método que se va a elegir, se debe de tomar en cuenta su ancho de banda útil máxima, costo, robustez (tolerancia de falla), y sobre todo la facilidad de instalación y de mantenimiento.

Dentro de los más utilizados se encuentran los siguientes:

Bus Lineal(Ethernet 10 MB).

Bus lineal modificado (Ethernet 10 MB o Fast-Ethernet 100 MB).

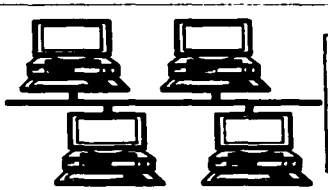
Anillo modificado (Token Ring).

1.2.2.1 BUS LINEAL (ETHERNET 10 MB).

Consiste de una línea troncal (o Bus) a la que están conectados todos los nodos. La señal viaja en ambas direcciones del cableado y es terminada en los extremos por medio de una resistencia (terminador). Es posible cablearla a través de coaxial, par torcido o fibra óptica (utilizando concentradores en las dos últimas opciones). La velocidad de conmutación es de aproximadamente 10 MBPS.

1.2.2.2 BUS LINEAL MODIFICADO (ETHERNET 10 MB, FAST-ETHERNET 100 MB).

El Bus lineal se encuentra de manera lógica dentro de un concentrador, al cual se conectan uno a uno los nodos formando una estrella. Típicamente este arreglo utiliza par torcido (UTP o STP) , siendo utilizado en redes Ethernet a 10 o Fast-Ethernet a 100 MB, dependiendo de la tecnología que maneje el dispositivo.
La ventaja principal de esta tecnología es que si una estación de trabajo falla o se desconecta, el concentrador de inmediato establece el Bus lineal, evitando así la caída de la red.



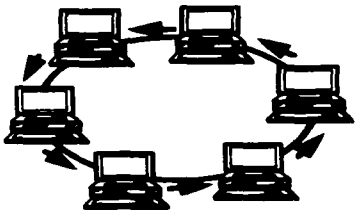
CARACTERISTICAS

ANCHO DE BANDA	10 Mbps
ACCESO AL MEDIO	COAXIAL, UTP, F.O.
ANCHO DE BANDA USADO	40 A 45 %
COSTO	DE BAJO A MEDIO
PROTOCOLOS	ETHERNET II, IEEE802.3

TOPOLOGÍA DE BUS PARA ETHERNET

1.2.2.3 ANILLO MODIFICADO (TOKEN RING).

También conocido como estrella-anillo, el anillo se encuentra dentro de un Ruteador de señal que puede ser un MAU (Multistation Access Unit), que hoy en día se está substituyendo por concentradores inteligentes, al cual se conectan uno a uno los nodos formando una estrella. La señal siempre pasa por el Ruteador. Tipicamente este arreglo utiliza cable de par torcido (UTP o STP) a 4 o 16 MBPS. La ventaja de utilizar esta topologia y no el anillo fisico es que si una estación falla o se desconecta, el concentrador de inmediato cierra el anillo evitando la caída de la red. Dentro de sus desventajas se encuentra que los equipos son de mayor costo y que por lo general no pueden haber más de 250 estaciones por LAN por causa del jitter (Leve desplazamiento de una señal de transmisión en el tiempo o en la fase).



CARACTERISTICAS

ANCHO DE BANDA	4 o 16 Mbps
ACCESO AL MEDIO	STP, UTP, F.O.
ANCHO DE BANDA USADO	75 A 80 %
COSTO	DE MEDIO A ALTO
PROTOCOLOS	IBM, IEEE802.5

TOPOLOGÍA DE ANILLO PARA TOKEN RING

1.3.- REDES MAN.

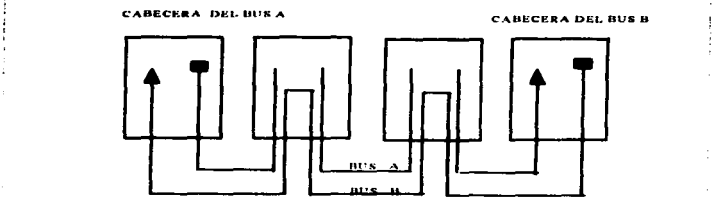
Los estándares para redes de área metropolitana (MAN) son patrocinados por IEEE, ANSI y las Regional Bell Operating Companies (RBOCs). Aunque 802.6 se diseñó inicialmente para dar soporte de servicio LAN-MAN, las compañías telefónicas la ven como una tecnología que permite la interconexión de LAN con sus oficinas centrales, e incluso la interconexión de dispositivos de conmutación telefónica.

802.6 forma la base del denominado Servicio de Datos Multimegabit Conmutado (SMDS), considerado como la solución al problema de "cuello de botella" de las WAN. En definitiva, los problemas de interconexión se solucionan con el empleo de la tecnología del estándar 802.6.

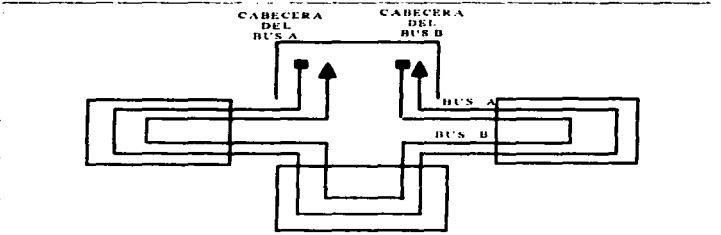
El estándar MAN se organiza en una topología denominada doble Bus doble cola (DQDB - dual queue dual Bus). Esto significa que en la topología mencionada se utilizan dos buces. Cada uno de los buces transmite tráfico en una sola dirección, la implementación de esta topología para MAN permite velocidades de transferencia entre 34 y 150 MBPS.

DQDB proporciona dos tipos de acceso. Un acceso, de servicios prearbitrados, garantiza cierta cantidad de "ancho de banda", y es útil para servicios de tipo asincrono, como voz y video. El segundo tipo de acceso, servicio arbitrado en cola, proporciona acceso basado en demanda. Esta diseñado para adaptarse mejor a servicios en ráfagas o bloques, como la transmisión de datos.

Las redes MAN proveen conectividad en distancias mayores a 50 Km., normalmente en conexiones regionales, por ejemplo dentro de un campus en una universidad o enlazando redes de edificios dentro de un corporativo grande. La red de área metropolitana se diseña en dos buces unidireccionales de fibra óptica. Cada Bus es independiente del otro en cuanto a la transferencia de tráfico. La topología se puede diseñar en Bus abierto o cerrado, como se muestra en la siguiente figura.



a) ARQUITECTURA DEL BUS ABIERTO



a) ARQUITECTURA DEL BUS CERRADO

ARQUITECTURA DEL BUS EN MAN

Las operaciones básicas del protocolo MAN se pueden resumir como sigue.

- Un nodo gana acceso colocándose en la cola (una cola para cada Bus).
- Cuando el nodo se libera, se realiza la cuenta de las solicitudes que pasan al Bus . B (contador de solicitudes).
- El contador de solicitudes se decrementa en 1 con cada ranura vacía del Bus A.

- El nodo lleva cuenta del número de requerimientos de envio y lo compara con el número de ranura vacía.
- Para enviar, el nodo pone una solicitud en el Bus B y recuerda la cuenta de ranuras.
- Enviando la cuenta de solicitudes a un contador descendente, el nodo puede determinar la ranura vacía.
- Cuando el contador llega a cero, el nodo utiliza la ranura.

1.3.1.- SMDS.

Las exigencias de un servicio de datos de banda ancha comprenden un nivel de desempeño igual al de las LAN y que admita las comunicaciones de LAN a LAN así como servicios equivalentes de LAN.

A fin de brindar comunicaciones de LAN a LAN que sean transparentes a las aplicaciones de software, un servicio de datos de banda ancha debe brindar los mismos servicios que una LAN, tal como entrega sin conexiones y servicios de multicast (Transmisión simultánea a múltiples abonados).

ATM será la tecnología que brindará las soluciones de bajo costo a estas necesidades en el futuro. SMDS es la tecnología actualmente vigente. Se trata de un servicio de datos de banda ancha ofrecido por varios proveedores de red como etapa intermedia hacia los servicios basados en células y como medio de evolucionar hacia los servicios de transmisión de datos sin conexiones por ATM. SMDS y ATM son tecnologías compatibles.

1.3.2.- ANILLO DOBLE REDUNDANTE (FDDI / CDDI)

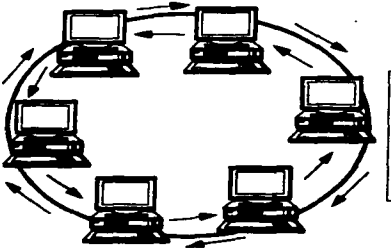
La tecnología de Anillo Doble Redundante fue diseñada para redes FDDI (Fiber Distributed Data Interface) Y CDDI (Cupper Distributed data interface) en donde se requiere de alta velocidad.

Las redes FDDI/ CDDI consisten en dos anillos de transmisión en contra sentido. El anillo primario es utilizado como canal principal. Si por alguna razón este anillo es interrumpido, el secundario restablece la continuidad del primario en forma automática, actuando como redundancia o anillo de respaldo.

Se utiliza como medio principal el cableado de Fibra Óptica y muy recientemente el cable UTP categoría 5 y cable STP.

Con esta topología se pueden alcanzar velocidades de 100 MBPS compartidos entre cada uno de los dispositivos conectados al doble anillo redundante, dentro de sus

desventajas es que no admite aplicaciones de voz o video y suele ser demasiado costoso para conexiones sencillas de PC a LAN.



CARACTERISTICAS

ANCHO DE BANDA	100 Mbps
ACCESO AL MEDIO	FIBRA OPTICA
ANCHO DE BANDA USADO	MAS DEL 80 %
COSTO	ALTO
PROTOCOLOS	FDDI

TOPOLOGÍA DE DOBLE ANILLO PARA FDDI

1.3.3.- SONET (SINCHRONOUS OPTICAL NETWORK).

La red sincrona de fibra óptica fue propuesta por "BELLCORE" y estandarizada por ANSI (Instituto Nacional Americano de Estándares). Fue diseñado para utilizar las ventajas que provee la fibra óptica en las transmisiones a altas velocidades. SONET tomará el lugar de las portadoras como la siguiente generación de transmisión a altas velocidades utilizando las facilidades que proporciona la TDM (Muliplexión por División de Tiempo).
SONET comienza su transmisión de datos a 51.84 MBPS (Llamado Portador Óptico Nivel 1 o OC-1), después subió su velocidad a un OC-48 o 2.488 Gbps con DS-0 (64 Kbps). Estas son las dos velocidades de transmisión básicas.

Ésta estructura puede soportar la próxima generación de servicios WAN, además que provee de facilidades en la transmisión a altas velocidades de conmutación de paquetes como lo es usado en ATM.
SONET provee, además, capacidad en la gestión de la red para que se incremente conforme la red, lo haga también. Esta capacidad adicional de administración será requerida cuando sea necesario soportar sofisticados servicios, como pueden ser por ejemplo, redes privadas virtuales, mayor demanda en el ancho de banda, y en servicios como la banda amplia de la Red Digital de Servicios Integrados (B-ISDN).

1.4 REDES WAN.

Durante las últimas décadas, la tecnología de Switches de paquetes ha sido dominada por X25, uno de los métodos de transmisión de comunicaciones de área amplia pioneros y más utilizados. Muchas fuentes de información describieron a Frame Relay como el protocolo de Switches de paquetes de la próxima generación. Frame Relay tiene sus orígenes en las especificaciones de la Red Digital de Servicios Integrados (ISDN) desarrolladas en los años ochenta.

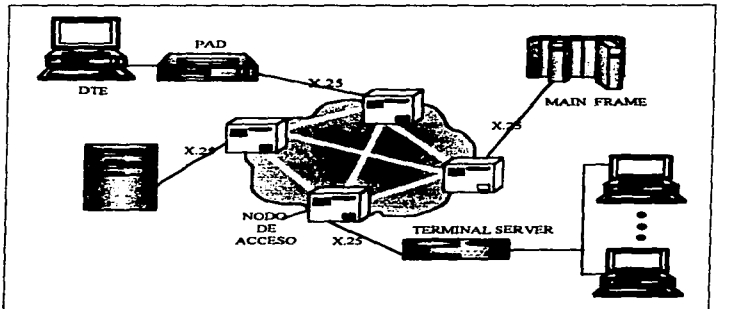
Las primeras contribuciones al protocolo Frame Relay aparecen en 1984. Sin embargo no fue hasta 1988 cuando el comité técnico T1 acreditado por el Instituto de Estándares Americanos (ANSI) aprobó la especificación de Frame Relay. Sus servicios estuvieron disponibles a partir de 1983.

Actualmente por la complejidad de las aplicaciones y los volúmenes de información que se transfieren de un punto a otro, han surgido tecnologías que ofrecen anchos de banda mayores y dedicados a cada usuario denominados "connection oriented", como ATM (Asynchronous Transfer Mode); así como dispositivos que procesan el tráfico a mayor velocidad y eficiencia al internarse en el mundo del Switches.

Las redes WAN (Wide Area Network) provee conectividad dentro de un ámbito nacional, y las redes GAN (Global Area Network) proveen una conectividad global, escapando del ámbito nacional.

1.4.1 ¿QUE ES X25?.

Los servicios públicos de conmutación de paquetes admiten numerosos tipos de estaciones terminales de distintos fabricantes. Por lo tanto, es de mayor importancia definir claramente la interface entre el equipo del usuario final y la red. X25 es la norma mundialmente aceptada que define esta interface. La norma X25 fue emitida originalmente por la CCITT en 1976. Desde entonces ha pasado por varias revisiones. La X25 especifica la interface entre una terminal de datos (DTE en modo de paquetes) y una red de paquetes (DCE) para el acceso a una red de paquetes pública o privada. Los protocolos definidos en X25 corresponden a los tres niveles más bajos del modelo OSI. El X25 admite corrección de errores y detección de errores, lo cual es ideal para entornos de baja calidad con líneas ruidosas cuando las aplicaciones en cuestión exigen una transmisión sumamente confiable. Tradicionalmente, X25 estaba diseñada para velocidades no mayores a 256 Kbps, sin embargo, en la actualidad se han desarrollado productos que soportan hasta 2.048 Mbps.



ELEMENTOS DE UNA RED X25

1.4.2 ¿QUE ES FRAME RELAY?.

Se conoce como Frame Relay al protocolo de transmisión "rápida" en una red de conmutación de paquetes.

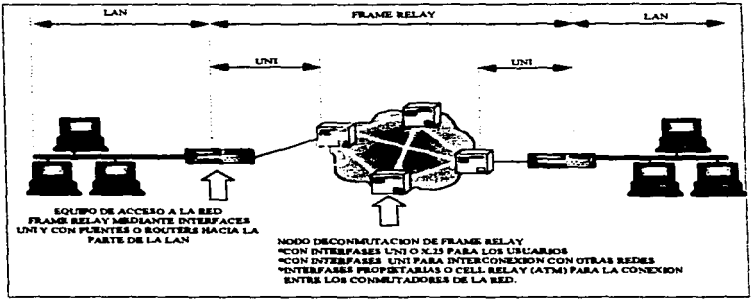
Este protocolo viene a optimizar los mecanismos tradicionales de conmutación de paquetes como el X25, el cual ejecuta funciones de detección y corrección de errores enlace por enlace causando grandes retrasos en el flujo de la información.

Sin embargo hay que destacar que Frame Relay por si mismo no mejora la capacidad de la red en lo referente a canales de comunicación, mas bien toma las ventajas de la disponibilidad y alta capacidad de los medios de transmisión, es decir que por ejemplo, puede mejorar la capacidad de transacción de paquetes en la red.

Dicho de otra forma Frame Relay aprovecha las bondades de los medios como la fibra óptica y ya no lleva a cabo la detección paso a paso de los errores, es decir, esa responsabilidad se la deja a los puntos extremos incrementándose con esto la eficiencia..

En general, el modo de operación de la red se puede categorizar dentro del modo orientado a conexión y soporta velocidades que van desde 64 Kbps y hasta 2 Mbps, sin embargo, una desventaja de Frame Relay es que no es aplicable para video u otros tráficos estacionarios que requieran procesamiento en tiempo real.

A diferencia de X25, Frame Relay elimina por completo cualquier proceso efectuado en la capa 3 del modelo OSI (capa de red o nivel de paquetes). Dicho de otra forma, las funciones de reconocimientos así como supervisión de tramas no son llevadas a cabo, lo cual permite aprovechar el concepto de procesamiento de tramas en red.



Otra característica importante de Frame Relay es que utiliza el multiplexaje estadístico por división del tiempo, es decir que dependiendo del flujo demandado por el usuario la trama se ajusta sin que se desperdicie ancho de banda a diferencia de la técnica TDM tradicional.

1.4.2.1 FDM, TDM Y STDM

Multiplexión por división de frecuencia (FDM), Multiplexión por división de tiempo (TDM) y multiplexaje por división de tiempo estadístico (STDM).

FDM.

Múltiples señales analógicas pueden ser multiplexadas en un mismo cable modulado, cada una de ellas con frecuencia portadora distinta, siendo muy útil para transmisiones telefónicas. Con el paso del tiempo se empezó a utilizar para la transmisión de datos, pero con malos resultados principalmente por el ruido, distorsión e interferencia generados entre las frecuencias portadoras. Su ventaja fundamental es que permite la transmisión ininterrumpida por cada canal. Sin embargo, si no es utilizado ese canal, el ancho de banda se desperdicia.

TDM.

Con la introducción de señales digitales fue posible dividir temporalmente el ancho de banda disponible. Cada canal utiliza la troncal completa por un periodo corto de tiempo.

MULTIPLEXIÓN POR DIVISIÓN DEL TIEMPO
TDM

STDM.

Opera igual que la TDM, pero con la ventaja de que puede asignar a cada segmento al canal que lo necesite. Esta ventaja permite obtener un 200% de rendimiento sobre una troncal con tecnología TDM.

1.4.3 ISDN (Integrated Services Digital Network, RDSI Red Digital de Servicios Integrados).

Las técnicas de transmisión digital utilizando STP, UTP, cables coaxiales, el espacio libre o fibra óptica han revolucionado los sistemas de comunicación , por lo que el incremento de la demanda y las demandas de las exigencias de calidad, han obligado a proporcionar servicios de comunicación, no solo para interconectar diferentes puntos, sino para optimizar el tiempo y costo así como, para mantener un ritmo de actualización tecnológica acelerado.

A raiz de la recomendación G.705 del CCITT en 1980, se normaliza de hecho el establecimiento de las bases para RDSI , lo cual se complementa más tarde con la aparición de la Rec. L120 y más aun cuando en el fascículo III.5 del CCITT se dedica toda una serie de libros (serie I) para la RDSI (Libros Rojos. 1984).

A partir de entonces se establecen modelos de referencia, protocolos, protocolos de acceso, así como técnicas de señalización aplicables a la RDSI.

RDSI no es un equipo, ni es un medio, ni un grupo de funciones, RDSI es un concepto global en el cual las facilidades y servicios propuestos por RDSI pueden resumirse del modo siguiente:

1.- Proporcionar una conexión completamente digital entre usuarios.

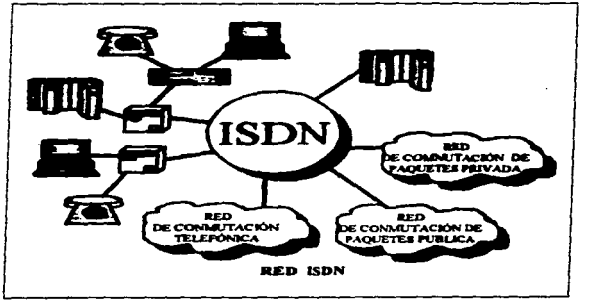
Es decir antes de RDSI el bucle de abonado analógico y el aparato telefónico realizaba funciones tan básicas como la detección de colgado y descolgado. Con RDSI se cambia el concepto de aparato telefónico por equipo terminal multifunciones.

Esto trae como consecuencia la necesidad de la digitalización del bucle del abonado, así como el diseño del aparato de usuario para soportar accesos a equipos con aplicaciones de conmutación como X.25, de tal forma que el usuario pueda seleccionar desde su aparato la aplicación que requiere e incluso utilizar más de una simultáneamente (por ejemplo voz y datos).

2.- Soporte de amplio rango de aplicaciones de voz , datos y video (de baja resolución) en la misma red.

RDSI permite la integración de aplicaciones de usuario y red que originalmente trabajaron de manera independiente proponiendo para este objetivo el acceso a los servicios proporcionados por la red. a través de un solo conector (RJ45) .

Se pueden observar los servicios de fax, voz y datos conectorizados en un solo ambiente, lo cual redunda las ventajas tanto en el bucle local como en la red.



RED ISDN

1.4.3.1 LA BROADBAND DE ISDN (LA BANDA AMPLIA DE ISDN).

El término de Broadband ISDN (B-ISDN) es usado al indicar el uso del ancho de banda mas allá de la banda base que ofrece ISDN. Con el nuevo concepto de B-ISDN se espera que a la segunda mitad de los años 90's ofrezca un rango de 150 a 600 Mbps. Mientras que la banda base de ISDN es provista casi exclusivamente por cable de cobre. El Broadband de ISDN usa fibra óptica en una menor parte de la red. En los servicios de B-ISDN se espera incluir: Altas velocidades en el transporte de datos, Videoteleconferencia, Videotelefonía, Alta calidad en audio, Distribución de video. Así, B-ISDN se espera que tenga su máxima utilización en las capacidades de la familia SONET. Sin embargo los estándares de B-ISDN son estudiados por la CCITT y todavía se encuentran en una etapa de formación.

1.4.4 ¿QUE ES ATM?.

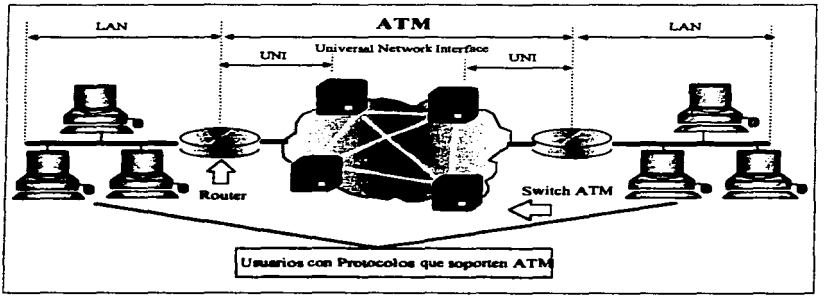
Una de las tendencias actuales en telecomunicaciones la constituye el surgimiento de redes de banda ancha que brindan un ancho de banda mas allá de las velocidades de T1/E1. El crecimiento explosivo de las interconexiones entre redes locales es en este momento causa de cuellos de botella en la tradicional infraestructura de las WAN.

El incremento de las aplicaciones de banda ancha y de multimedia y el deseo de integrar voz, datos y video en una infraestructura común de comunicaciones contribuye a su vez a estos cuellos de botella. Una red global que no sea afectada por distancias geográficas exige una infraestructura de conmutación de transmisión que sea capaz de manejar la demanda creciente de mayor capacidad.

Se ha elegido la tecnología ATM (Modo de Transferencia Asíncrona) como la técnica de multiplexado y conmutación para ISDN (RDSI) de banda ancha a fin de atender las necesidades de las redes de comunicaciones de alta velocidad y múltiples servicios.

Ésta tecnología puede llevar servicios a velocidades constantes o variables, servicios isócronos (voz/video) o asíncronos (datos), así como soportar servicios orientados a conexión o no conexión. El entorno de conmutación de ATM es independiente de las velocidades de datos y admite la conmutación tanto de redes públicas como de redes de área local a velocidades ultra altas que superan 1 Gbps.

ATM es apoyado intensamente por los proveedores de servicios de telecomunicaciones, los fabricantes de equipo y los usuarios, esto se debe a que elimina la necesidad de tener múltiples redes para diferentes tipos de servicios. Este apoyo se concretiza en el Foro ATM que es una organización internacional cuyo objetivo es acelerar el uso de ATM a través de una rápida convergencia de especificaciones de interoperabilidad.



1.4.5 DEFINICIÓN DE SERVICIOS WAN.

Un servicio WAN es aquel que proporciona la capacidad de comunicación entre varios puntos distantes mediante alguna tecnología en particular. Provisto generalmente de manera pública y cuando es necesario, como infraestructura privada.

Por su naturaleza dicha tecnología puede estar basada en:

-La conmutación de circuitos
-La conmutación de paquetes (paquetes , tramas, celdas) y que por su naturaleza pueden ser :
Orientada a conexión o connection oriented (PVC's y SVC's)
Sin conexión o connectionless.

1.4.5.1 CONMUTACIÓN DE CIRCUITOS.

El establecimiento de una conexión a través de una red telefónica conmutada se basa en el principio de conmutación de circuitos.

La OSI define a la conmutación de circuitos (circuit switching) en el procedimiento que enlaza a voluntad dos o más equipos terminales de datos y que permite la utilización exclusiva de un solo circuito de datos durante la comunicación.

A través de un sistema de este tipo los ETD pueden establecer comunicación ya sea de tipo asíncrono o síncrono; esto es, un sistema basado en el principio de conmutación de circuitos pude transmitir caracteres o paquetes.

En resumen, se puede decir que en la conmutación de circuitos:

- El trayecto esta dedicado a una sola llamada o conexión.
- El enlace puede ser dedicado o conmutado.
- Cuando es dedicado se hace un salto a las centrales de conmutación y se hace una conexión directa hacia los equipos que forman parte de la red de transmisión.
- En los circuitos conmutados las conexiones se hacen dentro de la central de conmutación.
  por ejemplo : Línea privada, DSO, E0, E1, T1, ISDN, etc.

Dentro de las desventajas de la conmutación de circuitos tenemos:

- El tiempo necesario para iniciar la llamada (para que se efectúe la conexión es relativamente largo).

- Los dos ordenadores han de comunicarse exactamente a la misma velocidad (baudios), ya que el sistema es muy flexible a cambios de velocidad.

- La red no proporciona control de errores ni control de flujo para los datos transmitidos, el control lo proporcionan los usuarios.

1.4.5.2 LÍNEA PRIVADA.

El término línea privada es muy general pero tradicionalmente hace referencia a un enlace dedicado contratado con una compañía de telecomunicaciones y con características similares a las de una línea telefónica. Dentro de las ventajas que ofrece son:

- Mejor calidad y por lo tanto reducción en la taza de error.
- Se tiene mejor control sobre el enlace y se asume muy alta disponibilidad por parte de la red.
- Adecuado para grandes volúmenes de tráfico.

Sus desventajas son:

- Costo fijo aunque no se utilice.
- Dependiente del lugar.
- Limitado a bajas velocidades (hasta 28.8 Kbps).

1.4.5.3 DS0

DS0 es el termino que Telmex utiliza para referirse al servicio de conexión dedicado punto - punto a 64 Kbps mediante un par de cobre en la ultima milla. DS0: Digital Signal 0.

Dentro de sus ventajas se encuentran:

- Mayor velocidad que las líneas privadas analógicas.
- Permite la implementación de nuevos servicios por parte del usuario.
- Utiliza un solo par de cobre.
- Mejor calidad y muy alta disponibilidad por parte de la red.
- Adecuado para grandes volúmenes de tráfico.

Dentro de sus desventajas tenemos:

- Costo fijo aunque no se utilice.
- Dependiente del lugar.
- Mayor costo que una línea privada analógica.
- Alto costo para redes con muchos nodos

1.4.5.4 E0

Cuando hablamos de un enlace E0 nos referimos a una conexión que se realiza a 64 Kbps.
En términos prácticos este servicio es el mismo que el DS0, Sin embargo para Telmex y por cuestiones de mercadotecnia se trata de dos servicios distintos que cuestan diferente y que trabajan a la misma velocidad.

Ventajas con respecto a! DS0 de Telmex:
Posibilidad de crecimiento de enlaces de 64 Kbps más rápida.
Desventajas con respecto al DS0 de Telmex.
Mayor costo.
Mayor tiempo de instalación y mucho más complicada.

1.4.5.5 E1, T1.

Este servicio consiste en la contratación de un enlace dedicado entre dos puntos, a una velocidad de 2.048 Mbps si se trata de un E1 o bien 1.544 Mbps si se trata de un T1, en México los servicios provistos son E1.

Cuando no se requiere el E1 o T1 completo es posible contratar los servicios FE1 (Fractional E1) o FT1(Fractional T1) respectivamente. Esto quiere decir que de los 32 canales solo se utilizan N (NX64).

Cabe mencionar que existen jerarquías superiores como son:
E2 Que corre a 8.448 Mbps., E3 a 34.368 Mbps., E4 a 139.264 Mbps.,
T2 a 6.312 Mbps., y T3 a 44.736 Mbps.

1.4.5.6 CONMUTACIÓN DE MENSAJES.

La conmutación de mensajes es una técnica que soluciona la mayoría de las desventajas de la conmutación de circuitos cuando se usa la red para transportar datos. En vez de conmutar el circuito, los circuitos están permanentemente preparados y el mensaje se pasa por toda la red. Es decir, en una red con topología irregular el mensaje se pasa de un nodo a otro hasta que llega a su destino.

Esta técnica funciona del modo siguiente:

· El mensaje incorpora algún tipo de cabecera que incluye la dirección del receptor remoto al que va dirigido el mensaje, y es evidente que se necesita algún algoritmo de direccionamiento.

· El mensaje se transfiere de un nodo a otro como una unidad, es decir, el mensaje completo es recibido en un nodo y almacenado antes de ser enviado al otro nodo de su ruta. En cada nodo se realizan comprobaciones de errores para asegurar que el mensaje sea recibido correctamente. El mecanismo se conoce como guardar y seguir.

VENTAJAS:

Se incrementa la eficiencia del canal.
Se reduce la congestión al almacenar temporalmente los mensajes.
Un mensaje puede ser enviado a varios destinos.

DESVENTAJAS:

Los dispositivos de almacenamiento - reexpedición requieren de gran capacidad de memoria para evitar la saturación en el nodo intermedio.
La conmutación de mensajes no es compatible con muchos sistemas en tiempo real.

1.4.5.6.1 SEGMENTACIÓN

La información intercambiada entre dos sistemas puede ser muy grande, por lo que se divide en partes y se lleva un control de transferencia.

se verifica que se reconstruya en el mismo orden en que fue enviada.

1.4.5.7 CONMUTACIÓN DE PAQUETES.

La conmutación de paquetes se denomina así porque el nodo fuente divide el mensaje en varios mensajes más pequeños, correspondiendo a cada uno de ellos a una longitud optima. El nombre de esta unidad de transmisión mas pequeña se conoce como paquete. Los paquetes se pueden entonces enviar por separado a través de la red, y cuando llegan todos ellos a su destino se vuelven a ensamblar para formar el mensaje original. Como estos paquetes se conmutan a través de la red la técnica se conoce como conmutación de paquetes.

Es evidente que el requisito de almacenamiento y gestión de cada nodo intermedio es mas sencillo que el de conmutación de mensajes, debido al pequeño tamaño máximo del paquete. Además, los pequeños paquetes pueden ser intercalados en los enlaces de la red, reduciéndose de esta forma las demoras.

Se puede decir que la conmutación de paquetes combina las ventajas de la conmutación de circuitos y la conmutación de mensajes; es decir, existe una mayor eficiencia en el uso de ancho de banda al igual que un tiempo de retardo mínimo.

Existen dos métodos para la conmutación de paquetes:

- DATAGRAMAS.
- CIRCUITO VIRTUAL.

1.4.5.7.1 DATAGRAMA.

Con un servicio de Datagramas, cada paquete se trata como una unidad separada. Por tanto, el paquete ha de incluir una dirección destino para asegurar que se reciba en el destino correcto. Como los paquetes se tratan por separado, cada paquete puede viajar a través de la red por rutas diferentes, llegando en un orden diferente al que fueron enviados. Naturalmente, es posible que haya alguno que no llegue jamás. Los usuarios de la maquina gestora han de implementar algún tipo de control (dentro del nivel 4: el protocolo de transporte) de error y de flujo, para detectar paquetes duplicados o que se hayan perdido. Este servicio tiene muchas ventajas para los nodos de la red, puesto que el direccionamiento puede ser flexible y por lo tanto no es necesario un control de secuencia y de flujo, pero requiere participación del usuario de la red.

A esto se le llama servicio de Datagramas porque tiene cierto parecido con el servicio que ofrece correos, usted puede enviar varias cartas a un mismo

destinatario, pero éstas pueden llegar en un orden diferente (o es posible que no lleguen).

1.4.5.7.2 CIRCUITO VIRTUAL.

Una de las ideas de la conmutación de paquetes consiste en entrelazar múltiples transmisiones de varias terminales en un solo canal. El efecto es el de una Multiplexión por división temporal de la línea de telecomunicaciones. Este esquema proporciona un mejor uso y aprovechamiento del canal de comunicaciones, que es un recurso costoso.

Pero la conmutación de paquetes es más que la simple Multiplexión de las líneas de comunicaciones. La lógica de paquetes también puede multiplexar varias sesiones de usuario en un solo puerto de comunicaciones del computador. En vez de dedicar un puerto a cada usuario, el sistema entrelaza las ráfagas de tráfico de distintos usuarios en un mismo puerto. El usuario percibe la situación como si tuviera un puerto dedicado, aunque realmente comparte el puerto con otros usuarios. El puerto y el canal multiplexados se denominan circuito virtual o canal virtual. "virtual" significa que el usuario cree que tiene un recurso dedicado, cuando en realidad es un recurso compartido.

	Subred de Datagramas	Subred de C.V.
Establecimiento del circuito	No es posible	Cada paquete contiene un número corto de C.V.
Enrutamiento	Cada paquete se enruta independientemente	Ruta seleccionada cuando el C.V se establece; todos los paquetes siguen esta ruta.
Complejidad	En la capa de transporte	Con la capa de red.
Ejemplo de aplicación	Protocolo IP de la red Internet	Protocolo X.25 capa de red de la disciplina X.25

COMPARACIÓN ENTRE DATAGRAMAS Y CIRCUITOS VIRTUALES

1.4.5.8 CONMUTACIÓN DE PAQUETES RÁPIDOS (FAST PACKET SWITCHING).

Es una tecnología digital de alta capacidad orientada a paquetes que proporcionan las funciones de conmutación, multicanalización y transmisión, un ejemplo es Frame Relay, SMDS y ATM.
También combina las ventajas de la conmutación de paquetes, es decir,
* Eficiente uso del ancho de banda.
* Tiempo de retardo mínimo.

1.4.5.9 CONMUTACIÓN DE TRAMAS.

Técnica que deriva del concepto de conmutación de paquetes que simplifica el protocolo de enlace (capa 2), reduciéndose a funciones de control de errores extremo-a-extremo en forma mínima (descarte de tramas erróneas)
Esta tecnología simplifica los nodos de conmutación, permitiendo mayores velocidades.
Un ejemplo de aplicación también podría ser Frame Relay.

1.5. NORMAS Y ESTÁNDARES INTERNACIONALES.

Como todo en la vida, la forma de asignar direcciones a las redes también tiene que seguir algunas normas y estándares internacionales para que no existan dos números de red iguales, ahora mencionaremos algunas normas y algunos tipos de numeraciones.

1.5.1 NUMERACIÓN IP.

La numeración IP se basa en el software, y es un número que asigna el administrador de la red en base al número de red asignado anteriormente cuando se registro la red.

1.5.1.1 DIRECCIONAMIENTO Y SUBREDES

Cualquier sistema global de comunicaciones requiere un método universal aceptado para poder identificar a todos los diferentes dispositivos que están conectadas a una red, a los dispositivos se les asigna un único direccionamiento que identifique donde están y como poder accesar a ellos, estos dispositivos pueden ser computadoras personales, servidores de terminales, Ruteadores, estaciones de administración o HOST de UNIX.

Existe algo que todos los dispositivos tienen en común, cada uno tiene asignada su propia dirección, algunos dispositivos como los Ruteadores, los cuales tienen conexiones físicas a más de una red, se les debe asignar una dirección única por cada conexión de red.

Las direcciones usan campos de 32 bits. Los bits en los campos de direccionamiento son números del 0 al 31, éste campo es dividido en dos partes, uno identifica al dispositivo y otro identifica le red en la cual el dispositivo reside. Los dispositivos que pertenecen a la misma red comparten el prefijo común designado para la red .

Existen cuatro clases de direccionamiento para identificar a las redes que pueden ser fácilmente determinadas por el bit que ocupe la posición inicial.

1.5.1.2 DIRECCIONAMIENTO DEL FORMATO CLASE "A".

El formato clase "A" tiene el bit principal colocado a "0", siete bits para el número de la red y 24 para el direccionamieto de los dispositivos. 126 redes clase "A" pueden ser definidas hasta con 16,777 216 dispositivos diferentes.

0	1 7 8	31
0	RED	Direccionamiento del formato clase "A"

La clase "A" va desde 1.0.0.0 hasta 126.0.0.0 .
En un número de red no están permitidos ni todos ceros ni todos unos.

1.5.1.3 DIRECCIONAMIENTO DEL FORMATO CLASE "B".

El direccionamiento de red clase "B" tiene los dos bits principales colocados a 1-0 , 14 bits para el direccionamiento de los dispositivos locales .
16383 redes clase "B" pueden ser definidas hasta con 65 535 dispositivos por cada red. El direccionamiento clase "B" se muestra en la siguiente figura.

Para clase "B" la numeración va desde 128.1.0.0 hasta 191.254.0.0

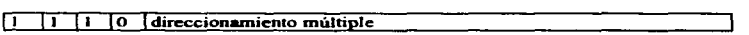
1.5.1.4 DIRECCIONAMIENTO DEL FORMATO CLASE "C".

El direccionamiento clase "C" tienen los tres primeros bits colocados a 1-1-0, 21 bits para el número de la red y 8 bits para el número de los dispositivos. 2,097 152 redes clase "C" pueden ser definidas hasta con 254 dispositivos por red. El direccionamiento clase "C" se muestra en la siguiente figura.

Para la clase "C" la numeración va desde 192.0.1.0 hasta 223.255.254.0

1.5.1.4 DIRECCIONAMIENTO DEL FORMATO CLASE "D".

El direccionamiento de formato clase "D" se usa como multicast. Los cuatro principales bits están colocados a 1-1-1-0, la clase "D" , como todas las direcciones IP son asignadas por la IAB.



Para calcular el número de redes y el número de nodos con sus numeraciones dentro de la Subred se utilizan las siguientes fórmulas:

Para calcular el número de redes.

$2^x - 2 =$ **Número de redes.**

x = El número de Bit's 1's para usar.

Para calcular el número de nodos.

$2^y - 2 =$ **Número de nodos.**

y = El número de Bit's para los nodos.

Ejemplo :

Se requiere implementar una red que tiene 125 subredes, se sabe además que la dirección proporcionada por el NIC es la 150.5.0.0. Determinar la dirección de cada una de las subredes y cada uno de los nodos.

Solución:
Para empezar es una red clase "B" (debido al número asignado por el NIC).

Según la formula tenemos el número de subredes, pero no el número de bit's 1's que debemos usar.

$$2^x - 2 = 125$$

$$2^7 - 2 = 126$$

Ahora sabemos que se requieren 7 bit's y se sabe que como es clase "B" los dos primeros Bytes están ocupados por lo tanto debemos trabajar en el tercer Byte.

10111111.11111111.11111110.00000000

Una vez identificada la mascara se codifica en decimal y algo muy importante que se debe tomar en cuenta es que ya no se aplica el 10 de la clase "B".

11111111.11111111.11111110.00000000
155 . 155 . 154 . 0

Partiendo de este hecho el cálculo para el número de cada red quedaría así:

1	1	1	1	1	1	1		0		N° de subredes
0	0	0	0	0	0	1		0		150.5.2.0
0	0	0	0	0	1	0		0		150.5.4.0
0	0	0	0	0	1	1		0		150.5.6.0
0	0	0	0	1	0	0		0		150.5.8.0
0	0	0	0	1	0	1		0		150.5.10.0
0	0	0	0	1	1	0		0		150.5.12.0
0	0	0	0	1	1	1		0		150.5.14.0
0	0	0	1	0	0	0		0		150.5.16.0
0	0	0	1	0	0	1		0		150.5.18.0
1	1	1	1	1	1	1		0		150.5.252.0

Para el Número de nodos nos quedarían el último bit del tercer Byte y los ocho bits del cuarto Byte, por lo tanto nos queda un total de 9 bits para numerar los nodos, lo cual resulta según la formula en:

$$2^9 - 2 = 510$$

Esto indica que nosotros podemos tener hasta un máximo de 510 nodos por Subred
La numeración para el primer nodo de la primer red quedaría así:

150.5.2.1

Y la numeración para el ultimo nodo de la ultima red quedaría así:

150.5.252.510

Cabe mencionar que cuando se asigna un número para red, ese número será internacionalmente el mismo para esa red, por lo que si la red es muy grande se tendrán que usar mascaras y submascaras que darán la opción de tener un número de redes mucho mayor al que se puede tener con solo el número asignado por el NIC y con ello evitar tener que solicitar otro número.

1.5.2 RECOMENDACIÓN X . 121.

Plan de numeración internacional para redes públicas de datos.

La recomendación X.121 propone un plan de numeración internacional para redes públicas de datos en base a las siguientes consideraciones.

a) El plan de numeración internacional para redes públicas de datos facilita la introducción de redes públicas de datos y permite su interfuncionamiento en un plano mundial.

b) El plan de numeración internacional considera la existencia de varias redes públicas de datos en un país.

c) El plan de numeración internacional permite la identificación de un país, así como la de una red pública de datos determinada de ese país.

d) El plan de numeración internacional prevé una capacidad de reserva adecuada para satisfacer futuras exigencias.

Las características de X.121 son las siguientes.

X.121 permite hasta 14 dígitos para direccionar, agrupando jerárquicamente zonas agrupadas o dominios.

Algunos dominios son administrados directamente por el CCITT, mientras que otros son asignados a los países para su administración local; los dominios en los países son a su vez particionados en subdominios.

La dirección de red X.121 esta dividida en dos secciones:.

Los primeros 4 dígitos representan el código de identificación de red de datos (CIRD).

El CIRD es asignado por el CCITT e identifica una particular red pública de conmutación de paquetes de datos.

1er DÍGITO	ZONA
0	RESERVADO
1	RESERVADO
2	EUROPA
3	NORTE AMÉRICA
4	ASIA
5	OESTE DE ASIA Y OCEANÍA
6	ÁFRICA
7	SUDAMÉRICA
8	REDES TELEX/TWX.
9	REDES TELEFÓNICAS

El primer dígito del CIRD especifica una zona geográfica mundial o tipo de red.

Los primeros tres dígitos del CIRD (la zona geográfica o tipo de red mas dos dígitos) son el código de país para datos (IPD).

Los 4 y últimos dígitos del CIRD identifican una red especifica de conmutación de paquetes de datos.

Los siguientes 10 dígitos de la dirección X.121 son asignados por una red pública de datos localmente.

FORMATO DE DIRECCIONAMIENTO X.121.

1.5.3 PLAN DE NUMERACIÓN E.164.

(Plan de numeración para la era de la RDSI).

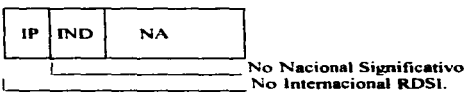
La recomendación E.164 define la numeración para el servicio telefónico internacional como un subconjunto del plan de numeración para la RDSI.
El plan de numeración internacional se establecerá de acuerdo con la recomendación, de manera que el abonado típico se le llame siempre por el mismo número en el servicio interurbano.
El plan de numeración nacional de un país (o de una región) deberá establecerse de modo que el análisis de cifras no tenga que rebasar los límites establecidos (Como máximo se permite un número de cifras igual a 15-n; con n= número de cifras del indicativo del país considerado) aplicables al número nacional pero que permita.

a) Determinar un encaminamiento que tenga en cuenta los factores económicos y otros factores de red apropiados.

b) Distinguir las diferentes tarifas a aplicar en función del área de destino en aquellos países en las que estas distinciones son aplicables.

1.5.3.1 ESTRUCTURA DEL NUMERO INTERNACIONAL RDSI.

El número internacional RDSI es un número de longitud variable compuesto de una cantidad variable de cifras decimales dispuestas en campos de código específicos. Los campos del número internacional RDSI son indicativo de país (IP) y el número nacional (significativo), la siguiente figura muestra la estructura del número Internacional para RDSI.



IP: Indicativo de país.
IND: indicativo nacional de destino
NA: número de abonado.

En la figura anterior el indicativo de país (IP) es utilizado para seleccionar el país destino y su longitud está determinada en base a las siguientes consideraciones:

a) El indicativo de país se compone de una, dos o tres cifras, según los desarrollos telefónico y demográfico previsibles en el país considerado.

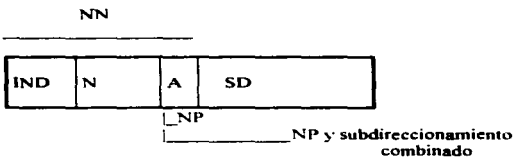
b) Las nueve cifras del 1 al 9, se han asignado como indicativo de país o como primera cifra de este indicativo.

El número nacional (NN) significativo es usado para seleccionar el abonado de destino. Sin embargo, al seleccionar el abonado de destino puede ser necesario seleccionar una red de destino. Para esta selección, el campo de código del NN comprende un indicativo nacional de destino (IDN) seguido del número de abonado (NA). En algunas aplicaciones nacionales el IND y el NA pueden estar enlazadas de una manera inseparable formando una secuencia única de marcación compuesta.

Cuando sea necesario, pueden utilizarse también prefijos para la selección de redes y servicios. Un prefijo es un indicador compuesto por una o más cifras, y que permite la selección de diferentes tipos de formatos de números (por ejemplo: local, nacional o internacional), redes de transito o servicios. Los prefijos no forman parte del número y no se señalizan a través de fronteras interredes o internacionales (Cuando se utilizan prefijos, siempre son introducidos por el usuario o por el equipo de llamada automática).

1.5.3.2 SUBDIRECCIONAMIENTO RDSI.

El subdireccionamiento ofrece una capacidad de direccionamiento adicional distinta fuera del plan de numeración de la RDSI pero, intrínsecamente, es parte integral de las posibilidades de direccionamiento de la RDSI como se muestra en la siguiente figura, el número de la RDSI puede ir seguido de uno o más octetos hasta un número de 20 (o 40 cifras decimales); estas cifras forman la subdirección de la RDSI que se transfiere a las instalaciones del abonado.



IND: Indicador Nacional de Destino; NN: Número Nacional; NA: Número de Abonado; SD: Subdirección; NP: Número parcial.

1.6. DIFERENTES DISPOSITIVOS PARA INTERCONECTAR REDES DE ÁREA LOCAL

La popularidad de las redes surge de su capacidad para interconectar sistemas localmente o sobre distancias extensas, para compartir inteligencia y acceso a los recursos de computación y sobre todo de información.

Existen cinco tipos de dispositivos para el entrelazamiento de redes LAN, estos son: Repetidores, Puentes (Bridges), Ruteadores, Gateways y LANSwitches, cada uno de ellos representa un nivel diferente de conectividad y funcionalidad como es definido por el método de interconexión de sistemas abiertos.

Éste modelo define una base común para el diseño empleado por los desarrolladores que trabajan cualquier tipo de productos de interconectividad. El modelo se aplica a cualquier clase de productos de conectividad, desde módems y redes X.25 hasta redes vía satélite globales, se conduce particularmente bien para la interconectividad de LAN's , ya que la mayoría de los fabricantes utilizan éste modelo para diseñar sus productos.

1.6.1 REPETIDORES

El producto más simple de enlazamiento de redes LAN es el repetidor, operando en la capa física (que es la más baja del modelo OSI) , los repetidores se extienden físicamente al alcance de redes idénticas para generar señales de un cable y transmitirlo a otro. Un repetidor simplemente saca la fuerza de la señal de los impulsos eléctricos de la red .

Como conectores de capa física, los repetidores no efectúan alguno de los niveles más altos que se requieren en las redes más complejas, por lo tanto los repetidores solamente pueden enlazar las redes con formatos de protocolos similares, están severamente limitados por la distancia, y tiene la desagradable virtud de repetir el ruido así como también repiten los datos correctos. Los repetidores típicamente apoyan solo el enlazamiento de redes locales dentro de un solo edificio.

Los repetidores efectúan mucho menor procesamiento de paquetes de datos que los Puentes, Ruteadores, Gateways o LAN Switches. Como resultados normalmente tienen índice de producción más altos, pasando los datos directamente de una red a otra con poco retraso en el procesamiento. Su simplicidad técnica también afecta en su precio relativamente bajo, en el margen de 300 a 400 U.S. dlls aproximadamente.

Como un dispositivo de interconectividad de redes, los repetidores están limitados a distancias cortas. La mayoría de las aplicaciones de los repetidores están limitadas a menos de una milla. Por ésta razón no se puede considerar como un concentrador de red remota.

1.6.2 PUENTES (BRIDGES)

Los puentes conectan a las redes en la capa de enlace de datos fig. sig. y más específicamente en el subnivel de control de acceso al medio (número MAC) y el control de enlace lógico (LLC) .El nivel donde se encuentra el MAC incorpora la capa física y la parte de la capa de enlace del modelo OSI . Principalmente la capa de enlace de la información está incorporada en el hardware de un NIC[1] específico. Eso es, que el software que controla los MAC y los LLC es de tarjeta y no están en los manejadores de dispositivos de las estaciones de trabajo. Son transparentes para IPX/SPX, NetBios y otras capas de redes y protocolos más altos.

Los Bridges conectan las LAN's a topologías y protocolos similares como podría ser Ethernet con Ethernet, Token Ring con Token Ring, pueden ser usados para eslabonar cables de tipos diferentes como por ejemplo cable coaxial de Ethernet con UTP de Ethernet.

Existen tres tipos de Bridges: Buffered, Filtering y Learning.

Bridge Buffered.- Aisla segmentos de LAN's conectadas entre si pero las colisiones no se propagan a través de los segmentos

Bridge Filtering.- Pueden estar filtrados por tipo de propagación de paquetes físicos, por ejemplo un Bridge Filtering puede filtrar tipos de paquetes mientras que TCP/IP transmite información.

Bridge Learning.- Este tipo de bridge escucha todas las transmisiones en segmentos. Todas las direcciones de la información están cuidadosamente almacenadas para luego ser enviadas a su nivel de origen.

[1] NIC (Netkork Interface Card).

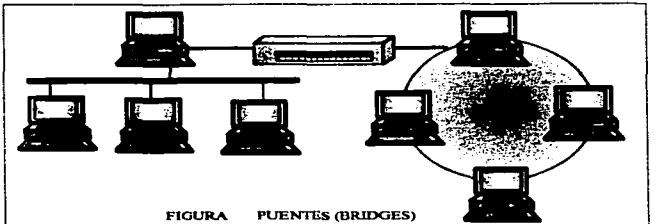


FIGURA PUENTES (BRIDGES)

Los puentes son inteligentes, aprenden las direcciones del destino del tráfico que pasan por ellos y lo dirigen a su destino final. Esto explica su importancia en la división de red: cuando un segmento físico de red tiene tráfico en exceso su rendimiento comienza a degradarse, se le puede dividir en dos segmentos físicos con un puente. Este dirige el tráfico a su destino y limita al que no debe pasar por un determinado segmento. Los Bridges usan un proceso de aprendizaje filtrado y envío para mantener el tráfico dentro del segmento físico al que pertenece.

Debido a que los puentes aprenden direcciones, examinan paquetes y toman decisiones de envío con frecuencia, pero como ya se mencionó su funcionamiento se degrada en cuanto el tráfico aumenta, de echo esta cuestión es de las más importantes a tomarse en cuenta si se pretende instalar un Bridge, sin embargo, en general, en ambientes de protocolos mixtos los puentes son muy útiles.

1.6.3 RUTEADORES[2].

Los Ruteadores son dispositivos de interconexión que operan dentro de la capa 3 del modelo OSI . Los Ruteadores soportan protocolos específicos como TCP/IP, IPX/SPX, DecNet y otros.

Este dispositivo es normalmente ciego para todos los protocolos que específicamente no soporten dicho dispositivo, sin embargo, algunos Ruteadores como los que ofrecen distribuidores tales como Proteon Inc. y Cisco Systems Inc. pueden ser programados de tal manera que soporten protocolos múltiples.

[2] El funcionamiento y todo lo referente a los Ruteadores se verá más a fondo en el capítulo 2.

Algunos Ruteadores como la serie Proteon 42xx y Schneider & kock y los de la compañía SK-Net, tiene la virtud de encapsular información de un tipo de protocolo dentro de otro tipo . Esta característica es usada por varias universidades cuya columna de comunicación entre campus es TCP/IP.

En conclusión los Ruteadores sirven para conectar LAN's con diferentes topologías o protocolos en un segmento real de la red.

1.6.4 BROUTER.

Existe una combinación entre Puentes y Ruteadores a los cuales se les conoce como Brouters que es una especie de híbrido de protocolos múltiples, los Brouters ofrecen muchas de las ventajas , tanto de los Bridges como de los Ruteadores para redes más complejas.

Estos dispositivos son costosos, complicados y difíciles de instalar, pero en casos de redes heterogéneas muy complejas, con frecuencia ofrecen la mejor solución de interconexión.

1.6.5 GATEWAYS.

Los Gateways operan en las tres capas superiores del modelo OSI (sesión , presentación, y aplicación). Ofrece el mejor método para conectar segmentos de red y redes mainframes.

Se selecciona un Gateway cuando se tienen que interconectar sistemas que se construyeron totalmente con base en diferentes arquitecturas de comunicación. Por ejemplo, se utilizara un Gateway para interconectar TCP/IP a un mainframe SNA (System Network Architecture, Arquitectura de Sistemas de Redes) , las dos arquitecturas no tienen nada en común, por lo que el Gateway debe traducir todos los datos que pasan entre los dos sistemas.

Un uso frecuente para los Gateways es conectar un sistema remoto como una red pública de datos con conmutación X.25 (método eficiente para empaquetar datos y enviarlos remotamente).

En cada extremo de la red el Gateway ofrece la conversión del protocolo de y a los segmentos de red conectados del otro lado. Los Gateways no proporcionan enrutamiento de paquetes dentro de un segmento de red; simplemente entregan los paquetes de datos de tal forma que los segmentos puedan leerlos. Cuando reciban paquetes del segmento, los traducen y enrutan el Gateway en el otro extremo, donde los paquetes vuelven al segmento de red en el extremo opuesto.

1.6.6 LAN SWITCHES[3]

Para redes de gran cantidad de estaciones y con varios servidores, productos como los LAN Switches ofrece una solución más inmediata para los problemas de tráfico.

Los LAN Switches aprovechan el método de Cut-Through mediante el cual el concentrador solo descodifica la dirección destino contenida en un paquete y automáticamente lo dirige hacia el puerto el cual está conectado el nodo destino, reduciendo así, significativamente la latencia de la red. De ésta forma LAN Switch elimina los cuellos de botella causados por la saturación de un solo canal de acceso entre los concentradores y servidores.

La solución es parecida ala ofrecida por un puente, solo que en este caso se está empleando una técnica de conmutación: al proporcionar tres caminos simultáneos y paralelos desde los concentradores hacia los servidores. Los LAN Switches triplican virtualmente el ancho de banda de Ethernet.

Además, como su funcionamiento se ubica en el nivel de OSI, los LAN Switch es compatible con cualquier paquete que se apegue al estándar 802.3 sin importar el tipo de enlace físico.

[3] El funcionamiento y todo lo referente a los LAN Switches se vera más a fondo en el capitulo 3.

CAPÍTULO 2

RUTEADORES

2.1.- FUNDAMENTOS DE LOS RUTEADORES.

2.1.1.- ¿PORQUE LA INTERCONEXIÓN?.

La interconexión de las LAN comprende todas las aplicaciones entre las cuales se conectan varias LAN entre sí, formando una red de gran tamaño. La interconexión de redes "Internetworking" se implementa por varia razones:

- Conectar las LAN de distintos lugares en una sola red.
- Conectar entre sí las LAN de los distintos departamentos de una organización, formando una LAN que comprenda toda la empresa.
- Subdividir una red de gran envergadura en segmentos por razones administrativas, de seguridad o de funcionamiento.

2.1.2.- PROTOCOLOS.

Cuando se desea enviar información de un punto a otro, se deben seguir algunas reglas, las cuales nos dicen como acomodar nuestra información para que se pueda enviar correctamente, la forma de acomodar junto con alguna otra información de control es conocida como protocolo.

En una red de área local (LAN) todos los nodos conectados requieren de un protocolo de comunicaciones que pueda transportar información de un nodo a otro. Estos protocolos operan en diferentes capas del modelo OSI.

Existen diferencias fundamentales entre protocolos superiores a capa 2 del modelo OSI, aunque todos ellos tengan la misma función. Una de sus principales caracteristicas es la de permitir catalogarlos como protocolos ruteables y protocolos no ruteables, además de que cada uno puede ser ruteable o no, pueden ser orientados a conexión y a no conexión.

2.1.2.1.- PROTOCOLOS RUTEABLES.

Un protocolo ruteable puede definirse como aquel que "interpreta" al origen y el destino de la información que llevan consigo sus paquetes, como ente lógico denominado red. En efecto, cada segmento físico de LAN es definido como una dirección lógica.

Los protocolos ruteables guardan una analogia con el servicio de correo. Los paquetes destinados a un nodo llevan dentro de sí un formato conocido como encabezado (Header) que lleva la información de la dirección de red origen (calle remitente) y de la red destino (calle del destinatario), y pueden también llevar al

número del nodo origen (número de casa del remitente) y el número de nodo destino (número de casa del destinatario).
En ésta analogía el número de red es el nombre de la calle y el número de nodo (MAC, address o nodo físico), es el número de la casa que estamos buscando.

Todos los protocolos ruteables se caracterizan por definir un origen y un destino a la información que propagan. Cuando se diseña y configura una red que opera con protocolos ruteables, cada segmento físico de la red debe definirse como una red lógica. Esto aplica tanto a segmentos LAN como a segmentos WAN.

2.1.2.2.-PROTOCOLOS ORIENTADOS A CONEXIÓN Y NO CONEXIÓN.

Volviendo a la analogía del servicio de correo , hay protocolos ruteables que se asemejan a un servicio de correo certificado. En éste el cartero nos devuelve un acuse de recibo firmado por el destinatario en el momento de la recepción. De esta forma se garantiza que el mensaje (carta) ha sido llevado a su destino sin contratiempos. De igual forma, algunos protocolos ruteables solicitan un "Acknowledgement" . Es decir, un reconocimiento por parte del destinatario de que éste ha recibido el paquete de información.

Puesto que éste proceso se realiza miles de veces durante una sesión normal de trabajo, el efecto final es como si ambos nodos mantuvieran una conversación constante entre ellos, y tal pareciera que las computadoras se encontraran conectadas entre si mediante una "conexión" virtual. A estos protocolos se les conoce como protocolos orientados a la conexión (Conection Oriented Protocol).

Los protocolos ruteables que no se orientan a un conexión (Conectionless Protocols), son como el correo ordinario. Si usted envía una carta y nunca le contestan, no tiene manera de saber si ésta llego al destinatario o simplemente se extravió. De igual manera los protocolos orientados a no conexión no garantizan que la información transmitida se envíe íntegramente.

La mayoría de los protocolos ruteables que operan en capa 3 del modelo OSI no son orientados a conexión. Para ofrecer un servicio orientado a la conexión requieren de un protocolo de capa superior. Tal es el caso por ejemplo de IPX, que no está orientado a conexión, pero que lo consigue transfiriendo información al protocolo de capa superior inmediata que si está orientado a la conexión, en esté caso el protocolo SPX. Lo mismo podemos decir del protocolo IP con su protocolo superior TCP.

La ventaja de los protocolos no orientados a la conexión sobre los otros es que por lo general son más rápidos; ya que no tienen que ejecutar algoritmos de verificación de transmisión y tampoco tiene que esperar los de reconocimiento (Acknowledgements) de los paquetes transmitidos. Sin embargo estos protocolos no detectan ni corrigen

errores, ni se recuperan de fallas en la transmisión. En la mayoría de los casos dejan estas tareas a los protocolos de capas superiores.
En los siguientes cuadros podremos ver los protocolos ruteables más importantes y sus principales características.

Nombre	Tipo	Desarrollado Por	Usado por	Direcciones de
IPX/SPX	Estándar de la Industria	Novell Inc.	Novell Servidores de aplicación y diversos clientes	4 Bytes para red y para nodo

Características

El Internetwork Packet eXchange / Secuenced Packet eXchange, es el protocolo que se usa en la arquitectura de Novell. Introducido en el mercado en 1983, opera virtualmente sobre cualquier plataforma de Hardware. IPX no es orientado a la conexión, SPX si lo es. Otros protocolos auxiliares son RIP (Routing Information Protocol), para el intercambio de información de ruteo, SAP (Service Advertiting Protocol), que regula las sesiones de trabajo entre servidor y cliente. Existen varios clientes que se comunican con el file server usando IPX, entre estos podemos citar Macintosh, UNIX, OS/2 , DOS, Windows NT, Windows for Workgroups etc. IPX está adecuado para redes de área local, pero no se recomienda para enlaces de red de área amplia a velocidades superiores de 64Kbps, aunque existen técnicas para mejorar su rendimiento.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
OSI	Estándar Internacional	ISO	DEC fase V, otras con arquitecturas abiertas	48 bits

Características:

El modelo OSI también define sus propios protocolos, para las capas de red y de transporte. A nivel de red OSI propone los protocolos. CNLS (Connection Less Network Service) y CONS (Connection Oriented Network Service). Como sus nombres lo indican, el primero en un protocolo de red no orientado a la conexión y el segundo si lo es. OSI también propone un protocolo de red derivado de X25, éste se conoce como X.25 nivel 3.
Para la capa de transporte OSI utiliza una serie de protocolos que proveen diferentes tipos de servicios. Esos protocolos se identifican como TP0, TP1, TP2 y hasta TP4. Tp es por Transfer Protocol y mientras que TP0 es un producto muy sencillo con servicios simples, los demás van aumentando su grado de complejidad y los servicios que ofrecen, hasta llegar al TP4.
A pesar de que el modelo OSI define toda una familia de protocolos y servicios muy completos, muy pocas arquitecturas de computo lo han adoptado.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
TCP/IP	Estándar de la Industria	DoD USA	UNIX, Netware, SNA Windows NT , OS/2 y muchos clientes mas	4 Bytes para la red y nodo

Características.

El Transmision Control Protocol / Internet Protocol, busca facilitar la comunicación entre computadoras de múltiples arquitecturas. Se le encuentra prácticamente en todas las arquitecturas de computo actuales IP no es orientado a la conexion, pero TCP si lo es. Desarrollado desde principios de los años 70's, hoy en día es uno de los protocolos utilizados a nivel mundial. TCP/IP se utiliza para definir a una familia de protocolos que proveen múltiples servicios de Internetworking, entre los que destacan ARP (Address Resolution Protocol), para mapear direcciones lógicas en físicas. RIP (Routing Information Protocol), para intercambio de información de ruteo, ICMP (Internet Control Mesage Protocol), que reporta condiciones de error de la red, UDP (User Datagram Protocol), Protocolo de transporte similar a TCP pero no es orientado a conexión, FTP (File Transfer Protocol), usado para transferencia de archivos, TELNET, que provee servicios de emulación de terminal, NFS (Network File System) , que provee acceso transparente a diferentes sistemas de archivo, RPC (Remote Procedure Calls), sirve para disparar procesos remotos, SNMP (Simple Network Management Protocol), usado para el control, monitoreo y administración de los dispositivos que componen la red, etc.
La familia de protocolos de TCP/IP provee mecanismos de detección de fallas y en ocasiones puede recuperarse de ellas. Esto lo sitúa como uno de los protocolos más usados para conexiones tanto LAN como WAN.
Una de las grandes ventajas de éste protocolo es que puede operarse sobre muy diversas plataformas de hardware de comunicaciones, esto ha provocado que pueda encontrarse en una heterogénea mezcla de arquitecturas tanto de cómputo como de comunicaciones.

Nota.- En la actualidad ya pueden convivir en un mismo ambiente IP e IPX

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
PPP	Estándar de la Industria	Internet Activities Board	Equipos de Comunicaciones que atienden TCP/IP	8 bits en Capa 2 4 bytes en capa 3

Características:

El Point to Point Protocol es un protocolo síncrono de comunicaciones para enlaces WAN tipo Punto a Punto. Forma parte del set de protocolos de TCP/IP, pero es considerado como un protocolo para WAN, porque permite encapsular información que no necesariamente debe de ser TCP/IP. Este protocolo entiende el concepto de "red" en el sentido de que conoce de que red viene y a que red va, pero no es un protocolo que permita integrar redes LAN con WAN en forma transparente, debido a que PPP es un vínculo entre redes, y cada segmento configurado con PPP es una red por si sola.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de:
Apple Talk	Estándar Propietario	Apple Computer	Macintosh, Netware, Windows NT	2 Bytes p/red 1 byte p/nodo

Características:

Apple Talk no solo es una familia de protocolos, sino también una arquitectura. Originalmente para servir a las redes de computadoras Macintosh, pero se ha convertido en uno de los protocolos más socorridos, para cuestiones de interoperabilidad. Muchas otras arquitecturas se comunican con Apple Talk para integrarse al mundo de las Macintosh. Todos los protocolos de esta familia están diseñados para facilitar las tareas que el usuario tiene que hacer para crear una red de computo, debido a la filosofía de la compañía Apple Talk requiere para su operación crear no solo redes lógicas por segmento físico, sino también grupos lógicos de redes llamados "zonas". Entre los principales protocolos que contiene la familia son: DDP (Deliver Datagram Protocol), éste no está orientado a la conexión y es el responsable de mover los datos entre redes; NBP (Name Binding Protocol), que se encarga de convertir los servicios de red en un nombre comprensible para el usuario y las aplicaciones; ZIP (Zone Information Protocol)
sus mensajes propagan la presencia de las "zonas" lógicas de la red; ATP(Appletalk Transaction Protocol), similar a DDP pero si es orientado a conexión; RTMP (Routing Table Maintenance Protocol), su propósito es mantener actualizadas las tablas de ruteo en los Ruteadores que operan con los protocolos de Apple Talk
Debido a que se trata de una arquitectura propietaria que cubre por completo las siete capas del modelo OSI , Apple Talk cuenta con muchos otros protocolos que le dan la característica principal que consiste en simplificar las tareas que debe hacer el usuario para accesar no solo a las computadoras sino a la red y a todos sus servicios.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de:
X25	Estándar Internacional	CCITT	Practicamente por todas las arquitecturas de comunicaciones	15 bytes

Características:

Se desarrollo en la segunda mitad de los años 70's para crear redes de comunicaciones para múltiples plataformas de computo que operan sobre una red publica de paquetes conmutados. TelePAC y TeleNET son ejemplos de éste tipo de redes. Hoy en día los costos de instalación de éste tipo de redes han bajado considerablemente, de tal forma que se pueden crear redes de paquetes conmutados de carácter privado. Esencialmente X.25 es un protocolo para crear redes WAN. Cada enlace de WAN es un segmento de red de una inter-red X25. Se puede instalar sobre cualquier medio físico de comunicaciones remotas como líneas telefónicas, enlaces satelitales, microondas, enlaces digitales RDI, etc. Su instalación se recomienda para enlaces de baja velocidad hasta no más de 256KBPS . X.25 es un protocolo orientado a la conexión y utiliza el concepto de circuitos virtuales para crear esa conexión lógica. Muchos protocolos modernos que caen dentro de la denominación de "paquetes conmutados" debe su desarrollo a las experiencias con el protocolo de X.25.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
DecNet	Estándar Propietario	Digital Equipment	Equipos DEC Gateways y Clientes	2 Bytes (6 bits para la red 6 bits para red en fase IV)

Características :

Siendo una arquitectura propietaria, cuenta con una serie de protocolos que cubren todos los servicios de red. Sin embargo, DecNet se caracteriza por se una arquitectura abierta, lo que le da la versatilidad para integrarse con otras plataformas tanto con protocolos propietarios como estándares, sobre todo en DecNet fase V, donde DecNet optó por los protocolos propuestos en el modelo OSI.
Dada la enorme cantidad de estos equipos en el mundo, sobre todo de fase IV, se considera que sus protocolos son ruteables. Las redes en DecNet fase IV se denominan "áreas" y éstas pueden extenderse por varios segmentos físicos, pero un Ruteador que "entiende" DecNet puede mover la información de un área a otra en un verdadero proceso de ruteo.
DecNet fase V, DEC mantiene un firme compromiso de mantener su arquitectura abierta y compatible con el modelo OSI, esto lo demuestra al integrar como parte de sus serie de protocolos, los especificados en las capas del modelo OSI.

Los protocolos que llevan la información en DecNet fase IV no son orientado a la conexión , pero se utilizan varios protocolos de control para mantener las sesiones de trabajo, entre ellos tenemos a DRP (DecNet Routing Protocol), que se encarga de las funciones de ruteo y transporte de información; y NSP (Network Services Protocol) que equivale a un protocolo de la capa de transporte que está orientado a la conexión.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
Frame Relay	Estándar Internacional	CCITT	Mayor parte de la arquitectura de las comunicaciones	10 bits (actual) 17 bits (futuro) 24 bits (futuro)

Características:

Muchas de las características de X.25 se pueden encontrar en Frame Relay. También es un protocolo orientado a la conexión, y opera bajo el concepto de conmutacion de paquetes, puede instalarse en redes publicas o privadas, y al igual que X.25 el tamaño de sus paquetes es variable. Frame Relay puede funcionar sobre cualquier plataforma de redes remotas. Es adecuado principalmente para funcionar a velocidades mayores a 64 Kbps; y una de las ventajas que tiene sobre X.25 es un protocolo desarrollado hace casi 20 años y que fue diseñado para proteger la información que viajaría por las líneas telefónicas poco confiables, tarea que consume muchos recursos en los equipos de comunicaciones. Frame Relay aprovecha la confiabilidad de los enlaces digitales modernos y su recursos se enfocan al manejo eficiente de la información que transporta.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
ATM	Estándar Internacional	ATM forum	Principales fabricantes de equipo de Internetworking	2 bytes

Caracteristicas:

ATM es un protocolo ruteable orientado a la conexion, que utiliza técnicas de conmutación de celdas de información . La conmutación de paquetes permite que el tamaño de las unidades de información sea variable, en conmutación de celdas, este valor es fijo. ATM opera a altas velocidades de transmision llegando incluso hasta los 2 Gbps, y como sus unidades de información son fijas, puede transportar lo mismo voz, datos e imágenes en tiempo real. Otra caracteristica fundamental de ATM, es que es un producto que define desde las primeras capas del modelo OSI y permite extender los servicios de las LAN a toda clase de redes con enlaces WAN. Esta versatilidad permite una amplia aceptación para el diseño y la implementacion de futuras interredes.

2.1.3.-¿ QUE SON LOS ROUTERS? .

Los Enrutadores (Routers) son dispositivos de interconexión de redes conceptualmente similares a los LAN Switches, pero con la diferencia fundamental que los Ruteadores trabajan en capa 3 del modelo OSI (capa de red); ver capítulo 1.

2.1.3.1.- ¿ COMO TRABAJAN ?.

Su funcionamiento se basa básicamente en las tablas de ruteo, donde se encuentran localizadas otras redes, la trayectoria para llegar a ellas y la relativa eficiencia de las trayectorias o rutas.

Los Ruteadores no usan las tablas para encontrar la dirección específica de un dispositivo de otra red, sino para seleccionar la mejor ruta por donde enviar cada paquete.

El Ruteador recibe únicamente paquetes direccionados a el, ya sea una estación final (dirección fuente) o por otro Ruteador.

Basado en la dirección de la red del destino final contenido en la tabla, determina a cual red enviar el próximo paquete, ocurriendo el proceso de ruteo de "salto en salto".

2.1.4.- INTERIOR Y EXTERIOR GATEWAY PROTOCOL.

Dos Ruteadores que intercambian información son referidos como "vecinos". Los Ruteadores pertenecientes al mismo sistema autónomo son llamados "vecinos interiores", y los pertenecientes a diferentes sistemas autónomos son llamados "vecinos exteriores".

2.1.4.1.- INTERIOR GATEWAY PROTOCOL (IGP).

Los Ruteadores con un solo sistema autónomo de comunicación usan uno de varios de los protocolos de ruteo, conocido generalmente como Interior Gateway Protocol (IGP). La comunicación continua es necesaria para alcanzar dinámicamente el ruteo e intercambiar información con cada Ruteador, ya que esto reflejará el estado de la topología de la red actual.

El rendimiento es la clave principal del IGP. El algoritmo de ruteo debe responder inmediatamente a fallas, y debe encontrar la ruta de costo mas baja hacia la red destino.

Dos ejemplos de Interior Gateway Protocol son el Routing Information Protocol (RIP) y el Open Shortest Path First Protocol (OSPF).

2.1.4.2.- EXTERIOR GATEWAY PROTOCOL.

La comunicación entre Ruteadores pertenecientes a diferentes sistemas autónomos requieren un protocolo adicional. Este tipo de protocolo es llamado Exterior Gateway Protocol (EGP). Los Ruteadores que ejecutan EGP, también deben de ejecutar IGP para obtener información acerca de su propio dominio. Cada sistema autónomo es libre de seleccionar el IGP que mejor cubra sus necesidades, pero todos los sistemas de comunicación autónomos deben usar el mismo EGP.

Cuando se rutea entre diferentes sistemas autónomos, existe generalmente una pequeña coordinación de administración entre las regiones. También existe algo de falsedad en la información obtenida de otros sistemas autónomos, por ejemplo, el administrador de la red no puede prevenir fallas a ocurrir en otras redes privadas. Como resultado, se deben de crear barreras para prevenir los efectos de tales fallas y su esparcimiento hacia otras redes privadas.

Existen mayores políticas de ruteo y control para EGP que para IGP. Dos de los más populares EGP's son la revisión para el primer Exterior Gateway Protocol (EGP2) y el border Gateway Protocol (BGP).

2.1.5.- ALGORITMOS DE RUTEO ESTADÍSTICO VS RUTEO DINÁMICO.

Hay dos técnicas básicas usadas por los host's y Ruteadores para obtener la información almacenada en sus tablas de ruteo. Los algoritmos de ruteo pueden variar en sus respuestas, de usar rutas estáticas teniendo los cambios en las rutas dinámicamente en respuesta a los cambios en el estado opcional de los recursos de la red.

2.1.5.1.- ALGORITMO DE RUTEO ESTÁTICO.

- El administrador de la red guarda una tabla de las redes, y manualmente actualiza estas tablas siempre que exista un cambio en el dominio del ruteo.

- El sistema estático no opera bien en un ambiente de rápido crecimiento o rápido cambio. Las tablas de ruteo no pueden ser completamente responsables en caso de fallas dado que los Ruteadores de respaldo pueden necesitar usar los recursos o dispositivos de la red dañada.

- Cuando son añadidas nuevas redes, la topología física cambia, cada Ruteador en el dominio debe de tener estas tablas actualizadas manualmente. Esto puede requerir una cantidad de tiempo de parte del administrador de la red.

- Los errores de configuración en las tablas de ruteo estático en grandes redes, pueden ser difíciles de encontrar o corregir.

2.1.5.2.- ALGORITMO DE RUTEO DINÁMICO.

- Los algoritmos de ruteo dinámico responden automáticamente a los cambios en la topología de la red.

- Los esquemas de ruteo dinámico automáticamente incorporan estos cambios añadiendo ó borrando entradas de sus tablas de ruteo.

Dos tipos de algoritmo de ruteo dinámico son usados por las redes de computadoras manteniendo sus tablas de ruteo y calculando la ruta más corta hacia el destino.

Estos son "algoritmo distancia-vector" y algoritmo "link-state" (también conocido como primera ruta más corta).

Todos los algoritmos deben usar métricas para seleccionar la mejor ruta hacia el destinatario. La ruta más corta entre redes es determinada examinando todas las rutas hacia el destinatario y seleccionando la ruta que tenga la métrica más corta.

2.1.5.3.- CONSTRUYENDO LAS TABLAS DE RUTEO.

Típicamente, la mayoría de Ruteadores usan una combinación de técnicas estáticas y dinámicas para obtener información de las tablas de ruteo.

Cada Ruteador primero establece un conjunto inicial de rutas. Esta información es usualmente obtenida leyendo las tablas de ruteo del disco de arranque. La información de esta tabla es proporcionada por el administrador de la red y generalmente incluyen las redes conectadas y posiblemente algunas rutas estáticas de redes remotas.

Una vez que las tablas de ruteo se han convertido en residentes de la memoria, el Ruteador debe de tener la habilidad de responder a las nuevas rutas o cambios en la topología de red. En una pequeña red, la tabla de ruteo puede ser actualizada y administrada por el administrador de la red.

2.1.5.4.- ALGORITMOS DE VECTOR-DISTANCIA.

2.1.5.4.1.-OPERACIÓN BÁSICA.

En los algoritmos de vector-distancia, el Ruteador envía a sus vecinos las distancias de sus vectores (sus tablas de ruteo). Esto es, cada Ruteador conoce la longitud de la ruta más corta de cada uno de sus Ruteadores vecinos hacia todas las redes destinos. Los Ruteadores usan esta información para registrar las rutas más cortas hacia cada destino eligiendo al vecino con la ruta más corta disponible.

2.1.5.4.2.- DESVENTAJAS.

Dependiendo del tamaño de la red, el promedio de información intercambiada entre vecinos puede ser demasiado grande.

En los algoritmos de ruteo de vector-distancia, cada Ruteador transmite información hacia sus vecinos acerca de las rutas de cada otro destino de la red. Es imposible para otros Ruteadores checar esta información con precisión . Como resultado, es difícil para un Ruteador ignorar automáticamente la información proporcionada por un Ruteador dañado o desincronizado. También, dado que la información transmitida por cada Ruteador está en la información que recibe de sus vecinos inmediatos, la identificación de Ruteadores corrompidos o mal sincronizados puede ser bastante difícil.

Un cambio en la tabla de ruteo de algún Ruteador puede traer como resultado una cadena de actualizaciones. Puede tomar bastante tiempo para que esta información alcance a todos los Ruteadores del dominio.

Finalmente, un algoritmo de vector-distancia no es adecuado para grandes redes.

2.1.5.4.3.-VENTAJAS.

Los algoritmos de ruteo vector-distancia han sido usados por muchos años. por lo tanto, muchas implementaciones están disponibles y son bien conocidos por los desarrolladores de software.

Los algoritmos de vector-distancia requieren solo un pequeño número de ciclos de CPU para determinar la ruta más corta hacia la red apropiada.

2.1.5.5.- ALGORITMOS LINK-STATE.

2.1.5.5.1.- OPERACIÓN BÁSICA.

En los algoritmos de ruteo Link-State, cada Ruteador debe de conocer completamente la topología de red antes de registrar la ruta más corta hacia cada destino de la red. Cada Ruteador envía mensajes de actualización a cada Ruteador del dominio. Estos mensajes contienen la métrica y el estado de cada uno de los Ruteadores conectados al enlace. Las rutas son consistentes por que cada Ruteador esta usando el mismo algoritmo de ruteo en bases de datos idénticas.

Cada cambio en la topología es detectado por el Ruteador local y reportado a todos los otros Ruteadores del dominio. Cada nodo tiene toda la información requerida para calcular la ruta de mínimo costo por si mismo hacia cualquier otra red en el dominio de ruteo.

2.1.5.5.2.- DESVENTAJAS.

Una gran cantidad de memoria puede ser requerida en grandes redes dado que cada Ruteador debe mantener actualizada la base de datos que contiene la completa topología de la red.

El algoritmo Link-State requiere más promedio de tiempo de uso de CPU para cálculos comparado con el algoritmo de ruteo vector-distancia.

2.1.5.5.3.- VENTAJAS.

Cada Ruteador mantiene una vista constante de la red, esto elimina los problemas de los loops y ajustes lentos en los cambios de condiciones de la red.

Los Ruteadores corrompidos son fáciles de detectar cuando se usa un algoritmo de link-state porque cada Ruteador mantiene una base de datos idénticas.

Los algoritmos de Link-State pueden eliminar los problemas que ocurren en redes muy grandes debido a la habilidad de particionarse en áreas de sistemas autónomos.

2.1.6.- TABLAS DE RUTEO.

Un Ruteador examina sus tablas de ruteo para determinar como enviar un paquete. Si el destinatario está directamente conectado a la red, el Ruteador libera el paquete sin usar los servicios de otros Ruteadores. Si el destinatario está en una red remota, el Ruteador debe enviar el paquete hacia otro Ruteador más cerca del destinatario final. La ruta hacia una red remota puede ser configurada estáticamente, o aprender dinámicamente a través de un protocolo de ruteo tales como RIP, OSPF, EGP.

La siguiente figura ilustra un ejemplo de entradas en una tabla de ruteo.

DIRECCIONAMIENTO DESTINO 140.5.0.0

NEXT ROUTER	HOPS	OWNER	TIME
140.5.3.2	3	RIP	145
140.5.4.7	3	RIP	170
140.5.3.9	6	RIP	25

Cada entrada en la tabla de ruteo incluye la siguiente información que determina como un paquete es ruteado hacia una ruta particular seleccionada.

Destination Address .- La dirección IP de la red destino, subred o host.

Next Ruteador.- La dirección IP del Ruteador remoto al cual el Ruteador local debe enviar el paquete antes de que el paquete sea ruteado hacia su destino.

Hop Count.- El número de saltos entre el Ruteador y el destinatario.

Owner.- El nombre del protocolo de ruteo que proporciona esta entrada a la tabla de ruteo.

Timer.- El promedio de tiempo desde que la entrada fue actualizada.

2.1.6.1.- RUTEO MULTI-RUTAS.

Para cada dirección destino (red, subred o host) algunos Ruteadores soportan múltiples rutas. Esto significa que el Ruteador puede enviar paquetes hacia el destinatario a través de varias rutas. Estas rutas, aprendidas o configuradas, son almacenadas en una tabla de ruteo. La habilidad de rutear paquetes a través de diferentes rutas es llamado "ruteo multi-rutas".

Algunas ventajas del ruteo multi-rutas son:

• Si la ruta primaria falla, el Ruteador puede seguir enviando paquetes usando una ruta alternativa. Como resultado, el Ruteador puede responder inmediatamente a los cambios en la topología de la red.

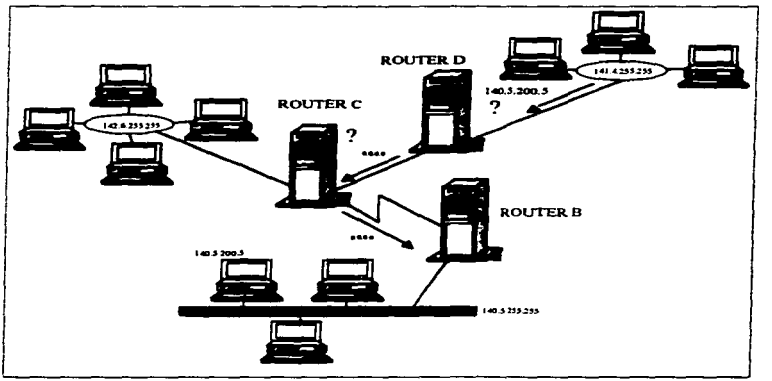
* Si existe más de una ruta apropiada, el administrador puede seleccionar la más adecuada mediante el método de round-robin.

2.1.6.2.-RUTAS POR DEFAULT.

El Ruteador debe descartar un paquete si no encuentra una ruta hacia el destinatario en su tabla de ruteo. Sin embargo, si una ruta default ha sido definida, el Ruteador debe enviar el datagrama hacia el Ruteador identificado como la ruta default. La ruta default es identificada como una ruta hacia la red 0.0.0.0. Todo el tráfico destinado para un destinatario que no está explícitamente listado en la tabla de ruteo debe enviarlo hacia el Ruteador con la métrica más baja hacia la red 0.0.0.0.

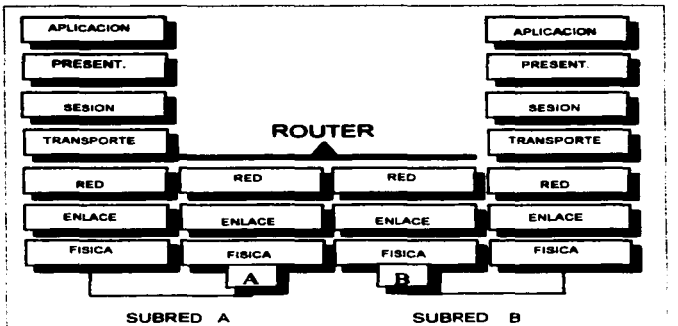
Las rutas default son normalmente definidas cuando no se desea listar cada red en los mensajes de actualización de las tablas de ruteo.

En la siguiente figura el Ruteador D aprende la ruta default a través del Ruteador C. El Ruteador D debe de considerar al Ruteador C como su ruta default. Esto es, el Ruteador D necesita rutear un paquete hacia un destino que no está en su tabla de ruteo, este envía el paquete hacia el Ruteador C. El Ruteador C debe continuar enviando el paquete hacia la ruta default.



2.2.- RUTEADORES.

2.2.1.-MODELO DEL RUTEADOR DE ACUERDO CON EL MODELO OSI.



MODELO DEL ROUTER DE ACUERDO A OSI

En éste modelo de comparación podemos ver que el Ruteador hace el enlace de ambas redes ocupando las últimas tres capas del modelo OSI pero trabajando fundamentalmente en la capa tres (capa de RED).

2.2.2.- PARAMETROS BÁSICOS QUE DEBE MANEJAR UN RUTEADOR:

- Diferentes esquemas de direccionamiento.
- Diferentes tamaños máximos de paquetes.
- Diferentes interfaces de red.
- Diferentes "tiempos-fuera".
- Técnicas de enrutmiento.

- Control de acceso.
- Recuperación de errores.
- Servicios "Orientados a conexión" y servicios "Orientados a no conexión".

2.2.3.- RUTEADOR DE PAQUETES.

Las características de los Ruteadores de paquetes son las siguientes:

Una de las principales características de los Ruteadores es que aíslan el tráfico, son capaces de saber que ruta es la más congestionada y cual es la más despejada para el envío de información.

Sus ventajas y desventajas con respecto de los LAN Switches se verán más a fondo en el capítulo 4 pero por ahora solo las mencionaremos.

2.2.3.1.- VENTAJAS.

- Tienen funciones de Ruteo.
- Es capaz de escoger la ruta más optima para el envío de paquetes (la más corta, la más barata y la que contenga menos saltos).
- Los Ruteadores son capaces de segmentar paquetes.
- También detectan y a su vez se hacen cargo de los "LOOPS".

2.2.3.2.- DESVENTAJAS.

- Los Ruteadores son dependientes de los protocolos, esto es que en el protocolo debe venir la información necesaria para saber cual es el destino final de la información .
- Los protocolos como LAT (DEC) no proporcionan la información necesaria para la función de enrutar los paquetes.
- manejan mayor procesamiento de la información, esto es porque tienen que manejar hasta la capa tres del modelo OSI y esto lleva más tiempo.

2.2.3.3.- COMO SE MUEVEN LOS PAQUETES A TRAVÉS DE LA RED.

1.- La capa de transporte particiona los mensajes en paquetes (datagramas) de un tamaño máximo fijo. Al final en la computadora destino, la capa de transporte reensambla .

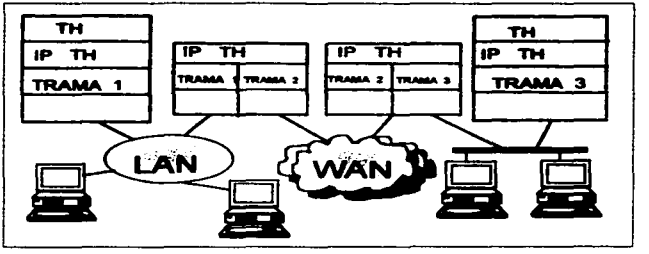
2.- Los paquetes son encapsulados y desencapsulados según el formato de la capa de enlace correspondiente a la red por donde está pasando.

3.- El Ruteador deberá tomar una decisión de enrutamineto de acuerdo a:

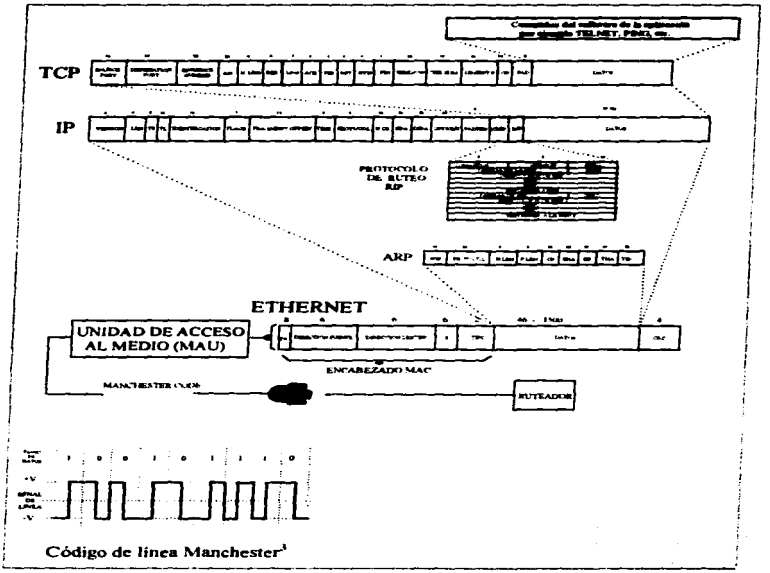
a) La computadora B está conectada directamente en la misma red que el Ruteador.
b) Para alcanzar a la computadora B (estación destino) ¿ Cuántos Ruteadores deben ser visitados?.
c) El Ruteador ¿ conoce la dirección destino?

Todas estas consideraciones deberá tomar en cuenta el Ruteador para poder enviar los paquetes a la dirección exacta contenida en el protocolo, ésta dirección es la que ya conocemos como IP.

En la siguiente figura se podrá observar mejor.



Analizando las tramas, de una manera más detallada se observaría de la siguiente manera:



Código de línea Manchester[1]

[1] Para mayor información de códigos de línea consultar APENDICE B

2.2.4.-CARACTERÍSTICAS IMPORTANTES DEL CONJUNTO DE PROTOCOLOS TCP/IP.

* Es el conjunto de protocolos de red y de transporte utilizados en la red INTERNET.
* Conjunto de protocolos de red utilizados naturalmente en UNIX.
* Excelente para interconexión de redes multivendedor, ya que fue diseñado para operar en un ambiente abierto a redes.
* Muy robusto ya que fue diseñado para funcionar en enlaces de comunicación de baja velocidad.
* También fue diseñado para soportar un ambiente de comunicaciones similar a los utilizados en redes locales tipo CSMA/CD, Mediante Datagramas.
* Adecuado para comunicaciones computadora a computadora.
* Sus aplicaciones son:
  - Login remoto (TELNET, RLOGIN).
  - Transferencia de archivos (FTP, TFTP, NFS).
  - Correo electrónico (SMTP).
  - Administración Internet (SNMP, CMOT).

2.2.4.1.-FUNCIONES PRINCIPALES DEL PROTOCOLO IP.

* Control de nombres y traslación.

* Estado de las comunicaciones.
  Mensajes de Estado.
  Destino no alcanzado invalido.
  Tiempo fuera.

* Enrutamiento de mensajes.
  Decisión de Ruteo.
  Parámetro de tiempo de vida.

* Fragmentación y reensamble.

* Tipo de servicio.
  Trayectoria de bajo retardo.
  Trayectoria de alto ancho de banda.
  Trayectoria de alta seguridad.

IP es uno de los dos principales protocolos utilizados en la interconectividad de sistemas, este protocolo proporciona tres importantes definiciones:

1.- IP define la unidad básica de transferencia de datos usada a través de Internet TCP/IP. Esto es, especifica el formato exacto de datos que pasan a través de la red Internet.

2.- El Software de IP ejecuta las funciones de ruteo eligiendo la ruta por la cual los datos serán enviados.

3.- IP incluye un conjunto de reglas que incorporan la idea de liberación de paquetes. Las reglas caracterizan cómo los hosts y los Ruteadores deben procesar los paquetes, cómo y cuándo los mensajes de error deben ser generados, y las consideraciones bajo las cuales los paquetes pueden ser desertados.

El protocolo IP es responsable de transferir bloques de datos a través de un conjunto de redes interconectadas. IP recibe este bloque de protocolos de alto nivel tales como TCP o UDP, y entonces los transmite a través de Internet.

IP provee servicios de desconexión entre estaciones finales, cada datagrama transporta el direccionamiento destino y es ruteado a través del sistema independiente de el resto de los datagramas.

No se establecen conexiones o circuitos lógicos.

IP también proporciona un mecanismo de fragmentación y reensamble de datagramas para la transmisión a través de redes en las cuales el máximo tamaño de paquete es más pequeño que le tamaño del datagrama.

El módulo de software IP reside en todos los hosts y Ruteadores del sistema Internet, éstos módulos comparten reglas comunes para interpretación de campos de direccionamiento, fragmentación y ensamble de datagramas a través de Internet. Adicionalmente, estos módulos tienen procedimientos para hacer decisiones de ruteo y otras funciones de ayuda, tales como mensajes ARP o ICMP.

La comunicación en Internet es posible a través del paso de datos del módulo Internet de una máquina, al módulo Internet de otra máquina, hasta que el datagrama alcanza su destino final.

El datagrama es ruteado de una máquina a otra basada en el direccionamiento Internet transportado en el encabezado antes de alcanzar su destino final.

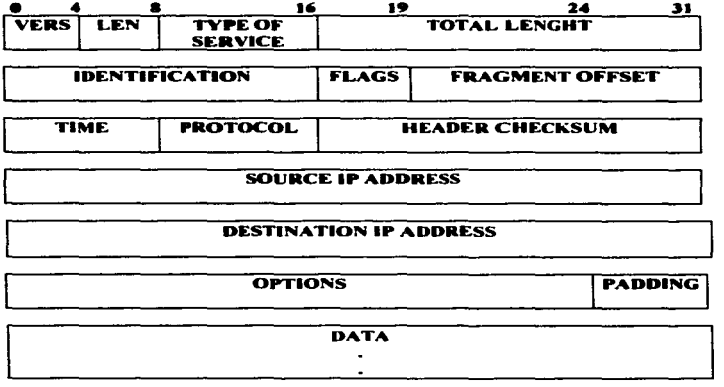
2.2.4.2.- DIRECCIONAMIENTO IP.

El propósito fundamental del IP es mover datagramas a través de conjuntos de redes interconectadas. Los datagramas son ruteados de un módulo Internet a otro a través de redes individuales basadas en la interpretación de direcciones Internet. Por lo tanto, una importante característica del IP es la implementación y el reconocimiento del direccionamiento Internet.

Como se vio en el capitulo 1, el direccionamiento Internet está formado por campos de 32 bits divididos en campos de cuatro octetos. El direccionamiento propio consiste en dos partes:
La parte de red y la parte de host.

Como se recordará, existen cuatro clases de direccionamiento de formatos, A, B, C, y D, mencionados en el capitulo anterior.

2.2.4.3.- FORMATO DEL DATAGRAMA IP



La longitud máxima del campo de datos más encabezado es igual a 8192 Bytes = 65536 bits.

- VERS.- (Versión Number) Es un campo de 4 bits que contiene el número de Versión de IP.
- LEN .- (Header Length) Contiene la longitud del encabezado.
- TYPE OF SERVICE .- El tipo de servicio que se requiere para la transmisión de datagrama IP (retardo, ruta, seguridad).
- TOTAL LENGHT.- Contiene la longitud total del datagrama, identifica un fragmento (datagrama fragmentado) de los otros en que se fragmento el datagrama original.
- FLAGS.- Indica si un datagrama esta fragmentado o no.
- FRAGMENT OFFSET.- Define la posición de un datagrama fragmentado en el datagrama original.
- TIME TO LIVE.- Indica el tiempo que un paquete deberá existir (generalmente incrementos de un segundo).
- PROTOCOL.- Usuario IP al cual los datos le serán entregados.
- HEADER CHECKSUM.- Cálculo para la verificación de errores.
- SOURCE IP ADDRESS Y DESTINATION IP ADDRESS.- Contiene la dirección IP del destino y de la fuente del datagrama , etc.
- PADDING .- Relleno para asegurar que el encabezado terminará en un múltiplo de 32 octetos.

2.2.4.4.- NÚMEROS ASIGNADOS EN EL CAMPO "PROTOCOL" PARA PROTOCOLOS QUE USAN IP.

1 CIMP (Internet Control Message Protocol).
2 GGP (Gateway-to-Gateway Protocol).
5 STREAM.
6 TCP (Transmisión Control Protocol).
8 EGP (Exterior Gateway Protocol).

9 Cualquier IGP (Interior Gateway Protocol).
17 UDP (User Datagram Protocol).
20 HMP (Host Monitoring Protocol).
22 XNS-IDP (Xerox Network System - Internet datagram Protocol).
27 RDP (Reliable Datagram Protocol).
29 ISO TP4 (ISO class 4 Transport Protocol).
61 Cualquier Protocolo Internet de Host.

2.2.5.- RUTEO IP.

2.2.5.1.- ARQUITECTURA DE INTERNET.

El sistema Internet puede ser visto como una colección de Hosts y redes interconectadas a través de Ruteadores IP. El protocolo IP fue diseñado para soportar comunicaciones entre hosts heterogéneos o redes heterogéneas. Los Ruteadores son dispositivos que conectan dos o más redes y controlan el tráfico de datos en ellas.

Dos hosts en la misma red son capaces de enviar paquetes uno al otro, también, cada red es capaz de aceptar paquetes de una red remota y liberarlos hacia un destino especifico de la red local.

Los Ruteadores envían paquetes basados en el número de red destino, y no en la dirección física de los hosts destino. Dado que el ruteo es basado en números de red, el promedio de información que el Ruteador necesita es primordial al número de redes que forman Internet, no el número de máquinas.

2.2.5.2.- RUTEO DENTRO DE INTERNET.

El ruteo ocurre en diferentes niveles. Por ejemplo, en una red de área local con múltiples conexiones físicas, la red es responsable de rutear los paquetes desde que entran hasta que salen. Dado que el ruteo interno está considerado en el interior de la red de área ancha. Los dispositivos en el exterior no pueden participar en las decisiones; ellos solamente ven a la red como una entidad que libera paquetes.

Rutear dentro de Internet puede resultar difícil, especialmente entre dispositivos con múltiples conexiones físicas. Idealmente, el software de ruteo debe examinar condiciones como carga de tráfico en la red, longitud del datagrama, o el tipo de servicios especificando en el encabezado del datagrama cuando se elige la mejor ruta.

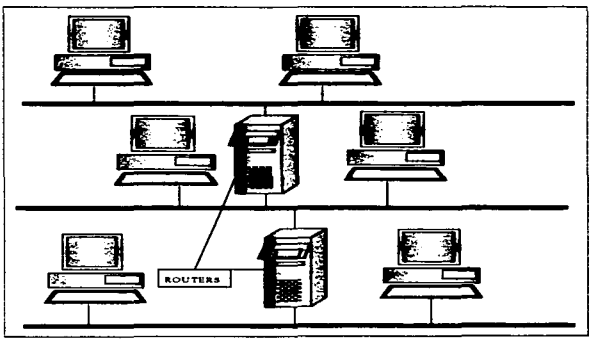
2.2.5.3.- RUTEO DIRECTO.

El ruteo se puede dividir en dos formas: ruteo directo y ruteo indirecto. En el ruteo directo la transmisión de paquetes dentro de una misma red de una máquina a otra es directa y no requiere los servicios de un Ruteador.

2.2.5.3.1.- LIBERACIÓN DE PAQUETES SOBRE UNA MISMA RED.

Sabemos que una misma máquina conectada en una red puede enviar una trama directamente a otra máquina en la misma red. Para transmitir un datagrama IP, el transmisor encapsula el datagrama dentro de un frame físico, mapea la dirección IP destino dentro de un direccionamiento físico y usa el hardware de la red para deliberarlo. En este caso, el direccionamiento fuente IP y el direccionamiento Ethernet fuente son asignados al host fuente y los direccionamientos IP y Ethernet destino son asignados al host destino.

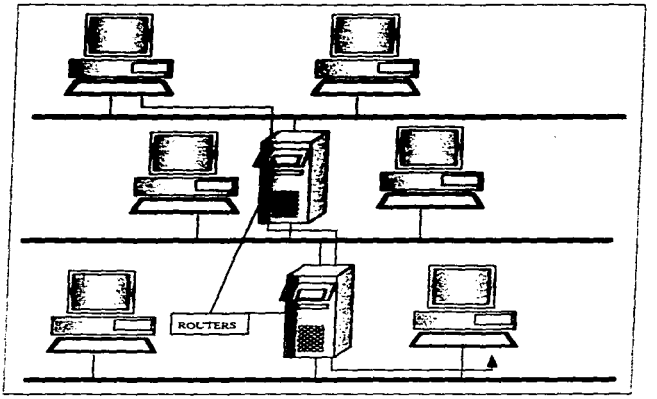
La distribución es el paso final en la transmisión de Datagramas, aunque el datagrama atraviese muchas redes y Ruteadores intermediarios.
El Ruteador final a lo largo de la ruta entre el datagrama origen y su destino lo conectará a la misma red física del destinatario. Esto es, el Ruteador que finalmente libera el datagrama usa ruteo directo.



2.2.5.4.- RUTEO INDIRECTO.

El ruteo indirecto ocurre cuando el destinatario no está directamente conectado a la red. Esto requiere que el host origen envíe el datagrama a un Ruteador para que lo libere. Este tipo de ruteo es más complejo debido a que el host fuente debe de identificar no solamente el destinatario final, sino también el Ruteador a través del cual debe pasar el datagrama. Es entonces, trabajo del Ruteador enviar el datagrama hacia la red destino.

Para visualizar como trabaja el ruteo indirecto, imaginemos una gran red con varias redes interconectadas con Ruteadores pero con solo dos hosts en los extremos. Cuando un host quiere enviar al otro, encapsula el datagrama y lo envía al Ruteador mas cercano. Una ves que el frame alcanza al Ruteador, El software extrae el datagrama encapsulado, y la rutina del ruteo IP selecciona el próximo Ruteador a lo largo de la ruta hacia el destinatario. El datagrama es nuevamente colocado dentro de un frame y enviado sobre la siguiente red física al segundo Ruteador, y así sucesivamente hasta que pueda ser deliberado directamente.



2.2.5.5.- UTILIZANDO LAS TABLAS DE RUTEO.

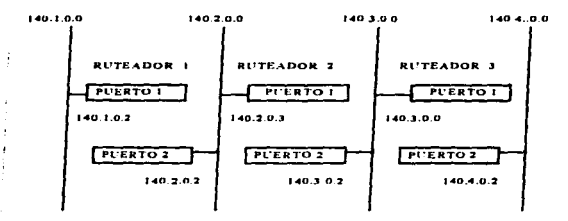
Un Ruteador IP toma la decisión de transmitir los datagramas buscando en sus tablas de ruteo. El Ruteador ejecuta esta tarea usando una clave de búsqueda, la cual consiste en el número de red IP obtenido del campo de direccionamiento de cualquier datagrama IP.

Si el destinatario está directamente conectado a la red, el Ruteador libera al paquete directamente sin usar los servicios de otro Ruteador. Si el destinatario está en una red remota, el Ruteador debe enviar el paquete a otro Ruteador cerca del destino final.

Mantener correctamente las tablas de información de todos los Ruteadores en una red Internet grande es una tarea difícil. Las tablas de ruteo deben mantenerse dinámicas para reflejar la topología actual del sistema Internet. Para cumplir esta tarea el Ruteador normalmente participa en ruteos distribuidos y algoritmos con otros Ruteadores.

Algunos de los protocolos de ruteo usados para intercambiar información en la red incluyen al protocolo de información de ruteo (RIP), el Open Shortest Path Firts Protocol (OSPF), el Exterior Gateway Protocol (EGP) y el Border Gateway Protocol (BGP). Dependiendo de la estructura de Internet, algunos Ruteadores pueden participar en más de un protocolo de ruteo IP.

La siguiente figura ilustra una Internet compuesta de cuatro redes y tres Ruteadores.



EJEMPLO DE UNA
INTERNET PEQUEÑA

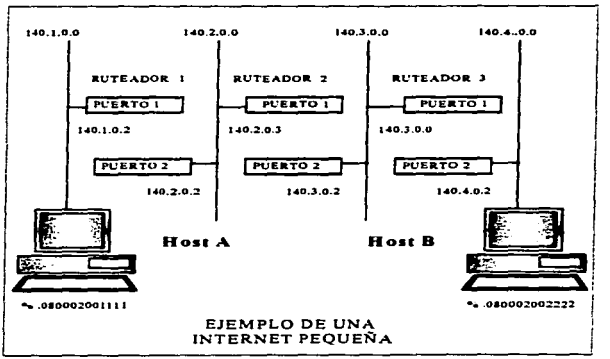
El Ruteador A usa el Protocolo de Resolución de Direccionamiento (ARP) para encontrar el direccionamiento físico que corresponda al direccionamiento Internet para cualquier host que esté directamente conectado a su red.

Las tablas de ruteo contienen una fila para cada Ruteador . Las columnas de las tablas de ruteo incluyen el número de red IP destino, el direccionamiento IP del siguiente salto del Ruteador, y la métrica la cual es usada para seleccionar el menor costo de ruteo si existe más de una ruta existente para la red destino.

2.2.6.- RUTEADOR DE DATAGRAMAS.

2.2.6.1.- MODOS DE OPERACIÓN.

El modo de operación para transmitir un datagrama de un host a otro sobre Internet se muestra en la figura. Este ejemplo involucra al host origen (host A), y al host destino (host B), tres Ruteadores intermedios y cuatro distintas redes físicas. Internet y el direccionamiento Ethernet para cada host y cada punto del Ruteador también son desplegados.



EJEMPLO DE UNA INTERNET PEQUEÑA

La ruta que el datagrama toma no es determinada por el Ruteador central, es el resultado de examinar cada una de las tablas de rutas usados en la jornada. Cada Ruteador define solo el siguiente Ruteador y así sucesivamente para enviar el paquete IP.

2.2.6.1.1.-HOST A.

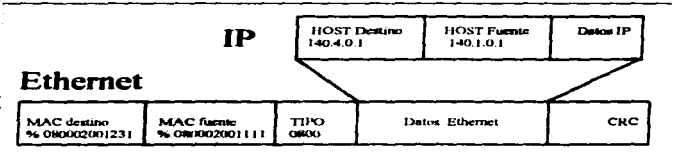
El host "A" en la red 140.1.0.0 desea conectarse con el host "B" en la red 140.4.0.0 usando el protocolo TELNET. Como el paquete es mandado de un Ruteador a otro, el encabezado IP definido por el host A permanece constante. El único direccionamiento que cambia al mover los paquetes hacia su destino final son el direccionamiento Ethernet origen y destino.

2.2.6.1.2.- PAQUETES EN LA RED 140.1.0.0.

Dado que el host "A" y el host "B" radican en diferentes redes, el host "A" debe ejecutar ruteo indirecto y usar los servicios de un Ruteador IP. Al final de la inicialización, el host "A" ha aprendido que el direccionamiento IP del Default Gateway es el 140.1.0.2.

Como resultado, el host "A" sabe que debe de usar al Ruteador "A" para transmitir paquetes a cualquier host residente en una red diferente. Si el host "A" no tiene ninguna entrada en su cache ARP para el dispositivo 140.1.0.2, debe enviar un requerimiento ARP y esperar que el Ruteador responda.

Dado que existen mapeos de direccionamiento, el host A transmite un frame Ethernet con un direccionamiento MAC destino % 080002001231 (Ruteador A), el direccionamiento MAC origen % 080002001111 (host A), y un tipo de campo 0800h (IP). La estructura del paquete colocado en la red 140.1.0.0 se muestra en la figura:



Paquete en la Red 140.1.0.0

2.2.6.1.3.-PAQUETES EN LA RED 140.2.0.0.

Después de recibir el paquete, el Ruteador "A" remueve el encabezado Ethernet y pasa el datagrama a un proceso IP. El proceso IP examina el número de red destino contenido en el encabezado IP, y localiza la ruta hacia la red 140.4.0.0 en las tablas de ruteo (tabla).

El Ruteador "A" sabe que la red destino está a dos saltos aún, y que debe enviar el datagrama al Ruteador B a la dirección IP 140.2.0.3 El Ruteador "A" debe hacer un requerimiento ARP y esperar que el Ruteador "B" si éste no tiene el direccionamiento mapeado en su cache ARP. Finalmente, el Ruteador "A" transmite un frame Ethernet sobre el puerto 2 con el direccionamiento MAC destino %0.80002001200 (Ruteador B), al direccionamiento MAC fuente %o80002001232 (puerto 2 del Ruteador A) y al tipo de campo 0800h (IP).

2.2.6.1.4.- PAQUETES EN LA RED 140.3.0.0.

Después de recibir el paquete, el Ruteador B remueve el encabezado Ethernet y pasa al datagrama a un proceso IP. El proceso de rutas IP examina el número de red destino contenido en el encabezado IP y localiza la ruta a la red 140.4.0.0 en la tabla de ruteo (tabla). El Ruteador B aprende que la red destino está a un salto aún, y que debe enviar el datagrama al Ruteador C a la dirección IP 140.3..0.0.

El Ruteador "B" debe hacer un requerimiento ARP, y esperar que el Ruteador "C" responda si no tiene la dirección mapeada en su cache ARP. Una vez que el mapeo es obtenido, el Ruteador "B" transmite un frame Ethernet sobre el puerto 2 con el direccionamiento MAC destino %080002001235 (Ruteador "C"), al direccionamiento MAC fuente %080002001234 (puerto 2 del Ruteador "B"), y al tipo de campo 0800h (IP). La estructura del paquete para la red 140.3.0.0.

2.2.6.1.5.- PAQUETES EN LA RED 140.4.0.0.

Después de recibir el paquete, el Ruteador "C" remueve el encabezado Ethernet y pasa el datagrama al proceso IP. El proceso IP examina el número de red destino y el encabezado IP y localiza la ruta a la red 140.4.0.0. en la tabla de ruteo el Ruteador "C" descubre que la red destino está directamente conectada al puerto 2, por lo que el Ruteador "C" puede liberar el datagrama directamente.

El Ruteador "C" debe hacer un requerimiento ARP y esperar a que el host "B" responda (Si este no tiene el direccionamiento mapeado en su cache ARP). una vez obtenida la dirección, el Ruteador "C" transmite el frame Ethernet sobre el puerto

2 con la dirección MAC destino %080002002222 (host "B"), a la dirección MAC fuente %08002001236 (puerto 2 del Ruteador "C").

2.2.6.1.6.- HOST B.

El host "B" recibe el paquete, remueve el encabezado Ethernet, y pasa el requerimiento al modulo IP. El proceso IP determina que el datagrama es direccionado al host local, remueve el encabezado IP, y pasa esto a TCP para futuros procesos. TCP examina el número de puerto y pasa el datagrama a la entrada de la cola para el proceso TELNET.

2.2.6.2.-INTERNET CONTROL MESSAGE PROTOCOL (ICMP).

El protocolo de control de mensajes en Internet (ICMP) es un requerimiento del protocolo Internet (IP) esto significa que todos los host que implementan IP deben implementar ICMP.

La función básica del ICMP es proveer un mecanismo que permita a los Ruteadores o host destino responder si existe un error en el proceso de envio de bloques de datos.

Algunos ejemplos de cuando usar los mensajes de ICMP son:

- Cuando el Ruteador no tiene la capacidad de buffers para reenviar el datagrama.
- Cuando el host o Ruteador descubren un error en el encabezado IP.
- Cuando el Ruteador no tiene una ruta para la red destino en su tabla de ruteo.
- Cuando el Ruteador debe descartar un datagrama porque la cuenta del tiempo de vida expiro.

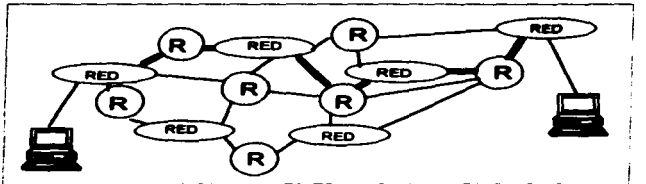
La función principal de ICMP es proporcionar retroalimentación entre varios problemas que pudieran ocurrir en el medio-ambiente de la comunicación.

Los mensajes de ICMP son encapsulados como una porción de los datos del datagrama IP como resultado, son ruteados como cualquier otro datagrama IP. Como los mensajes ICMP son transmitidos en el datagrama IP, el transmisor no puede garantizar que estos serán liberados hasta su último destino.

Dado que los mensajes ICMP no pueden ser considerados confiables, no existe garantía de que puedan ser perdidos o descartados.

2.2.7.- RESUMEN Y TRAMAS DE LOS PROTOCOLOS DE ENRUTAMIENTO.

Enrutamiento se refiere al proceso de elegir una trayectoria sobre la cual enviar paquetes de datos:



PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento aparecieron a finales de los años 70's y principios de los 80's, cuando las organizaciones comenzaron a formar interredes.

Algunos de los protocolos de enrutamiento más populares son:

RIP (Routing Information Protocol)	- ARPANET
IGRP (Interior Gateway Routing Protocol)	- CISCO
OSPF (Open Shortest Path First)	- ARPANET
IS-IS (Intermediate System - Intermediate System	- OSI
BGP (Border Gateway Protocol)	- ARPANET
I-IS-IS (Integrated IS-IS)	- DECNET (Propietario)
AURP(Apple Talk Update- Base Routing Protocol	- APPLETALK (Propietario)

2.2.7.1.- PROTOCOLOS DE ENRUTAMIENTO.

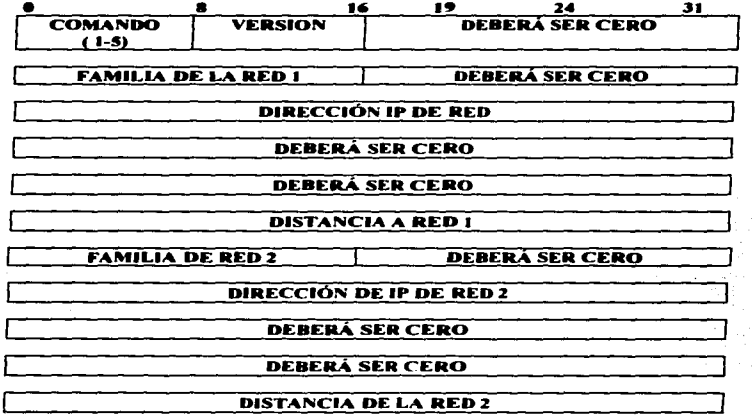
	IS-IS de ISO	IS-IS Integrado	OSPF	IGRP	RIP
Estándar ISO	ISO-10589	DEC Propietario	NO	NO	NO
Pilas de Protocolos Soportados	OSI-CNLP	OSI-CNLP TCP/IP DECNET	TCP/IP	OSI-CNLP TCP/IP	TCP/IP
Tipo "Link" State Protocol	SI	SI	SI	NO	NO
Soporte de "Tipo de Servicio"	SI	SI	SI	NO	NO
Actualización de información	Unicamente los cambios	Unicamente los cambios	Unicamente los cambios	Tabla de enrutamiento	Tabla de enrutamiento
Soporte de Autenticación	SI	SI	SI	NO	NO

2.2.7.2.- PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (ROUTING INFORMATION PROTOCOL, RIP).

- Basado en el protocolo RIP (Routing Information Protocol) de Xerox XN.
- El estándar RFC 10589 apareció en junio de 1988, para las aplicaciones de INTERNET.
- Utiliza la mejor trayectoria disponible entre dos puntos en una red, basado en el número de saltos existentes entre esos dos puntos (protocolo vector-distancia).
- Cada nodo envía una copia de su tabla completa de ruteo a cada uno de sus nodos adyacentes, sin importar si hubo cambios o no (cada 30 segundos).

- También se utiliza en aplicaciones Novell, 3Com, APPLE, BANYAN y APOLLO, como base de sus protocolos propietarios.

2.2.7.2.1.- FORMATO DEL MENSAJE RIP.



* COMANDO.- Especifica una de las siguientes operaciones:

COMANDO	SIGNIFICADO
1	Requerimiento para información parcial o total de enrutamiento.
2	Respuesta del conteniendo de pares Red-distancia desde la tabla de enrutamiento del enviador.
3	Obsoleto
4	Obsoleto
5	Reservado para uso interno de SUN MICROSYSTEMS.

* VERSIÓN.- Versión del protocolo RIP (Actualmente 1).

* **FAMILIA DE RED.- Identifica el protocolo bajo el cual la dirección de red deberá ser interpretada (Para IP el valor es 2, y para IPX el valor es 3).**

* **DISTANCIA DE RED.- Contiene en número de saltos para alcanzar la red deseada (Máximo 15 saltos).**

2.2.7.2.2.- ALGUNAS REGLAS DE RIP PARA MEJORAR SU CONFIABILIDAD Y RENDIMIEMTO.

* **Una vez que un Ruteador aprende una dirección desde otro Ruteador, él deberá mantener esa ruta hasta que una nueva ruta tenga estrictamente menor costo.**

* **Las rutas son invalidas si después de que pasen 180 segundos la ruta no ha sido advertida otra vez.**

* **Utiliza un valor bajo (16) para la distancia máxima posible, para minimizar problemas por bucles de trayectoria (LOOPS), o "cuenta al infinito".**

2.2.7.3.- OSPF , EL PROTOCOLO DE ENRUTAMINETO SPF (SHORTEST PATH FIRST) ABIERTO.

Características principales:

* **Estándar abierto (RFC 1247) , se espera que reemplace protocolos propietarios.**

* **La decisión de ruteo está basada en el " Tipo de servicio" (Bajo retardo, Alto rendimiento, Bajo costo, etc.).**

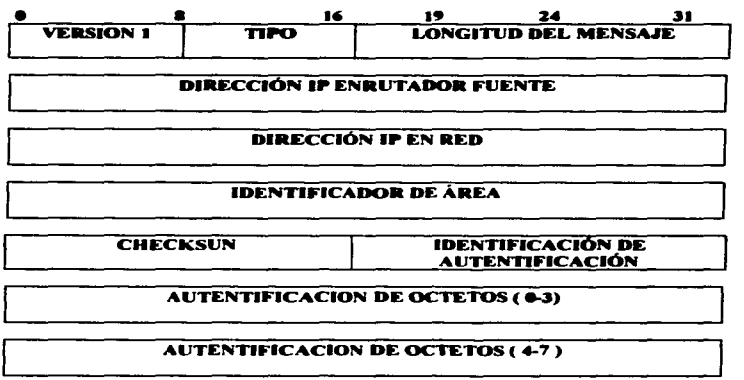
* **Permite el balanceo de cargas.**

* **Autenticación de todas las comunicaciones entre Ruteadores.**

* **Soporte de rutas específicas por el HOST.**

* **Envía actualizaciones de su tabla de ruteo solo si han ocurrido cambios en el estado de los enlaces (rutas).**

2.2.7.3.1.- FORMATO DEL MENSAJE OSPF



- VERSION.- Versión del protocolo.
- TIPO .- Especifica el tipo de mensaje.

TIPO	SIGNIFICADO
1	Hello.
2	Descripción de la base de datos.
3	Requerimiento de estado de enlace.
4	Actualización de estado de enlace.
5	Reconocimiento de estado de enlace.

- DIRECCIÓN IP ENRUTADOR.- Dirección IP del Ruteador que envía la información.
- IDENTIFICACIÓN DE ÁREA .- Número de identificación del área donde se encuentra el Ruteador.

* TIPO DE IDENTIFICACIÓN .- 0 = No autenticación, 1 = Password utilizado

* AUTENTIFICIACIÓN .- Password

2.2.7.3.2.- FORMATO DEL MENSAJE "HELLO" DE OSPF

ENCABEZADO OSPF CON TIPO = 1		
MASCARA DE LA RED		
TIPO DE MUERTE	ENTRE "HELLO	PRIORIDAD DE ROUTER
ROUTER DESIGNADO		
ROUTER DESIGNADO DE RESPALDO		
DIRECCIÓN IP, VECINO 1		
DIRECCIÓN IP, VECINO 2		
. . .		
DIRECCIÓN IP, VECINO n		

* ENCABEZADO.- Mensajes entre pares vecinos, que se intercambian periódicamente para probar " ALCANZABILIDAD".

- MÁSCARA DE RED.- Máscara para la red por la cual el mensaje tiene que ser enviado.
- TIEMPO DE MUERTE.- Tiempo en segundos, después del cual un vecino que no responde es considerado no disponible.
- ENTRE "HELLO" .- Periodo normal en segundos entre mensajes "Hello".
- PRIORIDAD DEL RUTEADOR.- Prioridad del Ruteador usado en seleccionar un Ruteador designado de respaldo.
- ROUTER DESIGNADO.- Contiene la dirección IP del Ruteador al cual es enviado el mensaje.
- ROUTER DESIGNADO DE RESPALDO.- Igual que el anterior para el Ruteador de respaldo.

2.2.7.4.- DIRECCIONAMIENTO EN REDES NOVELL.

Los identificadores de nodos (NODO ID) son de 48 bits; representados por grupos de números de cuatro dígitos en hexadecimal, separados por puntos. El Formato es: Número de red, Dirección de Host.

Las Direcciones del Host son representadas por números hexadecimales de 16 bits.
Ejemplo: 1A.0000.0000.25fe
1A: Número de red.
0000.0000.25fe : Dirección del Host.

Las direcciones físicas de los nodos son identificados por números hexadecimales de 32 bits.

2.2.7.4.1.- INTERNETWORK PACKET EXCHANGE (IPX).

- Protocolo de capa de red orientado a no conexión (Datagrama).
- Es el protocolo IDP de XNS.
- Diseñado para operar en un ambiente de red Ethernet.
- Máximo tamaño de paquete es de 576 octetos (30 octetos del encabezado y 546 de datos).

2.2.7.4.1.1.- FORMATO IPX.

FORMATO DEL PAQUETE IPX

- CHECKSUN.- Campo conforme a XNS, Novell no lo utiliza y siempre es FFFF.
- LONGITUD.- Tamaño del Datagrama IPX (Mínimo 30 octetos y máximo 576 octetos).
- CONTROL DE TRANSPORTE.- Contabiliza el número de veces que el datagrama pasa por el Ruteador (máximo 16)..
- TIPO DE PAQUETE.- Define el protocolo de nivel superior al cual la información del paquete deberá ser entregada.

  0 = Unknown Packet Tipe.
  4 = Packet Exchange Protocol.
  5 = Secuence Packet Exchange.
  17=Netware Core Protocol.

- RED DE DESTINO.- Dirección de red destino (asignado por el administrador de red).
- COMPUTADORA DE DESTINO.- La dirección física del computadora destino (la dirección de la NIC[1]
- SOCKET DE DESTINO.- Especifica el proceso de nivel superior (socket) de destino de la información.
- RED FUENTE, COMPUTADORA FUENTE Y SOCKET FUENTE.- Lo mismo que lo descrito para sus correspondientes parejas del lado destino.
- DATOS.- Los datos de nivel superior.

2.2.7.5.- PROTOCOLO DE ENRUTAMIENTO IS-IS (ISO-10589).

La ISO 10589 define un protocolo de enrutamiento IS-IS (sistema intermedio-sistema intermedio) para ser utilizado con el protocolo de nivel 3 ISO CNLP.

Para hacer más manejable la complejidad de una gran red Internet, define un ambiente de enrutamiento jerárquico. 4 niveles de enrutamiento.

- Enrutamiento de nivel 0 .- Enrutamiento de tráfico entre ES's[2] e IS's[3] en la misma subred.
- Enrutamiento de nivel 1.- Enrutamiento de tráfico entre IS's dentro de la misma área.
- Enrutamiento de nivel 2.- Enrutamiento de tráfico entre diferentes áreas dentro del mismo dominio de enrutamiento.
- Enrutamiento de nivel 3.- Enrutamiento de tráfico entre diferentes dominios.

[1] NIC Network Information Center

[2] ES Sistema Final (computadora)

[3] IS Sistema Intermedio.

2.2.7.5.1.- ALGORITMO DE ENRUTAMIENTO IS-IS.

Se deben de considerar los siguientes aspectos:

* Información necesaria : Topología.
  Costo del salto.

* Métrica de enrutamiento: Preasignada.
  Por retardo.
  Por costo.
  Por probabilidad de error.

* Cálculo de la trayectoria. "algoritmo de enrutamiento de menor costo".

"Dado una red de nodos conectados por enlaces bidireccionales, donde cada enlace tiene un costo asociado con él en cada dirección, define el costo de cada trayectoria entre dos nodos como las suma de los costos de los enlaces utilizados para cada par de nodos, así encuentra la trayectoria de menor costo".

2.2.8.- LA NUEVA TECNOLOGÍA DE RUTEADORES.

2.2.8.1.- RUTEADORES MULTIPROTOCOLO.

Son enrutadores con capacidad de manejar concurrentemente varios protocolos (IP, IPX, OSI, CNLP, X.25 Etc.,)

La mayoría de los enrutadores disponibles en el mercado tienen ésta funcionalidad y más bien depende de como el usuario lo requiera equipados.

2.2.8.2.-FACILIDADES Y CARACTERÍSTICAS CON QUE CUENTAN LOS ROUTERS MULTIPROTOCOLO.

- Conectividad.
- Administración de Tráfico.
- Administración de Red.
- Disponibilidad.
- Mantenimiento del Equipo.
- Características de Rendimiento.

Facilidades de Conectividad:

- INTERFAZ.

  Ethernet.
  Token Ring 4 MBPS.
  Token Ring 16 MBPS.
  FDDI - CDDI.
  Sincrona.

- PROTOCOLOS DE RED.

  TCP IP.
  OSI.
  DecNet FASE IV.
  NOVELL IPX.
  VINES DE BANYAN.
  APPLE TALK FASE 2.
  XNS.

- PROTOCOLOS DE PUENTEO.

  Puentes Transparentes.
  Puentes de Enrutamiento Fuente.
  Puentes de Translación.

* **PROTOCOLOS DE WAN.**

  X.25.
  FRAME RELAY.
  SMDS.
  PPP.
  ATM.

Facilidades de Administración de Tráfico.

PRIORIDAD DEL PROTOCOLO.
FILTRADO DE TRAFICO POR "SOFTWARE"

  Tráfico de Entrada.
  Tráfico de Salida.
  Dirección de Fuente/Destino.
  Red Fuente/Destino.
  Campos Definidos por el Usuario.

Facilidades de Administración de red:

SNMP (Simple Network Managment Protocol) MIBI/RFC 1156.
SNMP MIBI/ RFC1213.
Soporte del Comando SNMP GET/SET.
Soporte de Sistemas de Administración Como:

  SUN NET Manager de SUN.
  OPEN VIEW de HP.

Facilidades de Disponibilidad.

Recuperación Dinámica.
Aislamiento y recuperación de fallas por "software".
Reinicialización parcial del sistema.
Múltiples procesadores de enrutamiento.
Redundancia en "Hardware" del sistema.
Trayectorias de interconexión de procesadores.
Almacenamiento en imagen del software.
Fuentes de alimentación.

Facilidades del mantenimiento del equipo.

HARDWARE:

Autodiagnostico al encendido.
Acceso fácil frontal y trasero.
Luces de indicación de estado del equipo y de los puertos.

CARGA DEL SOFTWARE DEL EQUIPO:

Por disquete.
PROM.
Flash Eprom.
Remota por la red.

CARACTERÍSTICAS DE RENDIMIENTO

Rendimiento en paquetes por segundo.

Nota.- Para informacion a detalle de productos, consultar el capitulo 4

CAPÍTULO 3

LAN SWITCHES,

CONMUTADORES INFORMÁTICOS.

3.1 INTRODUCCION.

3.1.1 ¿QUE ES EL BACKBONE?.

El "Backbone" actúa como conducto primario (o "espina dorsal") del tráfico que usualmente viene de, o va hacia, otras redes. Es el sistema de cableado (normalmente fibra óptica) implantado en la red fundamental para proporcionar todos aquellos servicios (principalmente en redes de área local de alta velocidad) que requieren de este medio como recurso natural para la transmisión de datos, audio y video.

3.1.1.1 ¿QUE ES EL TROUGHPUT?.

El troughput es la medida de capacidad de la red, para transferir información de manera efectiva (trabajo útil de la red).

TROUGHPUT=DATOS TRANSFERIDOS/TIEMPO DE TRANSACCIÓN

3.1.1.2 ¿QUE ES LA LATENCIA?.

La latencia se refiere al tiempo para realizar una transacción de petición-respuesta a nivel de usuario-red. Mientras más fija sea la latencia es mejor el funcionamiento de la red.

3.2 PROTOCOLOS NO RUTEABLES.

Como su nombre lo indica, estos protocolos no son susceptibles de ser ruteados. Si no existe ruteo, no existe el concepto de red lógica. Para este tipo de protocolos el entorno de comunicaciones se desenvuelve en una sola red. Estos protocolos están diseñados para reconocer como único mecanismo de control de comunicaciones entre nodos, las direcciones físicas de los mismos. Esa dirección física es conocida como la dirección MAC (Media Access Control) del nodo.

Retomando la analogía con el servicio de correo, un protocolo no ruteable sería como un servicio de correos donde el único dato para reconocer el remitente y el destinatario serían los números de casa de una sola calle. Es decir, en este servicio de correos solo existe una calle a la cual dirigir la correspondencia. De la misma manera los protocolos no ruteables asumen que se están comunicando nodos de una sola red de área local.

Al conectar varios segmentos físicos de red entre sí, es decir, al crear una interred, ya sea con los segmentos de LAN o segmentos de WAN, debemos utilizar un dispositivo de "Internetworking" conocido como LAN Switch. Un LAN Switch es un elemento de interconexión que solo propaga las direcciones físicas de los nodos. Por ésta razón, los LAN Switches permiten extender los segmentos físicos de la red y hacen parecer a los protocolos no ruteables, como una sola red a todos los segmentos interconectados con LAN Switches. Hay que recordar que no existe el concepto de red lógica desde el punto de vista de los protocolos no ruteables, por lo tanto a estos protocolos solo les interesa saber las direcciones físicas de cada nodo.

Para éste propósito los LAN Switches crean en sus memorias una tabla de direcciones físicas para saber si propagan las tramas en un segmento de red hacia otros segmentos.

Los protocolos no ruteables generalmente no son "comprendidos" por los LAN Switches, por lo tanto la información de control contenida en los paquetes de información no es interpretada por los LAN Switches, la dirección de MAC es suficiente para que los protocolos no ruteables hagan su trabajo de mover información de un nodo a otro. Esto nos lleva a pensar que los protocolos no ruteables propagan la información más rápido que los protocolos ruteables y de hecho un LAN Switch es un dispositivo de "internetworking" más rápido que los Ruteadores. Pero para interredes muy grandes la eficiencia decae con este tipo de protocolos, por otro lado muchos protocolos no ruteables no están diseñados para trabajar en ambientes WAN, porque al asumir que se encuentran en ambiente de una sola red, demandan todo el ancho de banda disponible, que es un lujo que difícilmente nos podemos dar cuando estamos interconectando nuestras redes con enlaces WAN.

Al igual que los protocolos ruteables los no ruteables se dividen en orientados a conexión y orientados a no conexión. Además, los protocolos no ruteables generalmente abarcan los servicios de comunicación de nodos de LAN desde la capa 2 del modelo OSI hasta las últimas capas de éste.

Por ejemplo la trama LLC IEEE 802, va en el campo de datos de la trama de la subcapa MAC. El formato de esta trama es el siguiente:

DIRECCIÓN DSAP	DIRECCIÓN SSAP	CONTROL	INFORMCIÓN

DSAP.- Punto de acceso al servicio de destino.
SSAP.- Punto de acceso al servicio de la fuente.
CONTROL.- Campo de control.
INFORMACIÓN.- Datos de los Usuarios.

En las siguientes tablas encontraremos algunos de los protocolos no ruteables y sus principales características.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
APPC NetBIOS NetBEUI	Estándar Propietario	International Business Machines	Equipos IBM, Gateways y Clientes	12 bytes

Características:

El 60 % de las redes de cómputo hoy en día utilizan algún equipo de arquitectura de IBM SNA (Standard Network Arquitecture). IBM originalmente desarrolló esta arquitectura basada en grandes procesadores centrales que atendían un gran número de terminales tontas. Pero al integrarse a las nuevas tecnologías de LAN , IBM tuvo que idear nuevos protocolos más eficientes. NetBIOS (Network Basic Input Output System), que consiste en un protocolo de alto rendimiento a nivel de LAN y que utiliza las direcciones físicas de cada nodo para mover información; NetBEUI (NetBIOS Extended User Interface) es similar a NetBIOS pero permite encapsular la información en un formato LLC2 que es de reciente creación. APPC (advanced Program to Program Communication) es otro protocolo propietario de IBM más versátil y complejo que los anteriores, pero diseñado para operar con las nuevas interfaces físicas que vienen en los equipos de comunicaciones de la arquitectura SNA de IBM. Todos estos protocolos no ruteables, operan eficientemente en ambientes LAN, pero en WAN consumen muchos recursos y ancho de banda, por lo que no se recomienda su uso a lo largo de una WAN.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
DEC LAT DEC LAN Bridge	Estándar Propietario	Digital Equipment Corp.	Equipos DEC Terminal Servers	12 Bytes (MAC)

Características:

En ciertos equipos de DEC se utiliza el protocolo de LAT (Local Area Transport) principalmente para conectar terminales tontas de minicomputadoras DEC, usando una red Ethernet como medio de comunicación. Este protocolo asume que el servidor atiende a las terminales y siempre está conectado al mismo segmento de la LAN. Esto lo constituye como un protocolo no ruteable. DEC LAN. Bridge es un protocolo de DEC que permite extender las redes de VAX, que son computadoras de tecnología DEC a través de varios segmentos de LAN. Este protocolo consigue su propósito haciendo el trabajo de un protocolo de Switch. Esto implica un dispositivo del tipo Switch que haga estas funciones.

Nombre	Tipo	Desarrollado por	Usado por	Direcciones de
SNA	Estándar Propietario	International Business Machines Corp	Equipos IBM Gateways y Clientes	2 Bytes (WAN) 12 Bytes (LAN)

Caracteristicas:

Presentada en 1974, la arquitectura SNA es una de las más utilizadas debido a la gran aceptación de los equipos IBM que utilizan esta arquitectura. Durante más de una década SNA se mantuvo como una arquitectura monolítica y cerrada, de tal forma que para poder interconectar equipos entre sí debían ser de la misma naturaleza ya que SNA utilizo protocolos y esquemas de comunicación propietarios. Con el éxito que tuvieron las LAN's en la década de los 80's, IBM rompió con su esquema de cómputo centralizado para incursionar en la distribución. Para lograr esto, SNA fue modificado para aceptar información transportada por los protocolos de LAN. Los desarrollos que IBM realizó sobre Token Ring dieron como resultado que aunque el estándar internacional de Token Ring (802.5) se acepta como lo conocemos actualmente, en realidad se trata de una implantación y modificación de Token Ring original hecho por IBM.
SNA operando sobre Token Ring puede utilizar algún protocolo de LAN que no es ruteable.
Los protocolos usados son LLC2 donde un puerto lógico (Services Access Point), es usado para entregar y recibir información que solo los equipos IBM entienden; el otro protocolo usado por IBM es NetBIOS.
Recientemente IBM ha conseguido implantar protocolos ruteables a sus equipos de SNA, ahora ya se pueden encontrar conexiones tanto en Token Ring como Ethernet (FDDI inclusive) , que pueden comunicarse con TCP/IP.
Al adoptar IBM éste tipo de tecnologías se consigue una mejor interconexión de equipos de arquitectura SNA con plataforma de otras arquitecturas diferentes.
Es importante para una buena conectividad al saber si el equipo SNA que pretende ser integrado con otras arquitecturas, está utilizando protocolos no ruteables como LLC2 o NetBIOS o un protocolo ruteable como TCP/IP.

Nombre	Tipo	Desarrollado por	Usado por	
LLC2	Estandar Internacional	Proyecto 802 de la IEEE	Equipos IBM Gateways y Clientes Windows NT Novell OS/2 etc.	12 Bytes (MAC)

Caracteristicas:

El proyecto 802 de la IEEE define dos tipos de encapsulamiento de un Trama para diferentes tipos de LAN; 802.3 para Ethernet y 802.5 para Token Ring, pero define sobre estos un formato más, el 802.2 que le da ciertas ventajas de comunicación cuando se pasa la información de cada trama a las capas superiores. En esas capas pueden estar operando muchos diferentes protocolos de muy diversas arquitecturas. Un método eficiente para entregar esa información, es utilizar un puerto lógico (SAP) a cada uno de los protocolos, así se consigue que con un solo formato de trama pueda intercambiarse fácilmente información de una plataforma a otra . LLC2 asigna un numero de identificación a cada fabricante y/o protocolo de capa superior. Como LLC2 opera en la capa 2 del modelo OSI, se comporta como un protocolo no ruteable, ya que lo único que maneja para llevar información de un nodo a otro es la dirección física.

3.2 TÉCNICAS DE SWITCHEO.

3.2.1 CUT-TROUGHT.

Este método aprovecha la técnica mediante la cual el Switch cut-trought lee solo la dirección MAC destino contenida en cada encabezado de la trama y automáticamente la dirige hacia el puerto al cual está conectado el nodo destino reduciendo así la latencia de la red. Sin embargo, el Switch no está equipado para checar los datos que lleguen con error; por lo tanto, el cut-trought puede tener latencia inferior pero se tendrían que hacer otro tipo de gastos para evitar la propagación de errores a través de la red y en horas pico en la transferencia de datos los Switches Cut-Trought necesitan un buffer con mas capacidad, provocando que la latencia aumente.

3.2.2 STORE-AND - FORWARD (almacena y envía).

Ésta es una técnica de conmutación de mensajes en la cual estos se almacenan temporalmente esperando que la trama llegue completamente, hasta que llega el momento que haya recursos en la red (como por ejemplo enlaces libres) disponibles para su envío.
Este proceso de store-and-forward permite que el Switch verifique los datos entrantes para checar errores incluyendo runts, jabbers y el chequeo de redundancia cíclica (CRC).
Estos errores pueden tener un impacto devastador sobre redes "masticando" anchura de banda suficiente para traer una red a sus rodillas. Específicamente estos errores incluyen:

Los runts, que son las tramas cortas de menos de 64 bytes formadas cuando ocurre una colisión en una red Ethernet, comúnmente cuando existe una carga pesada de trabajo, si estos no son detectados por el Switch, el error de la trama es remitido a todos los puertos del Switch, de tal modo se incrementa la congestión y vence el propósito del Switch.

Los jabbers, que son otro tipo de error de red. En IEEE 802.3 se refiere a un paquete de datos cuya longitud excede a la prescrita en el estándar; esto también puede ser considerado una condición de error en la cual un dispositivo de la red continuamente transmite basura a la red, un Switch que no reconoce a los jabbers "pensara" que ha recibido una dirección MAC, y la enviara nuevamente a los puertos.

con el store-and-forward estos tipos de errores se aíslan en el segmento sobre el cual ocurre, además de que el Switch notifica al administrador de la red tan pronto el problema ocurra.

El CRC indica ruido electromagnético sobre una línea de comunicaciones, ruido que puede minimizar el desempeño de una red activa, el Switch store-and-forward permite a los usuarios detectar este tipo de error.

Por lo tanto se puede ver que mientras los switches cut-trought tienen una latencia mas inferior que store-and-forward, un diseño apropiado de la red puede minimizar las diferencias existentes entre las dos técnicas de switcheo.

El Switch cut-trought está limitado en sus aplicaciones a pequeños grupos de trabajo donde el throughput es un punto a considerar pero en donde los errores de la red no trastornen el potencial de la red en la empresa. En contraste los switches store-and-forward son diseñados para la empresa de amplias aplicaciones donde el chequeo de error y el throughput son los intereses claves..

3.2.3.- HIBRIDOS.

Algunos Switches pueden desarrollar ambas técnicas de enviar datos. Ellos pueden comenzar su operación con Cut-Trought pero cambiar su modo de operación a Store-and-Forward.

Las tramas erróneas (las cuales son detectadas con el chequeo de las secuencias de tramas) quizá se dejen pasar ininterrumpidamente en el Switch hasta que un usuario predeterminado alcance a detectar el error. Cuando cada uno de estos niveles ha sido excedido, el Switch cambia a modo de operación Store and Fordward y detiene la propagación de las tramas erróneas que se enviarían a la red.

La mayoría de los Switches operan en la capa de enlace del modelo OSI y como los puentes, ellos, en cuanto a protocolos son independientes. Muchos vendedores están comenzando a enfocarse más a los Switches debido a las capacidades que se incorporan a los niveles de la red. Este tipo de Switcheo ocurre usualmente en el Software por un microprocesador, esto aparenta ser solo una parte del tiempo antes del nivel tres que se Switchea con el hardware.

Normalmente, el máximo tamaño de las tramas en un ambiente Token Ring es de 4,500 bytes (aunque a 16 MBPS puede soportar tramas por arriba de los 17 Kbytes) que son mucho mas grandes que las de Ethernet que tienen un máximo de 1512 bytes. Los Switches Store and Fordward mostraran un incremento en la latencia cuando el tamaño de los paquetes incremente.

3.3 TECNOLOGÍAS DE ALTA VELOCIDAD EN EL BACKBONE.

Un trabajo de administrador de red no es un trabajo fácil, con la gama de opciones de redes de alta velocidad disponibles se tiene que determinar cual es la más apropiada para implementarse. Algunas redes requieren de diferentes tecnologías en ciertas áreas, mientras que otras tienen requerimientos de aplicación que dictan el uso estratégico de una tecnología en particular, cualquiera que sea el caso, antes de hacer una decisión adquisitiva es fundamental conocer los intereses que persigue la empresa sobre cualquier Backbone de LAN.

A continuación se mencionan algunas de las tecnologías para redes de alta velocidad y sus capacidades dentro del Backbone, esto con el objetivo de que se seleccione la técnica mas apropiada según sus necesidades, recordando que algunas de estas tecnologías ya se mencionaron en capítulos anteriores pero no se tomó en cuenta como influye en el Backbone.

3.3.1 100 BASE T (Ethernet rápido).

Velocidad de operación disponible:(100 Mbps half dúplex, 200 Mbps full dúplex).
Método de acceso al medio: CSMA/CD.
Arquitectura: Shared or Switched.
Topología: estrella.
Cable: UTP categoría 3,4 y 5; STP y fibra óptica.
Distancia: cobre-100 m Fibra-2Km.
Dispositivos soportados: Adaptadores, hubs, Ruteadores, Analizadores y Switches.
Latencia: variable.

La extensión de la IEEE es la especificación 802.3 comúnmente conocida como estándar Fast Ethernet, muchos dispositivos Ethernet apoyan ésta norma, pero el cable UTP categoría 5 tiene unos 100 Mbps - 100 m y el límite de longitud de la red es de 210 m. aunque ésta limitación puede superarse instalando dispositivos que extiendan esta distancia, la limitación puede impedir la eficiencia de 100 base T como un tecnología de Backbone, aunque debido a sus capacidades rápidas es óptima como un conducto para alcanzar el Backbone.

3.3.2 100VG-AnyLAN.

Velocidad disponible: 100 Mbps half dúplex.
Método de acceso al medio: Prioridad de demanda.
Arquitectura: Shared or Switched.
Topología: Estrella y anillo.
Cable: UTP categoría 3, 4 y 5; STP y fibra.

Distancia: cobre 100 m; fibra -2 Km.
Dispositivos soportados: Adaptadores, hubs, Ruteadores y Switches.
Latencia: Variable.

Un competidor fiero de Fast Ethernet es 100VG-AnyLAN, definido por IEEE en la especificación 802.12. La diferencia con 100 base T es que ésta tecnología no apoya la transmisión en full dúplex, 100VG-AnyLAN soporta Token Ring y Ethernet aunque no en el mismo dispositivo, la traducción entre ellos se realiza por medio de un puente o un Ruteador.

La distancia no es un factor limitador como en 100 base-T con el cobre, el diámetro de red sobre la categoría 3 es de 500 m. y 750 m. sobre la categoría 5. Esta tecnología puede dar una cierta prioridad al tráfico sensible al tiempo, como ATM, sin embargo, las aplicaciones deben de ser reescritas para llegar a ser un QoS[1] consciente, son muy pocos vendedores que fabrican Switches 100VG-AnyLAN para el ambiente del Backbone.

3.3.3 ISOCHRONOUS ETHERNET.

Velocidad de operación disponible: 16.144 Mbps half dúplex.
Método de acceso al medio: CSMA/CD.
Arquitectura: Shared or Switched.
Topología: estrella.
Cable: UTP categoría 3,4 y 5; STP.
Distancia : 100 m.
Dispositivos soportados: Adaptadores y hubs.
Latencia: variable en Shared(compartido) y fija en implementación de Switched.

Isochronous Ethernet también conocido como IsoEnet, es desarrollado por el cuerpo de normas de la IEEE, los 16.144 Mbps de ancho de banda se dividen en 10 Mbps para un canal dedicado a transmitir datos y 96 canales B de ISDN de 64 Kbps para transmitir la voz y el video, otro canal maneja la señalización, este sería un canal D a 64 Kbps.

IsoEnet y los 16.144 Mbps no es el ancho de banda suficiente para considerarlo en uso de Backbones; además, ningún Switch esta disponible en este momento.

[1] QoS Calidad del servicio. (Quality of Service).

3.3.4 FDDI/FDDI II.

Velocidad de operación disponible: 100 Mbps half dúplex; 200 Mbps full dúplex.
Método de acceso al medio: FDDI-token-passing.
Arquitectura: Shared or Switched.
Topología: Estrella o anillo.
Cable: UTP categoria 5 ,STP, Fibra.
Distancia Cobre 100 m; fibra-2 Km.

Dispositivos soportados: Adaptadores-FDDI, Ruteadores, hubs, Switches y Analizadores. FDDI II- adaptadores y hubs.
Latencia: FDDI- variable , FDDI II fija.

El comité de ANSI X3T9.5 ratificó FDDI en 1995 y FDDI II en 1994. El mas común es FDDI, el cual se menciono en el primer capítulo. FDDI II divide los 100 Mbps de ancho de banda en canales de 166.144 Kbps, estos a su vez son subdivididos en 96 canales que utilizan protocolos ISDN .

FDDI II tiene dos MAC a fin de multiplexar paquetes y datos sensibles al tiempo al mismo puerto físico. El ancho de banda disponible y el uso difundido de la industria lo ha favorecido para aplicaciones en el Backbone.

3.3.5 HIPPI.

Velocidad de operación disponible: 800 Mbps, 1.6 Gbps half y full dúplex.
Método de acceso al medio: Señalización.
Arquitectura: Switcheo.
Topología: Estrella.
Cable: STP, Fibra.
Distancia: Cobre-25 m; multimodo - 2 Km; un solo modo 10 Km.
Dispositivos soportados: Adaptadores, compuertas, Switches, Ruteadores.
Latencia: Flexible.

HIPPI (Interfaz Paralela de Alto Rendimiento) se definió originalmente en 1988 por el ANSI X3T11. El valor principal de esta tecnología es su velocidad en Gigabits, esta tecnología se desarrollo primero para aplicación en supercomputadoras. La transmisión de datos que provee HIPPI no tiene sentido en el típico ambiente de las LAN, ya que su arquitectura está basada en bus por lo que resulta difícil manejar una tarifa de datos de 1 Gbps.

HIPPI basa sus créditos en el control de flujo de mecanismos para controlar la congestión del tráfico, ésta tecnología carece de un soporte de multicast/broadcast

por lo que para proveer esta funcionalidad los puertos se configuran manualmente para dirigir el tráfico a un puerto específico donde un servidor de multicast/broadcast adjunto a él, proporciona el servicio.

Para alta velocidad sobre distancias mas largas, se está planeando el uso de HIPPI y ATM con base en SONET (red óptica sincrónica).

3.3.6 CANAL DE FIBRA (Fiber Channel).

Velocidad de operación disponible: 100, 200, 400 y 800 Full dúplex.
Método de acceso al medio: determinado por el Header.
Arquitectura: Shared or Switched.
Topología: Estrella o Anillo.
Cable: Fibra, coaxial.
Distancia: Multimodo-175 m, Monomodo - 10 Km, coaxial - 25 m.
Dispositivos soportados: dispositivos de almacenaje y canalización, hubs, Switches.
Latencia: Variable o Fija.

El comité técnico del ANSI X3T11 desarrolló el canal de fibra en 1990 en respuesta a requerimientos de alto rendimiento y aporte de los hubs y periféricos. En esta tecnología se pueden ofrecer diferentes clases de servicios que pueden proveer varios niveles de QoS. El control de flujo es parecido al utilizado en TCP de ventana deslizante, éste permite al canal de fibra construir exitosamente una red de dispositivos que operen a diversas velocidades.

Una desventaja es que no apoya al UTP (Par torcido sin blindaje) y la extensa mayoría de empresas todavía usa categoría 3 UTP.

A pesar de estas diferencias, el canal de fibra acopia mas apoyo, no así como una tecnología de nicho, pero si como una capaz de proveer interconectividad de LAN de alta velocidad.

3.3.7 GIGABIT ETHERNET.

Velocidad de operación disponible: 1000 Mbps half dúplex 2000 Mbps full dúplex.
Método de acceso al medio: CSMA/CD.
Arquitectura: Shared or Switched.
Topología: estrella.
Cable: UTP categoría 3,4 y 5; STP; Fibra.
Distancia: cobre-5 a 100 m; fibra 500 a 2 Km.
Dispositivos soportados: Adaptadores y hubs (preestandar).
Latencia: Variable.

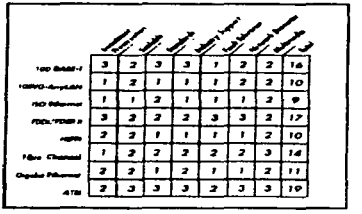
Gigabit Ethernet aliado a IEEE 802.32 son los encargados en desarrollar los criterios necesitados para hacer de esta tecnología una realidad, si bien, la norma no estará lista hasta 1998, la intensión de la alianza es construir sobre el conocimiento y las normas ya existentes para Ethernet y proveer continuidad e interoperabilidad entre 10 Mbps, 100 Mbps, 1000 Mbps, y dirigirse hacia los problemas fundamentales como velocidad y distancia, por lo que se espera que Gigabit Ethernet sea una solución óptima para las LAN's Ethernet.

3.3.8 ATM.

Velocidad disponible: 1.54, 6.3, 25.6, 44.7, 51.8, 100, 155.5, y 622 Mbps (todos teóricamente full dúplex).
Método de acceso al medio: señalización.
Arquitectura: Switched.
Topología: Estrella.
Cable: UTP, categoría 3,4 y 5; STP Y fibra óptica.
Distancia. Cobre 100 m, fibra - 2 Km.
Dispositivos soportados: hubs, Ruteadores, Switches, multiplexores y Analizadores
Latencia: Fija.

Debido a las soluciones que ofrece ésta tecnología (descrita en los capitulo 1 y 2), ATM no podría ser la mejor solución para todas las aplicaciones, pero si dirige el volumen de los intereses que plagan la mayoría de los ambientes LAN ahora y en un futuro previsible.

Los comités técnicos del foro ATM tienen puntos clave recientemente resueltos tal como, control de flujo de mecanismos, acceso a baja velocidad e interoperabilidad entre los vendedores de Switches que permitan despliegue global de ATM.



3.3.9 EMULACIÓN DE LAN ATM.

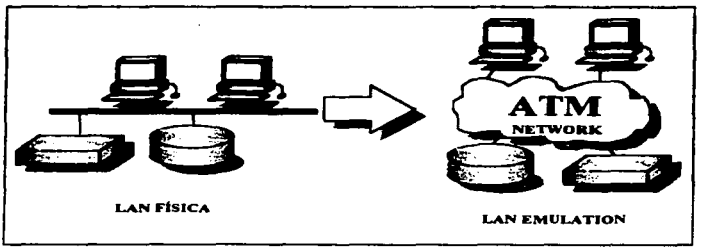
Desarrollada en 1994, la Emulación de LAN (LANE) es un estándar de ATM utilizado para conectar redes Ethernet y Token Ring legadas, a una red ATM.

La especificación de LANE esconde la red ATM de los usuarios y permite que dicha red se vea como un legado de LAN Ethernet o Token Ring. Esto funciona permitiendo a la red ATM emular una red de Control de Acceso al Medio (MAC). Esto permite que todos los puntos finales se envíen el uno al otro, transparentemente, paquetes basados en MAC.

La Emulación de LAN permite que los protocolos de capas más altas que esperan por servicio sin conexión, puedan usar Switches ATM orientados a conexión, Esto requiere de software en clientes y de servicio de emulación de LAN.

sus características son:

- Configuración de administración de red.
  - Resuelve el problema de mover, agregar y cambiar.
  - Red adaptable.
  - Direccionamiento de la capa 3.
- Cada ELAN es un dominio de broadcast independiente.
- Las ELAN's están interconectadas vía un Ruteador.
- Soporta Switches LAN y hosts ATM de la capa 2 de enlace.



Una LAN emulada es un grupo de dispositivos ATM adheridos, incluyendo dispositivos de medio compartido y dispositivos ATM adheridos de lleno. Una ELAN es tratada como un dominio de broadcast independiente, y puede ser pensada como un segmento simple de Ethernet o un Token Ring independiente.

Un frame de tipo broadcast que se origina en una ELAN particular es enviado sólo a miembros de la misma ELAN. Para comunicarse con miembros de otras ELANs, se debe de usar un Ruteador.

La emulación de LAN es equivalente a un protocolo de la capa de enlace de datos, operando en la subcapa de MAC y más abajo. El protocolo de LANE está directamente en la cima del protocolo de ATM y del protocolo de la Capa de Adaptación de ATM (AAL).

3.3.9.1 COMPONENTES DE LANE.

La Emulación de LAN define dos componentes, el cliente de la Emulación de LAN y los servicios de la Emulación de LAN. Los servicios de la Emulación de LAN están constituidos por el Servidor de Configuración de Emulación de LAN (LECS), por el Servidor de Emulación de LAN (LES), y por el Broadcast and Unknown Server (BUS).

Los servicios de LANE pueden estar localizados todos en el mismo dispositivo, o distribuidos entre uno, dos o tres. El Cliente de Emulación de LAN puede estar localizado en el mismo dispositivo como los servicios de LANE.

3.3.9.2 EL LEC (Cliente de la Emulación de LAN).

El cliente de la emulación de LAN (LEC) implementa el protocolo de LANE vía software. El software del LEC debe de estar en cada dispositivo final de ATM que participe en la red LANE, para proveer LANE a sistemas legados.

Un dispositivo de la orilla es un sistema intermedio (Ruteador, Switch o puente) que da servicio de conexión de LANE para estaciones de red Ethernet o Token Ring legada.

El LEC es responsable de las siguientes funciones:

- Envío de datos.
- Resolución de direcciones.
- Funciones de control.
- Interfaces de servicio Ethernet/IEEE 802.3 o IEEE 802.5 emuladas a nivel MAC.

El LEC registra sus direcciones MAC y ATM con el LES.

3.3.9.3 LECS (Servidor de configuración de LANE).

El LECS contiene información de configuración para todas las ELANs en el dominio administrativo. Es responsable de asignar cada LEC a una LAN emulada. Esto lo hace dando al LEC la dirección ATM del Servidor de Emulación de LAN asignado a la ELAN.

Hay un LECS por dominio administrativo. Un dominio administrativo puede ser una compañía o un campus.

El mover una estación a una ELAN diferente, significa que se deben de alterar las tablas contenidas en el LECS.

3.3.9.4 LES (Servidor de Emulación de LAN).

El LES administra las estaciones que constituyen la ELAN. Registra y resuelve todas las direcciones MAC a direcciones ATM utilizando el Protocolo de Resolución de Direcciones de Emulación de LAN (LE-ARP). Los LECS registran todas las direcciones MAC con el LES.

Cuando un dispositivo de la ELAN tiene datos que mandar a otro dispositivo de la ELAN, la estación que envia pide al LES la dirección ATM de la estación destino.

3.3.9.5 BUS (Broadcast Unknown Server).

Todas las LAN's son sistemas broadcast. Es necesario que la LANE emule capacidades de broadcast de sistemas de LAN legados.

El BUS es responsable de manejar los broadcast y los multicast. Cuando se manda un frame tipo broadcast al BUS, éste manda el frame a todas las estaciones en la ELAN, utilizando una conexión de canal virtual (VCC) punto-a-multipunto.

Actualmente se permite un BUS por ELAN, por lo tanto, cada LES puede tener un sólo BUS asociado a él.

3.3.9.6 INTERFACES LANE.

La LANE es un protocolo cliente-servidor. Actualmente, la especificación de LANE en su fase 1 del Forum de ATM, estipula sólo la interacción entre los clientes de LANE (LEC) y sus servidores. No especifica las interfaces ni los protocolos LNNI- entre las entidades del servidor. Esto está siendo checado en la fase 2 del protocolo de LANE.

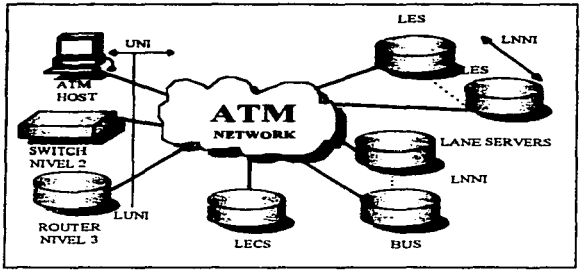
La interface entre los clientes de LANE y el resto de la red que soporta LANE es llamada interfaz de Red del usuario de LANE (LUNI).

3.3.9.7 Interim Local Management Interface (ILMI).

La Interim Local Management Interface (ILMI) provee el intercambio de información de administración entre sistemas ATM que son entidades administradas en SNMP.

La ILMI se comunica utilizando SNMP. Las estaciones finales ATM mantienen una base de información de administración (MIB). Las estaciones finales ATM y los Switches se pueden comunicar utilizando ILMI.

La ILMI es utilizada por los clientes de Emulación de LAN para localizar los LECS inicialmente.



3.3.9.8 MIB I , MIB II (BASE DE MANEJO DE INFORMACIÓ).

El MIB describe los objetos o las entradas, las cuales van incluidas en las base de datos del SNMP. Por esa razón, algunas veces los agentes del SNMP son referidos al MIB. El diagrama muestra algunas entradas del MIB.

Management Information Base (MIB).

TIPO DE OBJETO	DIRECCION DE ROUTER	TIPO DE OBJETO	DIRECION DE RED
SINTAXIS	OCTETOS (4 CADENAS)	SINTAXIS	OCTETOS (4 CADENAS)
ACCESO	LECTURA / ESCRITURA	ACCESO	LECTURA / ESCRITURA
STATUS	MAESTRO	STATUS	MAESTRO
TIPO DE OBJETO	HOP COUNT	TIPO DE OBJETO	[illegible]
SINTAXIS	ENTERO (CONTEO)	SINTAXIS	ENTERO (CONTEO)
ACCESO	LECTURA/ESCRITURA	ACCESO	LECTURA/ESCRITURA
STATUS	MAESTRO	STATUS	OPCIONAL

Los objetos en el MIB son definidos y están desarrollados en la estación que maneja el software, la cual sabe que objetos están disponibles, los nombres de los objetos y el valor de ellos. Ésta información está incluida en la especificación del MIB.

Existen tres categorías de la especificación del MIB, las cuales son la estándar, la experimental y la privada.
MIB estándar: Éste incluye el MIB estándar de objetos determinados, aceptados y ratificados en el grupo de estándares de Internet. El primer estándar MIB es conocido como MIB I, el cual contiene alrededor de 114 objetos. Este pronto será reemplazado por el MIB II, el cual contiene alrededor de 172 objetos. La información de estos MIB's es proporcionada para diseñar y administrar ruteo IP.

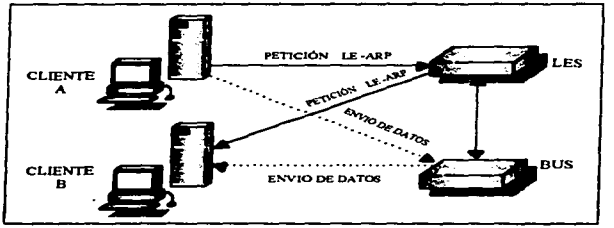
RMON (Monitoreo Remoto): RMON hace una función diferente que el MIB II, este contiene objetos para monitorear la red, y es capaz de proveer información al administrador de la red acerca del promedio de utilización, como checar el número de paquetes con errores etc. RMON puede también ser usado para monitorear dispositivos que no tengan SNMP, es decir actúa como agente protector de estos.

MIB experimental: La categoría experimental incluye MIB con información específica acerca de otros aspectos en la red y dispositivos de administración que son considerados con información valiosa, pero aun no se considera como estándar MIB.

MIB privado: Esta categoría (algunas veces llamado MIB empresarial) es diseñado por compañías individuales que necesitan colectar datos particulares para sus propios dispositivos de red. Ellos definen sus propios objetos. Los objetos en el MIB privado son un producto específico y generalmente no están disponibles en el estándar MIB tradicional.

3.3.9.9 ¿COMO FUNCIONAN LAS LANE?.

Un ejemplo se muestra en la figura siguiente, en donde el cliente A tiene información para el cliente B.



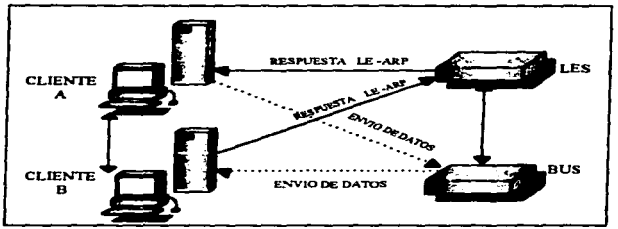
Para que el cliente A le mande información al cliente B, ocurren las siguientes transacciones:

1.- El cliente A conoce la dirección MAC del cliente B, pero necesita aprender su dirección ATM. El cliente A manda una petición del LE-ARP al LES.

2.- Simultáneamente al paso 1, el cliente A empieza a enviar frames de datos al BUS.

3.- El LES checa su tabla del LE-ARP para la dirección ATM del cliente B. Si ésta se encuentra en la tabla, el LES manda la dirección ATM al cliente A. Si la dirección ATM no está en la tabla del LE-ARP, el LES manda la petición del LE-ARP a todos los LECS que están usando la VCC distribuida de control (punto-a-multipunto). Note que si el LEC es un puente, la dirección ATM no estará en la tabla.

4.- Simultáneamente al paso 3, el BUS envía los frames iniciales a todas las estaciones que están usando la VCC de envío multicast(punto a multipunto).



5.- El cliente B responde al LE-ARP mandado por el LES.

6.- El LES transmite la respuesta del LE-ARP(que contiene la dirección ATM del cliente B) al cliente A.

7.- El cliente A establece una VCC directa de datos con el cliente B.

8.- El cliente A manda un mensaje de Flush al BUS. Este mensaje dice al BUS que pare de enviar cualquier frame que no haya sido mandado aún.

9.- El cliente A utiliza la VCC directa de datos para comunicarse con el cliente B.

Cuando dos sistemas finales necesitan comunicarse dentro de la misma ELAN, sus transmisiones de datos son manejadas por los Switches que están en la ELAN.

Si los dos sistemas finales se encuentran en ELANs distintas, un Ruteador o Switch de la capa 3 debe de ser utilizado para interconectar estas ELANs. Esto es verdadero incluso si los dos sistemas finales están físicamente conectados al mismo dispositivo que está en la orilla.

Si la ELAN contiene dispositivos utilizando IP como el protocolo de la capa de red, todos los dispositivos de la ELAN deben ser parte de la misma subred IP. Recíprocamente, los dispositivos en subredes IP distintas no pueden ser miembros de la misma ELAN, puesto que ellos necesitan un Ruteador para comunicarse.

3.4 REDES VIRTUALES DE ÁREA LOCAL (VLAN's).

3.4.1 INTRODUCCIÓN:

Hoy en día el buen desempeño de los Switches para redes de área local (LAN) ofrece a los usuarios una microsegmentación superior, a la vez que ofrece una menor latencia en los paquetes remitidos y aumenta el ancho de banda a través del tendido de la red. Los LAN Switches también pueden segmentar las redes lógicamente definidas dentro de grupos de trabajo virtuales.

Esta segmentación lógica comúnmente es la referencia de las Virtual LAN's (VLAN's) , que en comunicaciones ofrecen un cambio fundamental en el diseño y administración de las redes de área local. Mientras la segmentación lógica provee substanciales beneficios en la administración y seguridad de las LAN emitiendo "broadcast" a través de la empresa para conocer su actividad. Hay muchos componentes de las soluciones VLAN que deben ser considerados anteriores a la larga escala de VLAN que se ha desplegado.

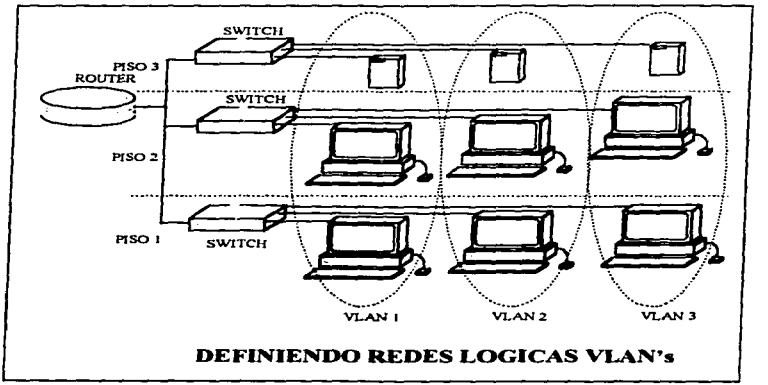
Los componentes adicionales de las VLAN's incluyen también alto rendimiento de los Switches conectados para segmentos lógicos y estaciones de trabajo finales, protocolos de transporte que llevan el tráfico de las VLAN's de la LAN a través del tendido de ATM, soluciones de transporte a nivel de capa tres que extienden las comunicaciones de las VLAN's entre los grupos de trabajo, sistemas compatibles e interoperabilidad con sistemas LAN instalados previamente, además con lo que respecta a la administración de la red ofrece soluciones de control centralizado, configuración y funciones administración del tráfico. Todos éstos componentes son críticos para las soluciones VLAN's de la empresa, debido a que provee la escalabilidad necesaria para emigrar desde una base instalada de LAN, hasta poder compartir las nuevas tecnologías.

3.4.2 CONSTRUYENDO LAS SOLUCIONES VLAN's.

Conceptualmente las VLAN's proveen mayor flexibilidad en la segmentación y en la administración. La tecnología VLAN permite que los administradores de red, puedan agrupar los puertos de los Switches y a los usuarios en comunidades del mismo interés lógico. Estas agrupaciones pueden ser cotrabajadores dentro de un mismo departamento, a través de un mismo equipo de productos funcionales, diversos usuarios compartiendo el mismo software de la red. para ello se debe agrupar puertos y usuarios dentro de comunidades de interés común referidas a la organización que provee las VLAN's dentro de un Switch único o más poderosamente, entre Switches interconectados dentro de una misma empresa.

Agrupando puertos y usuarios juntos a través de múltiples Switches, las VLAN's puede construir infraestructuras de solo una interconexión en una empresa o construir conexiones WAN.

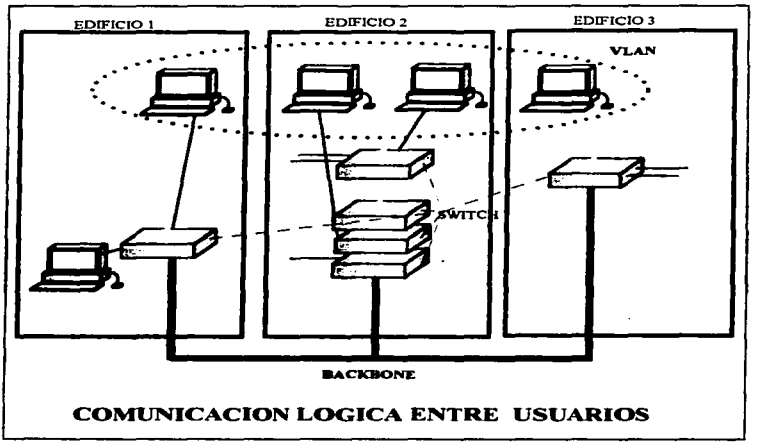
Las VLAN's quitan completamente las limitaciones físicas de comunicaciones en grupos de trabajo a través de la empresa como se ve en la siguiente figura.



DEFINIENDO REDES LOGICAS VLAN's

Las VLAN's proveen a cualquier organización la capacidad para ser físicamente dispersas a lo largo de la compañía mientras puede mantener la identidad de la empresa, por ejemplo. El personal puede mantenerse en el piso de taller, en el centro de investigación y desarrollo, en las oficinas administrativas y en las oficinas corporativas, y todos los miembros de la empresa radican sobre la misma red virtual compartiendo un transito único.

La siguiente figura ilustra una típica arquitectura VLAN que pone a éstos empleados más cerca de sus áreas asignadas por la administración y con la gente con la que ellos laboran recíprocamente, y a la vez, manteniendo integra la comunicación dentro de la organización.



Hoy en día las VLAN's equiparán mejor la manera en que se organizan las compañías y permitirán a los administradores de red alinear más estrechamente la manera en que los empleados trabajan y se comunican.

3.4.3 SWITCHES - EL NÚCLEO DE LAS VLAN's.

Los Switches son el componente fundamental de las comunicaciones a través de VLAN's. Ellos son los que indican la entrada de las workstations finales para fabricar las comunicaciones a través de la empresa.

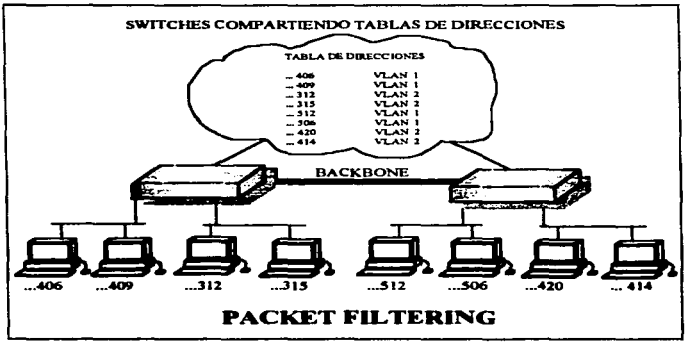
Los Switches proveen la "inteligencia" necesaria para agrupar a los usuarios y a los puertos o direcciones lógicas (IP) en comunidades de interés común. Cada Switch tiene la capacidad y la "inteligencia" de tomar decisiones para filtrar y enviar los paquetes de datos conforme la unidad de medida de la VLAN definida por los administradores de red y para comunicar ésta información a los demás Switches y Ruteadores dentro de la misma red. Y mientras que los LAN Switches se instalan entre los segmentos que comparten los HUB's y los Ruteadores ubicados dentro del Backbone, ellos tomarán un papel de mucho mayor importancia para las VLAN's en cuanto a lo que se refiere a la segmentación y a la latencia, además que son la base para las instalaciones inalámbricas. Los LAN Switches ofrecen importantes aumentos en el desempeño y en el ancho de banda dedicado a través de la red, sin olvidar la inteligencia necesaria para la segmentación VLAN.

Uno de los términos más comunes cuando se definen las VLAN's es el packet filtering y el packet identification. El filtrado del paquete (packet filtering) es una técnica que examina la información particular de cada paquete con base a lo que el usuario definió. La identificación del paquete (packet identification) (etiquetado) singularmente se asigna a un número de identificación a cada paquete. Ambas técnicas examinan el paquete cuando es enviado y recibido por los Switches.

Con base en el conjunto de reglas definidas por el administrador, estas técnicas determinan la dirección de los paquetes (estos mecanismos de control pueden ser centralmente administrados con el software de administración de la red.)

El concepto de filtrar los paquetes es muy parecido al concepto usado por los Ruteadores. Una etapa de filtrado se desarrolla en cada Switch, lo que provee un nivel de control administrativo muy alto debido a que puede examinar muchos atributos de cada paquete. Los administradores de la red pueden agrupar a los usuarios basándose en el número MAC, y/o los tipos de aplicación.

El Switch compara una tabla de direcciones utilizando el packet filtering, para así tomar una decisión en base a las entradas para enviar los paquetes. (ver figura).



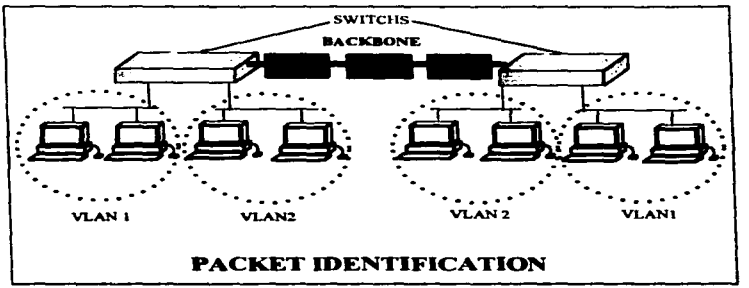
El "Packet filtering" es un concepto que típicamente provee un nivel adicional de procesamiento al Switch antes de enviar cada paquete a otro puerto o a otro Switch dentro de la red.

Este procesamiento adicional puede producir efectos en la latencia y desempeño de la red, además al mantener tablas de direcciones agrega también un nivel extra en la administración del Switch y también requiere de sincronía de las tablas entre los Switches.

El "Packet identification" es un concepto relativamente nuevo que ha sido específicamente desarrollado para la comunicación con Switches. Ésta técnica pone un identificador único en la cabecera del paquete para después ser enviado a los Switches.

El identificador es entendido y examinado por cada Switch antes de cualquier emisión o comunicación con otro Switch, Ruteador u otro dispositivo. Cuando el paquete sale del Switch, éste le quita el identificador antes de que el paquete sea transmitido a la tarjeta de la estación final.

Durante los dos años pasados el "Packet identification" ha ganado aceptación al igual que los Switches han ido aumentando su popularidad; las funciones de identificar el paquete en la capa 2 requiere un procesamiento superior en cuanto a lo administrativo de la red (como se puede ver en la figura).



Los beneficios totales de ambos conceptos (filtering e identification) permite a las arquitecturas de VLAN comunicarse íntegramente con la arquitecturas LAN existentes, mientras ofrecen la posibilidad de ser escalables y poder emigrar a las redes ATM.

3.4.4 CONFIGURANDO VLANS.

Los usuarios pueden ser asignados a las VLAN's usando diferentes tipos de configuración, que incluyen los puertos estáticos, los puertos dinámicos y los multipuertos VLAN. Estas opciones son funciones de las capacidades de los Switch, al igual que la manera en como son vinculadas las estaciones de trabajo en cada puerto del Switch y las capacidades de software de administración de las VLAN's.

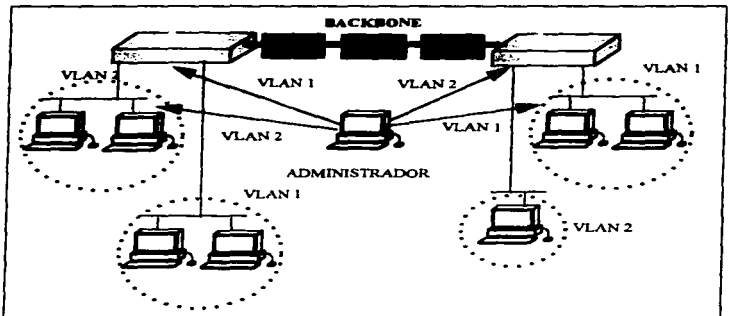
Las estaciones directamente vinculadas a los puertos de los Switches proveen la más grande flexibilidad para la configuración y administración de las VLAN's. Todas las estaciones de trabajo pueden ser individualmente asignadas a las VLAN's, cuando ellas se mueven a otro sitio donde usen directamente conexión con otro puerto de otro Switch, mantienen su identidad de VLAN, independientemente de sus nuevas ubicaciones. Las estaciones conectadas a un hub y a un Switch usualmente se

agrupan dentro de una misma VLAN, porque todos ellos comparten el mismo puerto del Switch.

Mientras este concepto es menos flexible para cada usuario en la red, para los administradores de la red provee soluciones muy deseables.

Las "Static VLAN's" (VLAN estáticas) son puertos de un Switch que el administrador a asignado como VLAN estática, usando una aplicación de control de la VLAN o configurándolo directamente dentro del Switch. Estos puertos mantienen su configuración asignada hasta que el administrador de la red tome otra decisión. Aunque las "Static VLAN" requieren cambios por el administrador, ellas son seguras, además que son fácil de configurar y de monitorear.

Este tipo de VLAN trabajarán en donde las redes se mueven, son controladas y administradas por un robusto software de administración para configurar puertos y donde los administradores de red no requieran de manejar adicionalmente algo superior a la dirección MAC.



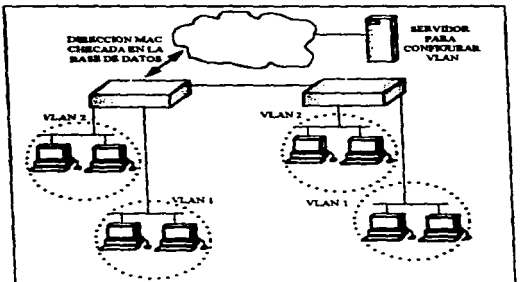
CONFIGURANDO PUERTOS ESTATICOS DE VLAN'S

Las "Dinamic VLAN" (VLAN dinámicas) son puertos en un Switch que automáticamente pueden determinar sus VLAN asignadas con la ayuda de la inteligencia del software de administración .

Las "Dinamic VLAN" funcionan basándose en la relación que existe en una VLAN y el número MAC del usuario final o con su tipo de protocolo, ésta asignación se mantiene en una aplicación VLAN de control centralizado.

Cuando las estaciones de trabajo inicialmente son conectadas a un puerto de un Switch que no tenga un VLAN asignada, el propio Switch checa las direcciones MAC con la base de datos de control de las VLAN y automáticamente configura el puerto con su correspondiente asignación VLAN.

Los mayores beneficios que se obtienen al configurar VLAN's dinámicas se reflejan en una menor administración, en una optimización del cableado cuando éstos cambian de lugar o cuando aumentan, además cuando un nuevo usuario se conecta a la red existe una notificación centralizada.



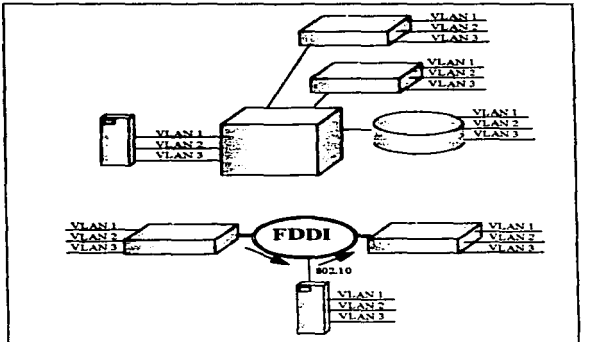
CONFIGURANDO PUERTOS DINAMICOS DE VLAN's

Multi VLAN's; éste tipo de configuración se refiere a los puertos que proveen comunicación entre múltiples VLAN's o un puerto único, esto incluye a los usuarios y a los servidores compartidos quienes necesitan pertenecer a múltiples grupos de trabajo.

Estos puertos actúan como Gateways dentro de otros grupos de VLAN's y por consecuencia crean una VLAN más grande, aunque éste concepto no es decisivo para que los grupos de VLAN's lleguen a ser más grandes.

Para resolver la necesidad de optimizar los recursos en varias conexiones VLAN, la mejor manera de hacerlo es conectar las estaciones finales directamente al Backbone y configurar directamente las trayectorias de comunicaciones de todas y cada una de las VLAN's, así se proveerá de recursos compartidos mientras se mantiene la integridad de las "Firewalls" de las LAN.

Este método ha sido definido en la redacción de estándares de ATM y de LANEmulation, y también esta siendo evaluado para la implementación a través de los Backbones de LAN compartidos y para las arquitecturas de Switches.



SERVIDORES COMO PARTE DE LAS VLAN's MULTIPLES

3.4.5 SEGMENTANDO CON ARQUITECTURAS DE SWITCH.

Cuando se reestructuran a los usuarios de acuerdo a su lógica asociación con la empresa o simplemente se cambia su locación física, se desarrolla un cambio fundamental en las topología desarrolladas hasta hoy.

La gran mayoría de las redes actualmente instaladas, proveen muchas limitaciones lógicas para la segmentación, los usuarios son comúnmente agrupados basándose en las conexiones dentro de un Hub y los puertos del Ruteador. Adicionalmente, los usuarios en dos diferentes segmentos con un Ruteador no pueden ser conectados al mismo segmento de LAN.

Las topologías hasta hoy usadas proveen segmentación solo entre Hubs, que son típicamente localizados en pisos diferentes de la empresa y no entre usuarios conectados en el mismo Hub, lo cual impone limitaciones físicas dentro de la red.

Lo que lleva a que este tipo de arquitecturas compartidas provean un grado pequeño de capacidades de agrupamiento, lo cual significa que los administradores de red son restringidos en la forma de agrupar lógicamente a los grupos de trabajo.

Los Switches quitan las limitaciones físicas impuestas por la arquitectura de Hub compartido, ya que los Switches sí agrupan lógicamente a usuarios y puertos dentro de la empresa.

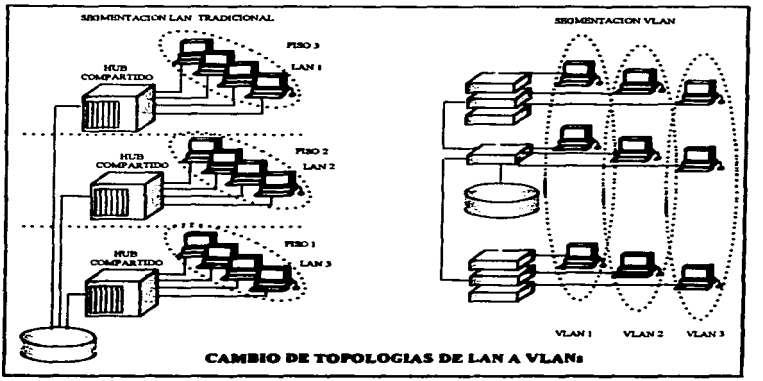
Como un reemplazo para los Hubs compartidos, los Switches quitan las barreras impuestas por el cableado. Adicionalmente, el papel del Ruteador evoluciona más allá del tradicional papel de "Firewalls[1]" y "Broadcast" y la ruta de procesamiento y dirección.

Ya que igualmente son importantes, los Ruteadores siguen vitales para la arquitectura de los Switches configurados como VLAN's, porque son ellos los que proveen la comunicación entre los grupos de trabajo lógicamente definidos (VLAN's), además de que los Ruteadores también proveen acceso a las VLAN's para compartir los recursos tal como servidores o Host y conectan a otras partes de la red que son segmentadas lógicamente con el tradicional concepto de subredes, o también provee del acceso remoto con las WAN.

El nivel 3 de comunicaciones se ensamblo al Switch externamente y es una parte integral en el alto rendimiento de las arquitecturas de switcheo.

Externamente los Ruteadores pueden ser integrados dentro de la arquitectura de Switches usando una o múltiples conexiones de Backbone de altas velocidades, las cuales típicamente son FDDI, CDDI, Fast Ethernet o conexiones ATM. Estas conexiones incrementan las interacciones entre Switches y Ruteador, al igual que proveen una asociación lógica uno a uno entre las configuraciones VLAN.

[1] Firewall.- Software de protección para la red.



CAMBIO DE TOPOLOGIAS DE LAN A VLANs

Esta arquitectura no solo provee segmentación lógica sino que mejora muchisimo la eficiencia de la red.

3.4.6 LAS VLANS A TRAVÉS DEL BACKBONE.

Algo importante de la arquitectura VLAN es la habilidad de transportar información entre Switches interconectados y Ruteadores que residen en el Backbone, esto es que las VLAN's transportan información a toda la empresa.

Estas capacidades de transporte quitan los límites físicos entre usuarios, incrementa la flexibilidad en la configuración de las VLAN's cuando los usuarios son reubicados.

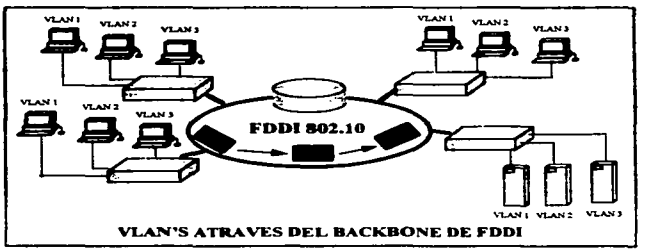
El Backbone actúa normalmente como el punto de agregación para grandes volúmenes de tráfico, al igual que actúa como el portador de la información de los usuarios finales de las VLAN's, además que lleva la identificación de los Switches, Ruteadores y servidores compartidos. Por eso es importante el ancho de banda que soporte el Backbone.

Los Backbones más populares de alto ancho de banda son los ya mencionados FDDI, CDDI, Fast Ethernet, ATM, debido a que los Switches y Ruteadores son adjuntos directamente al Backbone, ellos deben ser capaces de transportar información VLAN e interoperar con otros componentes de la red manejando ese gran ancho de banda.

Con respecto a los requerimientos, varios y diferentes mecanismos de transporte están siendo considerados para la comunicación de información VLAN a través del alto rendimiento de los Backbones; entre ellos se encuentra el estándar de LANEmulation que recientemente ha sido redactado y aprobado por el ATM forum y la IEEE 802.10 , el protocolo provee comunicación VLAN a través de los Backbones compartidos. Ambos definen un mecanismo de interoperabilidad para configurar y transportar VLAN's a través de diferentes tecnologías de Backbone.

La propuesta 802.10 ha sido recomendada para proveedores de Switches, Ruteadores y Hubs.

En la siguiente figura se muestran las aplicaciones típicas para 802.10. Esta propuesta define una dirección de 32 bits para la identificación de la VLAN.



VLAN'S ATRAVES DEL BACKBONE DE FDDI

Con la estandarización de estos protocolos de transporte, los administradores de red pueden implementar VLAN's dentro de grupos de trabajo individuales, a través del Backbone de la empresa y así obtener acceso a las WAN.

Adicionalmente, Cisco ha desarrollado el enlace InterSwitch (ISL) un protocolo de transporte VLAN para entregar eficientemente la comunicación a través del Backbone Ethernet. Cisco lo implementara como un protocolo propietario y ha hecho recomendaciones disponibles para los proveedores que quieran interoperar.

3.4.7 LA INTEGRACIÓN VLAN

Las arquitecturas de redes tradicionales están experimentando significativos cambios debido a que han evolucionado a una mayor microsegmentación, más ancho de banda en el Backbone y utilizan Switches para los circuitos dedicados con la adopción de ATM.

El núcleo de estos cambios se basan en los Switches, con aplicaciones de cableado, Backbone con Switches para un mayor rendimientos, ancho de banda y por la utilización de Switches ATM para conmutar circuitos dedicados.

Para los administradores de red, la migración a productos VLAN's ha llegado a ser una realidad. Típicamente la integración de las VLAN's comenzó con la primera instalación de un Switch en un departamento, como el número de Switches creció a toda a empresa, las VLAN's se convirtieron en las solución para los problemas de comunicaciones en las empresas de gran amplitud.

Las VLAN han llegado a ser una implementación natural para las arquitecturas LAN, debido a que los diseñadores y administradores de red otorgan ancho de banda dedicado al "Desktop" (aplicaciones) y realizan la segmentación basada en grupos lógicos de trabajo a través de la empresa.

Las arquitecturas de Switch junto con las soluciones de ruteo que son capaces de interconectar VLAN's están evolucionando con cambios en el diseño, comparados con la segmentación física que la mayoría de las redes tienen hoy en día.

Las VLAN's son una de las tecnologías esenciales para romper cualquier paradigma de restricción existente hoy en día.

3.4.8 LOS BENEFICIOS DE LAS VLANS

Las VLAN son frecuentemente colocadas como respuestas a los problemas asociados con movimientos, cambios y al agregar un nuevo usuario, ya que ellas solo reducen una gran parte de los costos de administración cuando los usuarios cambian sus locaciones físicas dentro de un edificio debido a que la tecnología VLAN provee muchos beneficios de "Internetworking".
Adicionalmente a la reducción de los costos de administración, los beneficios de las VLAN incluyen un ajuste en la seguridad de la red con el establecimiento de grupos de usuarios seguros, mejor administración y control del "Broadcast", cargando la distribución del tráfico al Switch de tráfico intensivo ("Hot Spot" dentro de la red).

3.4.9 MEJORAS EN LA EFICIENCIA DE LA ADMINISTRACIÓN

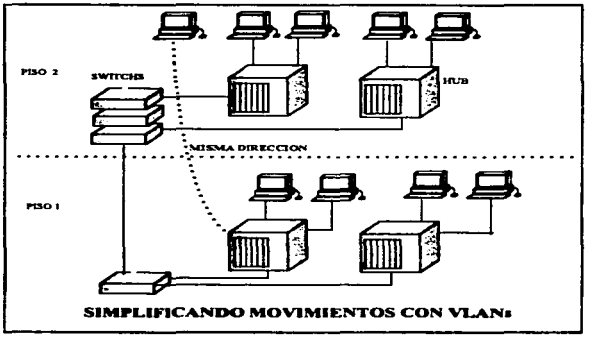
Las compañías continuamente se reorganizan para buscar mejoras en su productividad, en promedio de 20 a 40 % de la fuerza de trabajo es físicamente movida todos los años, estos movimientos, adiciones y cambios son uno de los más grandes dolores de cabeza para los administradores de red, además de causar grandes gastos en la administración de la misma.

Muchos movimientos requieren de un nuevo cableado y además todos los movimientos requieren de una nueva dirección y reconfiguración de los Hubs y Ruteadores e invariablemente el tiempo para estabilizar la red es mayor.

Las VLAN's proveen un efectivo mecanismo para controlar estos cambios y reducen en mucho los costos asociados con la reconfiguración de los Hubs y Ruteadores, los usuarios de una VLAN pueden compartir la misma red (espacio de dirección) independientemente de su ubicación física.

Cuando los usuarios de una VLAN son movidos desde un lugar a otro, y mientras sigan perteneciendo a la misma VLAN, solo serán conectados a un puerto del Switch, su dirección de red no cambia.

Los cambios de ubicación pueden ser tan simples como conectar a un usuario a un puerto VLAN de un Switch o simplemente configurando el puerto del Switch como VLAN.



SIMPLIFICANDO MOVIMIENTOS CON VLANs

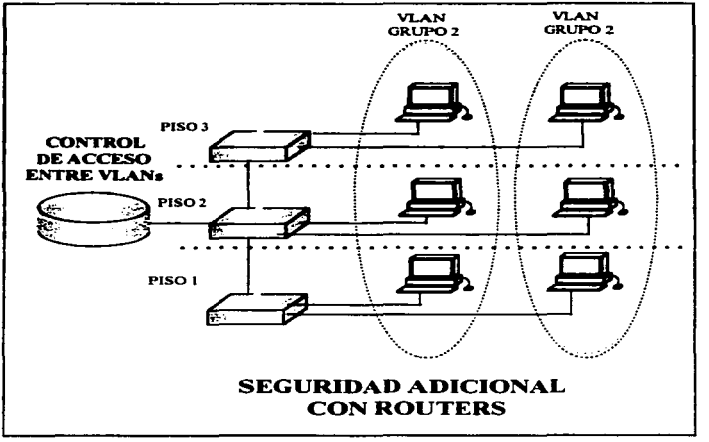
Esto simplifica mucho el recableado, configuración y el tiempo necesario para tener de regreso en la línea al usuario. Esto es un significativo mejoramiento sobre las técnicas de cableado usadas en la actualidad. Además las configuraciones de los Ruteadores permanecen intactas; un simple movimiento de un usuario de una ubicación a otra , no crea alguna modificación en la configuración de los Ruteadores ya que los usuarios residen dentro de la misma VLAN.

3..4.10 MEJORAS EN LA SEGURIDAD DE LA RED.

Durante los últimos cinco años, el uso de las LAN se ha incrementado exponencialmente, como un resultado de este incremento, las LAN frecuentemente tienen colisiones de los datos que se mueven a través de ellas, además la seguridad de los datos confidenciales solo se aseguran mediante la restricción de acceso.

Otra de las deficiencias de compartir las VLAN es que son relativamente fácil de penetrar, solo es necesario conectarse a un puerto activado y así un usuario intruso puede tener acceso de emisión a toda el segmento, a menos que haya funciones de control en el Hub.
Una de las más fáciles y efectivas técnicas de administrar con seguridad es hacer segmentos de red dentro de distintos grupos de broadcast, adicionalmente las VLAN permiten al administrador de Red restringir el número de usuarios en un grupo VLAN y no permite a otro usuario unirse sin primero recibir aprobación de la aplicación del administrador de red.

Las VLAN así proveen los "firewalls" de seguridad, restringiendo el acceso a cada usuario individualmente, controlando las banderas indeseables que se introduzcan a la red y también controla el tamaño y la composición del grupo.
Implementando este tipo de aplicación es relativamente confiable, los puertos del Switch son agrupados, basándose en el tipo de aplicación y privilegios de acceso. Para restringir las aplicaciones y los recursos comúnmente se colocan en un grupo de seguridad VLAN. Algunos usuarios intentaran explorar en estas VLAN pero la seguridad activara banderas por el software de administración de la red. Los aumentos adicionales en la seguridad de la red se pueden lograr utilizando las listas de accesos de los Ruteadores.
Las restricciones pueden ser colocadas basándose en la dirección MAC, tipos de aplicación, tipo de protocolo o mediante el horario del día.



3.4.11 APOYÁNDOSE EN LA HERENCIA DE LA INVERSIÓN HUB.

Durante los últimos cinco años los administradores de red han instalado un número significativo de chasis de Hub compartidos. módulos y dispositivos escalables, mientras muchos de esos dispositivos están siendo remplazados con nuevas tecnologías de Switcheo debido a que las nuevas tecnologías requieren de un mayor ancho de banda dedicado, y un mayor rendimiento directamente al usuario, pero los Hubs compartidos todavía pueden desempeñar funciones útiles en muchas instalaciones existentes, los administradores de red están apoyándose en sus investigaciones para conectar Switch con el "Backplane" de los Hubs.

En el contexto de esta discusión, una conexión de Hub a un "Backplane" define un medio compartido del Hub conectado dentro del Backbone de la red; los Hubs escalables, los chasis de Hub al igual que los módulos de Hub proveen alguna forma de esta conexión. Esto se refiere a la conexión de los Hubs compartidos y los Switches que proveen oportunidades para la segmentación de redes VLAN.

Cada segmento del Hub conectado a un puerto del Switch, puede ser asignado a una VLAN. Las estaciones que comparten un segmento de Hub son todas asignadas al mismo grupo VLAN. Si una estación individual necesita ser conectada a otra VLAN, la estación será reubicada a un apropiado y correspondiente modulo de Hub. La interconexión que realiza el Switch maneja las comunicaciones entre los puertos del Switch y automáticamente determinará el segmento receptor apropiado. Además el hub puede ser compartido y dividido en grupos pequeños, para proveer mayor microsegmentación y mas flexibilidad para usuarios individuales de cada segmento VLAN.

3.4.12 EL CONTROL CENTRALIZADO DE LAS VLANS

El control del "Broadcast" de la red, planear movimientos, establecer accesos y privilegios en la red, y la seguridad de los recursos son funciones comunes en la planeación central y administración del grupo.

Las comunicaciones VLAN's facilitan este tipo de planeación por proveer efectivas aplicaciones de administración que pueden ser configuradas, administradas y monitoreadas centralizadamente.

Desde una aplicación de administración centralizada VLAN, los administradores de red pueden determinar grupos VLAN, asignar usuarios específicos a los puertos del Switch, colocando niveles de seguridad, límite en el tamaño del dominio, cargar el tráfico y distribuirlo a través de los enlaces redundantes, configurar las comunicaciones VLAN a través del Switch y además monitorear que el tráfico fluya

adecuadamente, también optimizar la utilización del ancho de banda de las VLAN's cuando existan colisiones dentro de la red.

Estas capacidades substancialmente incrementan el control, la flexibilidad y las funciones de monitoreo de las aplicaciones de la administración de red. reduciendo el costo de la administración e incrementando todos los servicios de las operaciones de administración centralizada.

Las aplicaciones de control de las VLAN jugaran un gran papel en la configuración y administración de las redes ya que los usuarios evolucionan a una arquitectura LAN Switcheada.

Las VLAN ofrecen un significativo beneficio en el costo y rendimiento para la mayoría de las LAN instaladas actualmente, estos beneficios son aprovechados por los administradores de red que emigran a las arquitecturas LAN con Switches.

Mientras las VLAN's son una parte integral de las arquitecturas ATM, el concepto y muchas de las tecnologías han sido diseñadas dentro de los Switches que ofrecen beneficios similares a través de los Backbones de LAN. Adicionalmente las aplicaciones de los usuarios no necesitan cambios al realizar los beneficios VLAN's como parte de la arquitectura de Switch, ya que son transparentes para los usuarios finales.

Finalmente las VLAN's son más que un Hub compartido, un Ruteador, un Switch o la solución a los problemas de administración de la red. Sino que la combinación de todos estos componentes proveen mayor potencia en la segmentación y en la eficiente administración a lo largo de toda la red.

3.5 SWITCHES ETHERNET.

La tecnología de los Switches esta incrementando la eficiencia y velocidad de las redes. Esta tecnología, esta haciendo los sistemas corrientes mas poderosos, mientras que al mismo tiempo facilitan la migración a redes de altas velocidades. Es importante comprender que esta tecnología solo se puede implementar y diseñar desde lo que ya estaba conectado.

Muchas redes están experimentado escasez en el ancho de banda, una de las razones es el incremento del trafico por el aumento de los usuarios de la red, la suma de los datos transportados entre aplicaciones cliente/servidor y la ineficiencia en el control del trafico en algunas redes son otras de las razones de la falta de ancho de banda.

Switcheando directamente el tráfico de la red es una manera muy eficiente ya que se envia directamente la información desde el puerto de origen y solamente al puerto destino.

El incremento del rendimiento de las redes switcheadas, mejora la flexibilidad en los movimientos adiciones y cambios de ubicación de los usuarios.

Al switchear se establece una línea directa de comunicación entre dos puertos y mantiene simultáneamente enlaces múltiples entre varios puertos.

Esta tecnología permite algunos beneficios sobre los tradicionales puentes Ethernet o redes ruteadas.

Primero.- Un ancho de banda de 10 MBPS o 100 MBPS de medios compartidos puede ser cambiado a un ancho de banda de 10 o 100 MBPS dedicados. Los Bridges y Ruteadores típicamente tienen muchos dispositivos adjuntos a sus puertos compartiendo al ancho de banda disponible, los Switches permiten que conectes cada segmento compartido o uno dedicado a cada puerto del Switch.

Segundo.- Esto es realizado sin modificación alguna en el software o en el hardware, el costo por puerto de un Switch esta por debajo de los $1000 dólares, para un puerto de un Bridge es sobre los $1000 dólares y para un puerto de Ruteador es sobre los $3000 dólares, finalmente la instalación de un Switch es menos compleja que la configuración de un Bridge o Ruteador, esto es lo que hace al Switch una atractiva solución.
Históricamente, las LAN crecieron y proliferaron en un ambiente compartido, caracterizado por emplear varios métodos de acceso al medio, como por ejemplo

el MAC (Media Access Protocol), protocolos para Ethernet, Token Ring y FDDI cada uno tiene reglas arbitrarias que determinan como deben ser enviados los datos sobre algún tipo de medio físico.

El tradicional Ethernet corre a 10 MBPS sobre un tipo común de BUS, las estaciones físicamente adjuntas al BUS mediante un HUB repetidor o concentrador, creando un dominio de Broadcast.

Cada estación es capaz de recibir todas las transmisiones desde todas las estaciones, pero solo en modo Half-Duplex, lo que signfica que la estación no puede enviar y recibir información al mismo tiempo. Además, los nodos en una red Ethernet transmiten información siguiendo una simple regla. Ellos escuchan antes de hablar.

En el ambiente Ethernet, solo un nodo en el segmento le esta permitido transmitir en cualquier tiempo debido al protocolo CSMA/CD (Carrier Sense Multiple Access/Collition Detect), permitiendo así un control en la colisión de paquetes e incrementar el tiempo de transmisión en dos maneras:

Primero.- Si dos nodos comienzan a hablar al mismo tiempo la información choca, y ambos nodos detienen la transmisión y la intentan otra vez mas tarde.

Segundo.- Una vez que el paquete ha sido enviado a un nodo, una LAN Ethernet no transmitiría ninguna otra información hasta que este paquete llegue a su punto final, esto es lo que demora a este tipo de redes. Incontables horas han sido perdidas esperando que un LAN Ethernet este libre para enviar.

El Bridge, el Ruteador, y el Switch, intentan reducir el tiempo de transmisión e incrementar el rendimiento de la red. Por ejemplo, un puerto de un Bridge parte una red lógica en dos segmentos físicos y solo permite una transmisión a través del segmento, si el nodo destino esta "alive" (dado de alta) del otro lado.

Estos paquetes son enviados únicamente cuando es necesario, reduciendo la congestión de la red, aislando el tráfico a uno de los segmentos, lo que permite que el tráfico local permanezca local.

En contraste los Ruteadores enlazan múltiples redes lógicas juntas, estas redes son físicamente distintas y deben ser vistas como colisiones separadas. El rendimiento del Ruteador no solo es en la segmentación física (cada puerto tiene un numero único de red) pero también provee la segmentación lógica referida a la función de un "firewall"

Los Bridges y Ruteadores tienen arquitecturas similares basadas en el BUS que por diseño y función en el medio compartido, con el empleo de simples o múltiples procesadores los datos son recibidos dentro de un buffer, donde son examinados antes de ser enviados.

La contienda de múltiples segmentos es necesaria para el acceso al BUS; considerando que el Switch elimina la arquitectura de BUS y además los Bridges y Ruteadores tienen latencias significativamente mas altas que los Switches (de 1 a 2 mseg en almacenar y enviar 1518 bytes de la trama Ethernet, comparadas con 0.020 mseg para un Switch) los Switches son una buena solución.

Finalmente el diseño basado en tecnología de BUS no es escalable, debido a que la propagación se demora inevitablemente en cuanto incrementa la longitud del BUS.

Un puerto del Switch puede ser configurado como un segmento con muchas estaciones adjuntas o con una simple estación conectada a él. Las reglas de contención son basadas en CSMA/CD, y la regla es que solo una conversación puede originarse desde cualquier puerto en cualquier tiempo, independientemente si hay una o muchas estaciones conectadas con este puerto. Esto es, todos los puertos escuchan todavía antes de hablar.

3.5.1 ARQUITECTURAS ETHERNET CON BRIDGES Y SWITCHES.

Cuando una estación LAN es conectada a un puerto de Switch puede operar en un modo de Full duplex, por lo que no requiere Detection Colition, esto provoca una suspención de los protocolos MAC.

Un simple dispositivo reside en este puerto y por lo tanto las colisiones no existirán.

Un calculo en el aumento del ancho de banda de una Ethernet con Switch puede ser calculado multiplicando el numero de puertos switcheados "n" por el "media bit rate" y dividiendo este número por 2 cuando la comunicación involucra dos partes (Cuando la comunicación involucra al que envía y al que recibe).

Para una operación Full Duplex, es la misma ecuación excepto por la división entre 2 por ser innecesaria debido a que un puerto individual envía o recibe información. El modo de Switcheo Full Duplex permite que el trafico sea enviado y recibido simultáneamente. Agregando un salto de los 10 MBPS de Ethernet a 20 MBPS y desde los 100 MBPS a 200 MBPS de las Fast Ethernet.

Los grupos de trabajo entre Hubs y Switches no correrán Full Duplex debido a que los Hubs son gobernados por los requerimientos de Colition Detection. por lo tanto los grupos de trabajo conectados a un HUB no se pueden Switchear.

3.5.2 LOS SWITCHES SOPORTANDO COMUNICACION FULL DUPLEX Y VELOCIDADES DE TRANSMISION DE 10/100 MBPS.

Hoy en día la línea definida entre Bridges y Switches esta desapareciendo, ahora los Switches mejoran la segmentación que realizaban los Bridges y los Ruteadores.

Los Switches pueden hacer mas que dirigir un paquete de un lado a otro, ellos envían el tráfico directamente a su destino.

Un Switch cambia un segmento compartido de 10 MBPS a un segmento dedicado de 10 MBPS. Los Switches Ethernet transfieren paquetes desde un segmento compartido de 10 MBPS a un segmento LAN o a una workstation corriendo a 100 MBPS, esto permite que múltiples estaciones o grupos de trabajo corriendo a 10 MBPS se conecten a un servidor o servidores corriendo a 100 MBPS.

Ethernet esta basado en un medio compartido lo que significa que todos los dispositivos comparten el mismo cable para transmitir datos.

3.5.3 VENTAJAS DE LOS SWITCHES ETHERNET.

Es una tecnología establecida y bien comprendida.
Muchos vendedores están disminuyendo el costo por puerto.
El costo de los movimientos, adiciones y cambios se reducen con las VLAN's.

3.5.4 DESVENTAJAS .

La utilización de la red se limita alrededor de 33% en ambientes compartidos.
No muy bueno en el manejo del tiempo para tráfico sensible a él.

El futuro para los Switches Ethernet es brillante, ya que proveen alrededor del 70 % de la renta del mercado de los Switches, de acuerdo al IDC el porcentaje de crecimiento para el número de los puertos podrá ser de 171 % para éste año (1997) ya que en el año de 1995 el número de puertos instalados fue de 2,000 000 y para 1996 fue de 5,300 000 puertos instalados.

3.6 SWITCHES FAST ETHERNET O 100 BASE T.

Los Switches Fast Ethernet mejoran las LAN Ethernet existentes, debido a que proveen 2.6 GBPS con el Switch interno a los 10/100 MBPS del ancho de banda dedicado de las redes de la actualidad, además de ser escalable.

Entregando un dedicado y escalable ancho de banda, en lugares donde es necesario, y así mejorar el rendimiento, relevando los embotellamientos que son una plaga en las redes de medios compartidos.

3.6.1 REDUCIENDO LOS COSTOS DE LA SEGMENTACION.

Instalados en el centro de la red, los Switches proveen segmentos de red distribuidos por enlaces de 10 y 100 MBPS dedicados, proporcionando una solución efectiva en el costo de la segmentación de la red y mejorando el rendimiento.

Como un resultado de los altos costos de los puertos de los Ruteadores, estos pueden ser reservados para el establecimiento de dominios de la red, basándose en niveles de red, subredes o locaciones geográficas. La solución también permite a los usuarios de la red que están conectados al Switch ser movidos a cualquier parte de la red sin cambiar su dirección, reduciendo los costos asociados a la administración, y haciendo modificaciones similares en el ambiente de Ruteador.

3.6.2 ELIMINANDO LA CONGESTION DE LA RED.

Por el ofrecimiento de la soluciones a 100 MBPS de la alta utilización de los dispositivos, tales como servidores, los Switches relevan los embotellamientos de datos encontrados en las redes de medios compartidos a 10 MBPS por enlaces dedicados con Switches a 100 MBPS.

3.6.3 DESCRIPCIÓN DE LAS CARACTERISTICAS DEL SWITCH FAST ETHERNET.

Los Switches Fast Ethernet entregan Switcheo interno, conectividad y soporte a las demandas de red en ambientes a altas velocidades.

Los Switches son dispositivos escalables, proveen ancho de banda dedicado, adjunto a los segmentos de medios compartidos para los usuarios finales, y así relevando el congestionamiento común en el ancho de banda de los ambientes Ethernet tradicionales.

Como en Ethernet o Token Ring, el Switcheo 100 base T o Fast Ethernet, esta basado en un medio compartido. La mayor ventaja de 100 base T es que las funciones son idénticas a las de 10 base T (Ethernet) pero opera a 10 veces la velocidad nominal, por lo que se incrementa el costo. Algunos de estos Switches soportan Full Duplex, Fast Ethernet que agrega una velocidad bidireccional de 200 MBPS.

3.6.4 VENTAJAS DE LOS SWITCHES FAST ETHERNET.

Ofrece un buen entendimiento con la tecnología heredada.
Existe un amplio rango en la tecnología de soporte.
Mas ancho de banda disponible que el que ofrece 10 base T.

3.6.5 DESVENTAJAS.

Menor madurez y mayor costo que los Switches 10 base T.
El tamaño de las redes completamente se restringe.
Incompatibilidad de las implementaciones VLAN entre vendedores.

3.7 SWITCHES TOKEN RING.

Los Switches Token Ring han tenido un significativo impacto en el mercado. Las redes están cambiando y con estos cambios se generan intereses que necesitan ser bien direccionados.

Una mirada al futuro revela que las redes necesitarán aplicaciones de soporte como multimedia que requieren mucho mas grande el ancho de banda que el que las redes compartidas pueden ofrecer. El diseño permanecerá como un factor definitivo en el rendimiento que provean las redes, los Switches cambiarán la forma en que estas redes serán diseñadas y los cambios que proponen, también maximizarán la productividad de la red.

Ethernet y FDDI han sido rejuvenecidas mediante un rendimiento impulsado desde la tecnología de Switcheo y con las redes Token Ring no ha sido diferente.

Las ventajas que proveen los Switches también se aplican a esta tecnología, al usar Switches se incrementa la velocidad y la eficiencia de las redes proporcionando líneas dedicadas entre los usuarios y los recursos que ellos requieren. Por establecer estas líneas directas y siendo capaz de cambiarlas instantáneamente, los Switches administran el tráfico, incrementan la flexibilidad de una red, mejora el rendimiento y reduce los movimientos incrementos y cambios de ubicación de los usuarios. Agregando ancho de banda e incrementando la productividad, todo ello como

resultado de las múltiples conexiones simultáneas que se pueden lograr con un Switch. Con todas estas flexibilidades los Switches permiten la escalabilidad redes dedicadas y toda una promesa para la migración a ATM.

Para Token Ring específicamente, el Switcheo ofrece un mas simple y mas eficiente significado de los múltiples anillos conectados hasta ahora ruteados o el modo de los enlaces Token Ring con Bridges.

Ahí nada es agraviado con el empleo de Ruteadores y Bridges, sin embargo ellos no son ni aproximadamente lo eficientes que son lo Switches.

Usando el estándar IEEE 802.5 los Switches proveen un Token Ring Dedicado (DTR) que puede duplicar el ancho de banda de un usuario individual o servidor, por suspender el protocolo Token Passing.

Este protocolo (Token Passing) controla el acceso al medio, al Switchear se pueden transferir paquetes desde un anillo a otro con una demora despreciable. Mediante el incremento del ancho de banda agregado se reduce la demora en la transferencia y habilidad de dirigir números igualmente que conversaciones, la productividad de las redes Token Ring puede subir increíblemente.

3.7.1 PROBLEMAS QUE LOS SWITCHES TOKEN RING RESUELVEN.

Las nuevas aplicaciones y los mas altos anchos de banda, como son las crecientes aplicaciones de video y la escalabilidad llegan a ser muy importantes. La tecnología del Switcheo permite una eficiencia máxima en el ancho de banda mediante líneas que son dedicadas mas que compartidas.

La utilización de toda la red.- La segmentación puede ser usada para mejorar el rendimiento al utilizar gran parte de la red. Como un resultado de la naturaleza de las redes Token Ring , pueden mantener alrededor del 80% utilizada antes de la degradación del rendimiento, opuesto al 30 % de las redes Ethernet.

La limitación en el uso de los Bridges.- Las redes Token Ring con puentes pueden tener limitaciones (tales como las limitaciones del conteo de brinco, la carencia de densidad de los puertos y la carencia del rendimiento) típico de las redes con Bridges, ya que muchos de esos Bridges tienen solo dos puertos y naturalmente están embotellados.

3.7.2 TIPOS DE SWITCHES TOKEN RING.

Los tipos de Switch TR basan sus diferencias en dos diseños básicos de arquitectura que determinan el proceso de enviar las tramas, estos son: Cut Through y Store and Fordward.

3.7.3 TECNICAS DE TOKEN RING SWITCHEADO.

Los Switches Token Ring soportan una o mas de las siguientes técnicas. El ruteo transparente y el método de conectar mas de dos anillos Token Ring con Bridges. Utilizando los Ruteadores, los nodos originadores envian las tramas y el método de ruteo encuentra el mejor camino para llegar a su destino, ya sea un usuario final en otro anillo o un servidor.

Los puentes insertan la información a lo largo del camino (El numero de anillo y el numero designado por el Bridge) En esta exploración del paquete se define la trayectoria tomada.

El Route Information Field (RIF) es donde esta información es almacenada, durante el tiempo en que las tramas alcanzan su destino.

Cuando estas tramas regresan al originador, quizas por medio de trayectorias múltiples, el primero en regrezar es la ruta que será tomada por las siguientes tramas de la fuente al destino.

Estas técnicas también son usadas por las tecnologías de Switch usando las mismas reglas generales de operación. Bridges y Switches que soportan Source Routing, operando en la capa de enlace del modelo OSI y usando la trayectoria de información del RIF, para enviar las decisiones.

Source Routing no es requerida en una red de anillo individual debido a que todas las tramas se deben enlazar alrededor del anillo, permitiendo el acceso a las tramas transmitidas a todas las estaciones.

3.7.4 TOKEN RING DEDICADO (DTR).

Las redes de Cliente/Servidor tienen un diseño común, muchas workstations accesan a la información desde muy pocos servidores de archivos. En este ambiente el punto de entrada a un servidor de archivos es potencialmente un cuello de botella. El tráfico y la demanda aumentan. La segmentación de los servidores en una Token Ring y la distribución de las aplicaciones Cliente/Servidor entre ellas ayudaría a

resolver los problemas de embotellamiento. Los Switches proveen el tipo de segmentación para aislar los srvidores.

El Token Ring Dedicado.- Es un estándar Full Duplex que reemplaza a la especificación original IEEE 802.5. El hardware de la Token Ring es inherentemente capaz de la operación Full Duplex. Full Duplex puede ser implementado, mejorando el software y suspendiendo el Token Passing. Esto permite la comunicación entre un dispositivo y el puerto del Switch en cualquier momento.

Los servidores mas cargados pueden usar tarjetas Full Duplex, creando un anillo privado para algunos. Ellos serán los únicos dispositivos que necesitarán un puerto del Switch.

3.7.5 IMPLEMENTACIONES DE TOKEN RING.

El Switch Token Ring puede conectar múltiples anillos, permitiendo un muy alto rendimiento. un Switch puede actuar como un Backbone colapsado conectando anillos de grupos de trabajo y anillos soportados centralmente por servidores.

Las tres areas significativas para los Switches Token Ring son: El Backbone, Los Segmentos y los Grupos de trabajo.

3.7.5.1 EL BACKBONE.

En el ambiente Ethernet los Switches invariablemente son usados por Grupos de trabajo. La situación en Token Ring es diferente. La consolidación de los anillos es mas critica en el Backbone, donde los Switches pueden relevar la congestión e incrementar el control sobre la administración de la red. Un Backbone tipico consiste en muchos anillos conectados en un solo anillo por medio de dos puertos del Bridge. Otra configuración involucra a muchos anillos colapsando atrás a un Ruteador cuyo "Backplane" sirve como el Backbone del anillo. En ambos escenarios los servidores de archivos son distribuidos entre los anillos individuales o adjuntos directamente al Backbone del anillo.

Además, en ambos casos, los embotellamientos y la latencia indeseable, pueden existir debido a que la entrada de los recursos es mas pequeña que la basta demanda de esos recursos.

Al remplazar un Bridge y/o Ruteador por un Switch el rendimiento y la administración de la red son mejoradas manteniendo el número de anillos establecidos en el área del Backbone.

3.7.5.2 LOS SEGMENTOS.

Como el número de grupos de usuarios en una Token Ring incrementa, el rendimiento total en el anillo disminuye.

Los beneficios de Switchear Token Ring en ambientes donde existen numerosas unidades de acceso al medio o multiestaciones (MAUs) conectadas a múltiples usuarios en el mismo anillo de 4 o 16 MBPS compartidos, es que por el uso del Switch se puede microsegmentar éste gran anillo en unos segmentos mas pequeños, agregar un mayor "throughput" a la red y se puede lograr una mayor productividad en el segmento.

Con menos usuarios por segmento y cada segmento conectado directamente a un puerto del Switch, se logra una mas alta frecuencia de transmisión para cada estación.

3.7.5.3 LOS GRUPOS DE TRABAJO.

A los grupos de trabajo switcheados en el ambiente Token Ring se les proveen ancho de banda dedicado que es mucho mejor que la red Token Ring compartida.

Los dispositivos Token Ring de acceso al medio compartido y el ancho de banda disponible discuten por ganar el control de un Token.

Este Token Passing es suspendido cuando los adaptadores Full Duplex son adjuntos a un puerto del Switch. Los puertos del Switch proveen ancho de banda dedicado a los dispositivos de 4, 16 y 32 MBPS.

Como Ethernet, Token Ring está basado en un medio compartido, algunos Switches Token Ring soportan Half Duplex a 16 MBPS y Full Duplex operando a 32 MBPS.

3.7.6 VENTAJAS DE LOS SWITCHES TOKEN RING.

Tiene un buen entendimiento con las tecnologías heredadas.
La utilización de la red es cerca del 80 % en ambientes compartidos.
Soporta cargas pesadas de muchos usuarios.
Vence los límites de los Bridges y Ruteadores con el soporte VLAN.

3.7.7 DESVENTAJAS

Los estándares de soporte para Token Ring difieren entre los vendedores. Es menos maduro y es mayor el costo que la tecnología Ethernet.

En 1995 el numero de puertos de Switches Token Ring fue de 39,000, la predicción para 1996 fue que crecieran en un 1000 % y creció a más de 500,000 puertos.

3.8 SWITCHES ATM.

Un elemento clave en la era del ancho de banda compartido ha llevado a la era del Switcheo. Los usuarios esperan que los proveedores reúnan ampliamente los estándares aceptados. El estándar mas importante recientemente aceptado es el de ATM.

ATM ha llegado a ser ampliamente aceptado como el estándar de mecanismos de Switcheo para redes futuras. Está siendo desplegado rápidamente en la interconexión de redes LAN y WAN. Así como en las redes públicas y privadas. ATM usa pequeñas tramas de longitud fija que guarda una Latencia mas baja que los paquetes de longitud variable. Ya que estos pueden hacer una explosión de información tal como los paquetes de LAN y las constantes ráfagas de información como voz. Debido a que los Switches ATM son implementados en el hardware y los Switches pueden ser interconectados, estos también serán escalables para soportar aplicaciones que están a la orden del día en las mas grandes redes.

La cuestión no es si ocurrirá una transmisión ATM, sino qué tan rápidamente ocurrirá. Eventualmente las redes serán construidas con conexiones a altas velocidades de ATM a cada terminal, pero esto es inverosímil para ser difundido en un futuro próximo.

Las tarjetas de interface ATM son todavía mucho mas caras que las NIC's[1] Ethernet por lo que las arquitecturas con Switches ATM todavía están evolucionando; conectando todas las computadoras en un campus directamente vía ATM crearán una ráfaga agregada demasiada alta para los Switches actualmente usados.

Muchos usuarios quienes quieren correr ATM para manejar realmente grandes ráfagas de datos, necesitarán recablear con fibra óptica o con UTP nivel 5. En los próximos años mas organizaciones desplegaran ATM en una importante pero

[1] NIC Network Interface Card (Tarjeta de interfaz de red)

delimitada forma de Backbone y para grupos de trabajo con especial necesidad de ancho de banda.

ATM LANEmulation es una parte importante de las herramientas en las VLAN's. Podrán ser rápidas y soportar completamente los estándares al ser acopladas con otros mecanismos de VLANs, haciendo fácil la transmisión desde un Backbone FDDI o Fast Ethernet a un Backbone ATM.

3.8.1 EL SOPORTE ATM

Para muchos usuarios ATM será más que una tecnología de Backbone. En particular, aplicaciones que necesitan soporte mas fuerte para la calidad de servicio, tal como video en el desktop, serán mejor distribuidos con ATM que con otras tecnologías, además los precios de ATM están disminuyendo rápidamente.

La lista de los precios de una tarjeta de interface de red y un puerto en un pequeño Switch es por ahora mayor a $500 pero tiende a disminuir. Esto hace que la tecnología pueda competir con los Switches Fast Ethernet.

ATM esta orientado a conexión y provee cierta garantía y prioridades en los tipos de tráfico. La demora del tiempo en aplicaciones sensibles a él, como el video y el audio, es minimizada debido a que la trama ATM tiene un longitud de 48 bytes y 5 son del Header.

3.8.2 VENTAJAS DE LOS SWITCHES ATM.

Son la segunda y tercera generación de los Switches disponibles.
Ofrece un excelente manejo de todos los tipos de trafico (voz, video, datos e imágenes).
Al ofrecer LANE se asegura la protección de las inversiones heredadas de software y hardware.
La industria del soporte a disminuido sus costos.
Promete escalabilidad.

3.8.3 DESVENTAJAS.

Los Switches todavía no incorporan especificaciones comunes.
Falta de interoperabilidad en niveles fijos.
Comercialmente, los productos disponibles han disminuido y limitado el soporte a altas velocidades.

3.9 SWITCHES FDDI.

Siguiendo el nivel físico, nivel MAC, y las especificaciones de administración de las estaciones definidas por ANSI, FDDI es un anillo doble que usa Token Passing a altas velocidades y utiliza como medio la fibra óptica.

FDDI consiste en dos anillos un primario y un secundario en donde el trafico fluye en direcciones opuestas. Cuando el anillo primario se cae, el relevo en las estaciones finales cercanas envuelven la porción que falló y redirecciona el tráfico al anillo secundario.

Otra ventaja de FDDI está en la velocidad, que opera a 100 MBPS usando 4B5B (Código de línea, opuesto al manchester diferencial usado en Token Ring).

FDDI es usado como una "TUBERIA" que interconecta varias redes. Esto es ampliamente usado para correr LANs con aplicaciones de gran ancho de banda, como video o corriendo CAD/CAM en minicomputadoras o para LANs con muchas Workstations.

FDDI puede ser configurado en topología de anillo y desde un protocolo Token Passing, permite el acceso al medio.

Los Switches FDDI permiten que los anillos FDDI se comuniquen simultáneamente a través de ellos, muy similar a los Switches Token Ring.

Sin embargo el protocolo de acceso al medio para FDDI es menos eficiente que para Token Ring.

Un FDDI Full Duplex provee 100 MBPS para la transmisión y 100 MBPS para la recepción al mismo tiempo, pero el estándar no a sido aprobado aún. Esto suspenderá el protocolo Token Passing.

Mientras muchos Switches FDDI son capaces de utilizar la tecnología de Switcheo Cut-Through, la mayoría a implementado el proceso Store-and-Forward.

FDDI fue diseñado para ser tolerante a fallas, proporcionando mucho mas grandes redes con mucha mayor confiabilidad.

3.9.1 VENTAJAS DE LOS SWITCHES FDDI.

Provee madurez y un buen entendimiento con la tecnología heredada.
Alta utilización de la red, cerca del 98 % en ambientes compartidos.
Altas inversiones para la protección de instalaciones FDDI.

3.9.2 DESVENTAJAS.

Pocos productos compitiendo, por lo tanto se incrementa el costo.
No estandarizado para la operación Full duplex.

En 1995, los puertos del Switch FDDI fueron poco menos de 60,000, pero para el final de 1996 el número se proyecto a cerca de 171,000 puertos.

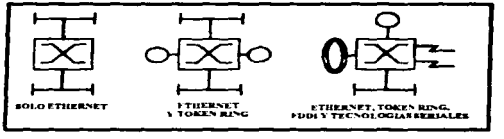
3.10 BACKBONE SWITCHING.

3.10.1 ¿QUE FUNCIÓN TIENEN LOS SWITCHES EN EL BACKBONE?.

a) Centralización recursos.
b) Consolidación del servidor.
c) Ancho de banda agregada.
d) Reducción de la latencia de la red.
e) Integración del ambiente LAN/WAN.

los Switches en el Backbone pueden tener segmentos de LAN, hubs, Ruteadores, servidores etc. Sin embargo, cada Switch debe de encontrar las necesidades de su Backbone.

Los Switches en el Backbone se encuentran en muchas variedades (fig. siguiente). Algunos soportan alguna tecnología única, por ejemplo Ethernet único, otros soportan múltiples tecnologías tal como Token Ring y Ethernet mientras otros soportan Shared, Switched y tecnologías en serie; éste tercer tipo provee conectividad entre estos tres dominios. En esta sección examinaremos los aspectos distintivos que un Switch debe de tener y porque.



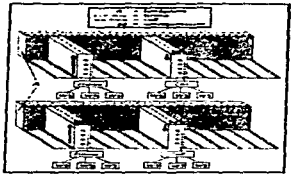
Los Switches del Backbone deben primero proveer tolerancia a falla, después de todo es el corazón de la red, estos Switches deben de tener tablas de dirección grandes que puedan soportar numerosos sistemas y segmentos de red.

Estos Switches necesitan tener un amplio Ancho de banda disponible y la capacidad de acomodar futuros aumentos en el número de usuarios y/o aplicaciones. Además, se requiere de grandes buffers y control de flujo de mecanismos a fin de servir como un punto de agregación para segmentos de bajas velocidades, esto se realiza con una inteligente combinación de software y Hardware. Con el soporte de múltiples tecnologías como Ethernet, Token Ring, FDDI y ATM. cualquier conectividad puede lograrse.

Además, si bien las VLAN's (LAN's Virtuales) aún no son implementadas ampliamente, ellas serán implementadas en corto tiempo, ya que las VLAN's facilitarán la creación de comunidades de intereses que trasciendan ubicación física. La comunicación entre estas VLAN's puede manejarse dentro de la unidad y no requerir de un Ruteador externo.
Otras herramientas de administración de red como RMON (monitoreo remoto) y el inminente RMON II provee capacidades de análisis de tráfico para el Switcheo de la red.

Algunos otros aspectos para considerar en la instalación de los Switches en el Backbone son:

a) Soporta varios tipos de medios físicos para conexiones en los puertos.
b) Soporta full duplex.
c) Soporta niveles de definición para VLAN's (puertos, MAC, política)
d) Configuración fácil de usar.
e) Soporta diversos protocolos.
f) Que cumpla con el estándar de operación de la industria.
g) Procesos distribuidos en lugar de centralizados (como se muestra en la sig. fig.)



CAPÍTULO 4

COMPARACIÓN ENTRE RUTEADORES Y SWITCHES

4.1.-CONSIDERACIONES BÁSICAS PARA EL DISEÑO DE UNA INTERNETWORK.

Antes de empezar a hacer una comparación entre los dispositivos de interconexión, se mencionarán algunos conceptos básicos que deben de tomarse en cuenta antes de hacer la segmentación de una red, los cuales se mencionarán a continuación.

4.1.1.-OBJETIVO DEL NEGOCIO.

El diseño del internetwork debe estar íntimamente enterado de los objetivos del negocio de la compañía. Al comprender los objetivos de la compañía dejará ver como la compañía puede beneficiarse del "internetwork".

4.1.2.-CRECIMIENTO FUTURO

Todas las compañías tienen a corto plazo y a largo plazo metas de negocio. un diseño apropiado de internetwok debe de apoyar estas metas; de modo que, si una compañía que se va extendiendo rápidamente y junto con esta extensión, crece la necesidad de manejar mayores cantidades de información, es importante tener en cuenta un diseño con flexibilidad, así la red puede tener cambios, reacomodos, extenderse, o sufrir cambios de tecnología etc.

4.1.3.-GRUPOS DE TRABAJO.

Toda red y plan de internetwork empiezan y finalizan con usuarios, es lógico que el internetwork debe de mejorar la ejecución del trabajo del usuario, el diseño sería un fracaso si a causa de este, se impide al usuario ejecutar sus tareas.

Idealmente, la red debe trabajar como una herramienta con la cual los usuarios puedan crecer, en consecuencia, esto mejorará la ejecución de su trabajo.

4.1.3.1.-NECESIDADES DEL GRUPO DE TRABAJO.

Los tipos y cantidad de recursos que el internetwork debe de soportar puede ser determinado por una recolección en la red o utilizar los recursos de estadística de workgroups individuales. los métodos estadísticos en la tendencia de los datos son los siguientes:

Utilizar el analizador de protocolos que recoge las estadísticas de la tendencia de los datos.
El throughput (Tráfico en bits por segundo)
Protocolos de transporte usados (IPX, Apple Talk, TCP/IP etc.)
Cantidad de recursos normalmente utilizados (servidor de archivo, impresión etc.)

Este último, es un punto importante, ya que una vez que se examinaron las necesidades de la empresa, el crecimiento futuro y las necesidades del grupo de trabajo. El seleccionar el equipo apropiado para la red puede ser mas sencillo, por ejemplo: si solo se tiene la necesidad de transmitir datos y se prevé que en un futuro no hay la necesidad de manejar tráfico sensible al tiempo, sería inconveniente instalar tecnologías de punta como por ejemplo ATM, esto debido a que la mayoría de las veces nos deslumbramos por lo nuevo en el mercado, pero si en realidad no se va a usar al 100% sería una mala inversión.

4.1.4.-SEGURIDAD.

La seguridad de los datos en la red es vital, para cualquier compañía.

Algunos aspectos a considerar en lo que respecta la seguridad son:
Autenticación del login para recursos críticos.
Seguridad física de dispositivos de recursos críticos (ruteadores, multiplexores etc; instalándolos en cuartos de acceso limitado para evitar manos curiosas o sabotaje).
Seguridad en los datos cuando viajen sobre la red.
Un backup de datos críticos.

4.1.5.-TOLERANCIA A FALLA.

Se puede resumir tolerancia a falla en una palabra:

redundancia; redundancia en ruteadores, dispositivos críticos, recursos etc. al existir la redundancia en estos elementos de la red garantiza el éxito de la compañía.

Por ejemplo: Si la red transfiere tráfico en tiempo real para instituciones financieras, reservaciones en la compañía aérea etc., cualquier caída de la red sin la redundancia puede ser catastrófica para la compañía. La redundancia es importante en todos los puntos críticos de fracaso.

Recíprocamente, si la red es usada sólo para intercambiar información que no es crítica o transmitir de vez en cuando, entonces la redundancia puede ser menos significativa.

4.1.6.-INFRAESTRUCTURA EXISTENTE.

Raramente los diseñadores de redes crean una internetwork en donde no exista algún tipo de dispositivo usado, por lo que la mayoría de las veces se tiene una porción de infraestructura del internetwork en el lugar; los grupos de trabajo existen, y pueden proveer información estadística acerca de lo que quieren los usuarios, requisitos de throughput, etc.. por otra parte, si se ha adquirido una compañía que tiene equipo anticuado, se utiliza de diferente forma o posiblemente incompatible a la compañía acreedora; entonces el desafío del diseñador es integrar el hardware que existe, determinar que protocolos utilizar para que exista una interoperabilidad de las redes sin olvidar el presupuesto que se tiene para alcanzar los objetivos de diseño.

Nunca se sabe cuando el internetwork que se diseña tiene que incorporarse a otro, o cuantos aparatos seguros llegan a ser obsoletos por lo que siempre es bueno escoger equipos y protocolos basados en los estándares de la industria.

4.2.-CRITERIOS TÉCNICOS Y ECONÓMICOS PARA DECIDIR POR RUTEADORES O SWITCHES.

Siempre se debe tomar en cuenta algunos criterios para la compra de cualquier cosa por lo tanto ahora mencionaremos algunos factores necesarios para decidir entre los Ruteadores o los Switches.

4.2.1.-FACTORES A CONSIDERAR.

Ahora veremos los factores principales que se deben tomar en cuenta para la instalación de los dispositivos para la interconexión de redes ya sea un Ruteador o un Switch.

4.2.1.1.- EL TAMAÑO DE LAS REDES.

El tamaño de las redes que se van a interconectar es un factor decisivo para la implementación de alguno de los dispositivos propuestos, ya que el tamaño de la red también tiene que ver con la atenuación de la señal y esto no es bueno para una buena internetworking.

Los Ruteadores son buenos para cuando se requieren conectar redes de grandes dimensiones (con más de siete Hops a través de la red) debido a que el control del flujo de las tramas es muy bueno ya que utiliza el número IP para direccionarlas, los que genera gran confiabilidad en las conexiones hechas por Ruteadores.

Los Switches no son tan eficientes para cuando las redes son muy grandes debido a que como usan el número MAC para direccionar las tramas no llevan un control estricto de los datos enviados y entre mayores sean las redes es mayor el flujo de datos erróneos que pueden circular por la red, y como no son detectados debido a que sus protocolos de transporte son no ruteables y la mayoría orientados a no conexión esto genera que la red desperdicie mucho ancho de banda en la transmisión de estos datos.

4.2.1.2.-REQUERIMIENTOS DE LA RED (EFICIENCIA).

Cuando hablamos de la eficiencia de una red podemos englobar muchos factores como son el throughput, la facilidad de encontrar datos erróneos, etc. Pero por ahora vamos a englobar estos conceptos en uno solo general la eficiencia en general de la red.

La eficiencia de las redes cuando se interconectan con Ruteadores es baja.
La eficiencia cuando se interconectan con Switches es mayor.

4.2.1.3.-PROTOCOLOS.

Los protocolos son una parte fundamental en las comunicaciones debido a que sin ellos no se podrán enviar los datos.

Los Ruteadores usan protocolos ruteables y por lo tanto ocupan más tiempo en desencapsular el número IP para saber hacia donde enviar la trama, pero esto también implica que se tenga un control mayor cuando se envían tramas erróneas.

Los Switches usan protocolos no ruteables lo que significa que para poder direccionar las tramas solo necesitan desencapsular hasta la capa de enlace para saber el número MAC de la maquina a la cual se le debe enviar la trama, esto hace que la red se vuelva mucho más rápida, pero esto también trae sus consecuencias desagradables, debido a que solo desencapsulan el número MAC, no se dan cuenta si en realidad es un número de dirección física o solo es el resultado de la colisión entre las tramas de datos enviadas al mismo tiempo hacia el Switch por dos dispositivos diferentes.

4.2.1.4.-ADMINISTRACIÓN

La administración de la red es un factor que en mucho define la instalación de los dispositivos.

La forma de administrar la red que ofrecen los Ruteadores es una administración Jerárquica, lo que indica que el administrador de la red puede delegar responsabilidades a algunos usuarios, lo que puede generar que se pierda un poco el control de los cambios que puedan existir en la red.

Los Switches ofrecen una forma de administración Centralizada, lo que significa que los administradores de la red son los únicos que pueden hacer cambios a la red y que ningún usuario se puede conectar a un puerto del Switch sin que el administrador se entere.

4.2.1.5.-CONTROL DE LA RUTA

La flexibilidad en el control de la ruta para cuando se esta utilizando los Ruteadores puede ser definitivo debido a que los Ruteadores basan su eficiencia en encontrar la ruta más corta para llegar al destino y así logran la rapidez necesaria para la red.

Los Switches no son tan exigentes en cuanto a un control de la ruta que debe seguir la trama, debido a que ellos solo mandan la trama a la red en donde se encuentra la dirección MAC destino contenida en la trama. (Con excepción de los IP Switches que hacen filtros dependiendo de la aplicación).

4.2.1.6.-ENLACES REMOTOS

Cuando se desean hacer los enlaces remotos es importante considerar que los Ruteadores ofrecen una alta tasa de error debido a que no pueden tener tantas direcciones lógicas en sus tablas de Ruteo.

Los enlaces cuando se utilizan Switches ofrecen una tasa de error menor debido a que solo envían las tramas hacia los Switches vecinos y estos son los que se encargan de direccionar las tramas a su dirección final.

En cuanto al uso del Backbone, la utilización de los Ruteadores limita el ancho de banda a solo líneas de baja y media velocidad (máximo 64 kbps).

Los Switches, sin embargo, utilizan el Backbone a sus máximas capacidades, ya que los Switches por ser una tecnología más nueva están diseñados precisamente para manejar estas velocidades.

4.2.1.7.-TIPO DE APLICACIÓN.

El tipo de aplicación que lleguen a utilizar los usuarios, no es un factor realmente importante, para considerar la evaluación de los Ruteadores o Switches, ya que ellos desencapsulan de las tramas, solo las direcciones (lógicas y físicas correspondientemente), que necesiten para direccionar la trama hacia su destino final, y el resto de la trama solo es desencapsulada por las capas superiores en la estación final a la cual se dirigió la trama. Por lo que los dispositivos nunca saben que tipo de aplicación están transmitiendo y a su vez estos dispositivos de internetworking son transparentes para el usuario.

4.2.1.8.-EL COSTO

El costo entre un Ruteador y un Switch, en la actualidad ya no es tan diferente, ya que los puertos de los Ruteadores (que eran más caros que los puertos de los Switches) han ido disminuyendo sus costos debido a la popularidad que han adquirido los Switches. Aun cuando en redes muy grandes, o más bien dicho, cuando se requiere implementar muchos dispositivos, el costo si se ve afectado, precisamente por el uso de muchos puertos, y aun cuando ya no es mucha la diferencia entre el costo de los puertos de uno y de otro, aun es mayor el costo de los puertos para un Ruteador.

4.2.1.9.-CONDICIONES IDEALES

La red ideal basada en los Ruteadores sería:

- Solamente un protocolo de enlace en toda la red.
- Una WAN muy grande con moderada o baja velocidad de enlace.
- Una organización interdepartamental utilizando la red con una administración y control de forma centralizada.
- Segmentación de la red física únicamente.

La red ideal basada en Switches sería:

- Una mezcla de protocolos de red, entre las estaciones que se comunican
- Una WAN muy grande con velocidades de enlace mucho muy grandes
- Una organización entre departamentos utilizando la red con una administración de tipo centralizada.
- Segmentación de la red de forma lógica.

4.3.-ANÁLISIS EN LA SEGMENTACIÓN DE LA RED.

El problema en las LANs tradicionales (compartidas) son las limitaciones que tienen los usuarios. Virtualmente, cualquiera que ha usado una red ha tenido que lidiar con otros usuarios. Un ejemplo que usamos aquí cuenta con un usuario de finanzas que está bajando del servidor de LAN información fiscal necesaria para un reporte trimestral, al mismo tiempo, un usuario de Mercadotecnia decide checar un nuevo y grandioso Web site en www.xxx.com. Estas demandas simultáneas en la red Ethernet causan colisiones que resultan en una interrupción menor en el servicio para todos los usuarios del segmento.

Mientras mas y mas usuarios demandan servicios de la red. las interrupciones limitan el beneficio que esta provee. Las quejas de los usuarios acerca de los tiempos de respuesta de la red y los timeouts de las aplicaciones. son signos de saturación de la red.

Otra debilidad en las redes compartidas, es el efecto del broadcasts en los usuarios. Los broadcasts son usados por muchos protocolos de red para dar un mecanismo que provee a todos los dispositivos de red interesados con información, tal como dónde se encuentra un servicio especifico y que ruta tomar para llegar a ese servicio.

Otra cuestión acerca de las redes compartidas es cuidar que los datos no caigan en manos equivocadas. Cualquiera que tenga un driver y una aplicación de modo promiscuo, puede capturar frames de red y decodificar los contenidos puesto que el tráfico, desde cualquier punto en el hub, es enviada a todos los puertos del hub.

Cabe mencionar que los análisis en este capítulo se hacen tomando como base a Ethernet. La que la mayoría de las empresas tienen este tipo de tecnología, esto debido a que en los primeros años de la implementación de Ethernet, unir múltiples workstations a una LAN para compartir los 10 Mbps de ancho de banda, era suficiente para mandar correo electrónico, hacer transferencias de archivos, compartir impresoras etc.

Los años recientes han visto el nacimiento de la arquitectura cliente/servidor. Los avances tecnológicos están produciendo computadoras desktop y workstations más rápidas e inteligentes. Audio y video acompañan ahora a los datos en la red.

Planeada cuidadosamente, la segmentación de red es una manera de lograr más ancho de banda por usuario. En la siguiente configuración, por ejemplo, se han creado tres segmentos. Cada segmento es un dominio de colisión, soportando tráfico entre nodos del mismo segmento sin interferencia de los nodos adheridos a los otros segmentos. Mientras más tiempo se quede el tráfico de usuario en un segmento de un grupo de trabajo, cada usuario tendrá más ancho de banda disponible, más que el que tendría si todos los nodos estuvieran unidos al backbone original.

Hay tres métodos principales para segmentar una LAN Ethernet para incrementar el ancho de banda disponible.

- **Segmentación con Puentes.**
- **Segmentación con Ruteadores.**
- **Segmentación con Switches.**

4.3.1.-SEGMENTACIÓN CON PUENTES.

Los puentes se usaban ampliamente para segmentar LAN's de tipo Ethernet para dar más ancho de banda por usuario. Ahora han sido remplazados en el mercado por Switches.

El funcionamiento de los puentes se describió en el capitulo 1, pero la razón por la que han sido reemplazados por los Switches es que los puentes introducen una penalidad de tiempo de espera para procesar la sobrecarga. El tiempo de espera es alrededor de 20-30% en pérdida de flujo para los protocolos orientados a reconocimiento y de 10-20% para los protocolos de ventana deslizante. Este retraso puede aumentar significativamente si el frame no puede ser enviado inmediatamente directo a la actividad actual en el segmento destino.

Los puente envian frames tipo multicast broadcast. Esta caracteristica puede disminuir las ganancias del ancho de banda logradas como resultado de la segmentación. Las direcciones de multicast y broadcast nunca son usadas como una dirección fuente, por lo tanto, nunca aparecen en las tablas de direcciones asociadas con los puertos del puente. Pueden surgir "tormentas de broadcast" mientras estos frames se propagan por toda la red.

4.3.2.-SEGMENTACIÓN CON RUTEADORES.

A diferencia de los puentes, el ruteador es conocido por las estaciones que usan sus servicios y, como se menciono en el capitulo 2, debe de ser usado un protocolo bien definido entre estas y el ruteador.

Los ruteadores ofrecen las siguientes ventajas en una red:

- **Manejabilidad:** Existen protocolos explícitos operando entre ruteadores, dando al administrador de red mayor control sobre la selección de rutas, y el comportamiento de ruteo de la red es más visible.

- **Funcionalidad:** Los ruteadores pueden implementar mecanismos para proveer control de flujo, control de error y congestión, servicios de fragmentación y reensamble, y control explícito de tiempo de vida de paquetes.

- **Rutas activas múltiples:** Las topologías de red pueden ofrecer más de una ruta entre estaciones. Al operar en la capa de red, los ruteadores pueden examinar el protocolo, el punto de acceso de servicio destino (DSAP), el punto de acceso de servicio fuente (SSAP), e información métrica de ruta antes de tomar decisiones de envío o filtrado.

Para dar las ventajas mencionadas anteriormente, los ruteadores deben de ser más complejos y tener más software que los puentes. Los ruteadores proveen un nivel más bajo de desempeño en términos de frames o paquetes que pueden ser procesados por unidad. Comparándolos con un puente, los ruteadores deben de examinar la sintaxis e interpretar las semánticas de más campos en un paquete. La penalidad por esta función agregada es una perdida del 30-40% de flujo para los protocolos orientados a reconocimiento y 20-30% para protocolos de ventana deslizante.

Cisco utiliza un mecanismo de software para reducir estos tiempos de espera llamado NetFlow Switching identificando flujos de tráfico entre hosts. Entonces, sobre una base orientada a conexión, este mecanismo switchea paquetes en este flujo. Los paquetes son switcheados y los servicios son aplicados a ellos mediante una tarea sencilla. Esta forma de manejo de paquetes por flujo permite a los ruteadores de cisco aumentar grandemente el desempeño para servicios de red.

4.3.3.-SEGMENTACIÓN CON SWITCHES.

La tecnología más reciente introducida para segmentación de LAN es el Switch de LAN. Los Switches de LAN permiten intercambio de datos de alta velocidad. Los servidores propiamente configurados en un medio ambiente de Switches, logran un acceso completo al ancho de banda del medio que se está usando.

El término "switcheo" ha sido aplicado a varios conceptos de red:

- **Switcheo de configuración de puerto:** Permite que un puerto sea asignado a un segmento físico de red bajo control de software. Esto es una manera muy simple de switcheo.

-**Switcheo de frame:** Fundamentalmente utilizado para incrementar el ancho de banda disponible en la red. El switcheo de frames permite que ocurran transmisiones múltiples en paralelo. Este tipo de switcheo lo efectúan todos los Switches Catalyst.

-**Switcheo de celdas (ATM):** Es similar al switcheo de frame. En ATM, pequeñas celdas de una longitud fija son switcheadas en la red. Este es el tipo de switcheo desempeñado por todos los Switches Cisco LightStream.

El switcheo de Ethernet incrementa el ancho de banda disponible en una red creando segmentos de red dedicados e interconectando los segmentos. Algunos dispositivos, tales como el Catalyst 3000 (pero no el Catalyst 5000), utilizan circuitos virtuales de alta velocidad para conectar los segmentos. Cada segmento puede estar comprendido de uno o más nodos. Mientras el ancho de banda total del Switch no sea excedido, cada segmento dedicado sumado a la red a través del Switch incrementa la velocidad agregada de ésta.

Un Switch de Ethernet trabaja con tarjetas de red que soportan el estándar 802.3 y cableado.

La habilidad para utilizar recursos existentes provee un desempeño de red incrementando a más bajo costo que otras alternativas. Un uso más eficaz del ancho de banda disponible y una mayor flexibilidad en la infraestructura de la red son los beneficios adicionales del switcheo.

4.3.4.-SEGMENTACIÓN CON RUTEADORES Y SWITCHES.

El switcheo de Ethernet es complementario al ruteo. Los beneficios del switcheo de LAN aumentan cuando la comunicación de datos se mueve del ambiente de WAN al desktop. Recíprocamente, la tecnología de ruteo aumenta en importancia cuando la comunicación de datos se mueve de LAN a WAN.

El switcheo de LAN provee un significativo perfeccionamiento de flujo entre servidores de LAN locales y computadoras desktop.

Los ruteadores establecen firewalls para limitar a los frames broadcast y multicast, dan a la red un alto nivel de seguridad, habilitan conexiones de WAN y también habilitan conexiones de LAN's distintas.

La tendencia en el diseño de LAN es dar auxilio a los usuarios finales cambiando de hubs compartidos a Switches de LAN. La gran ayuda que otorgan los Switches de LAN y ATM al ancho de banda -junto con las LANs virtuales y el ruteo- puede proveer redes estables y escalables.

Dando soporte de medios de comunicación para Ethernet, Fast Ethernet, ATM, FDDI y Token Ring, los Switches de LAN son reemplazos excelentes para hubs compartidos en una amplia variedad de ambientes.

El switcheo de LAN puede ser usado para microsegmentar redes existentes con el propósito de dar ancho de banda dedicado a los usuarios finales. Este incremento en el ancho de banda, el cual puede mejorar de una manera significativa la productividad del usuario decrementando la cantidad de tiempo que se pierde cuando se espera por el acceso a la red, puede ser doblado cuando se utiliza el modo full duplex.

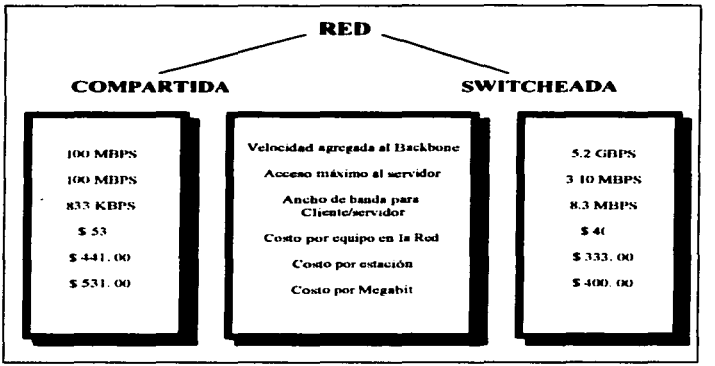
Finalmente, los Switches permiten el uso de LANs virtuales para reducir los costos de administración de red. Las LANs virtuales son discutidas a detalle en el capítulo 3 de Switches.

El switcheo de LAN reduce las razones de colisión dando múltiples segmentos dedicados para uno o varios usuarios. Enlaces de alta velocidad, como Fast Ethernet, FDDI y ATM son utilizados para conexiones de servidores y de backbone. Dando más ancho de banda y escalando el backbone a tecnologías de más alta velocidad, los Switches mejoran el tiempo de respuesta de la red e incrementan la productividad del usuario.

4.4.-ANÁLISIS COSTO/BENEFICIO.

Sería ingenuo no considerar algunas de las implicaciones comerciales del switcheo en el backbone. Después de todo, Las ventajas del switcheo en el backbone provee en los negocios toda la justificación requerida que explore e incremente una solución. Pero, un interés importante para la mayoría de las organizaciones es que es una tecnología muy cara: con inversiones en dispositivos que típicamente constituyen una red compartida (ruteadores, puentes, hubs) muchas compañías eluden el backbone de ATM a causa de que los costos son altos.

A continuación se hace un estudio del caso costo/beneficio entre una red compartida y una red de Switches.



El análisis de costo se calculó suponiendo 10% de la población de usuarios que lidia por recursos en la red.

Como se puede ver la diferencia en el ancho de banda y el acceso al ancho de banda en el backbone es dramática, si todos los usuarios intentaban conectarse al servidor de archivos simultáneamente, la red de Switches estaría muy por arriba de la red compartida en cuanto al ancho de banda disponible y el costo (no incluyendo adaptadores) por megabit de un sistema de Switches es significativamente más inferior que el de una red compartida.

4.4.1.-MANTENIMIENTO.

Aparte de lo costoso de los equipos, la instalación y mantenimiento en una red compartida puede resultar muy caro. Por ejemplo, el mantenimiento de un ruteador es complejo, si la pericia viene desde el personal dentro de una organización o desde un proveedor de outsourcing los costos pueden elevarse rápidamente.

4.4.2.-CRECIMIENTO FUTURO.

El crecimiento de red puede ser caro y no debería ignorarse. Mientras más usuarios y aplicaciones se agregan a la red, los cambios que se deben de hacer a ésta deben de ser sin la menor interrupción importante de servicio. Por lo que un backbone de Switches escalable aliviaría los posibles problemas que acarrearía una red compartida y ahorraría dinero a largo plazo.

4.4.3.-OPERACIÓN COTIDIANA.

El Switch en el backbone puede ahorrar dinero en operaciones cotidianas. Por ejemplo, instalando Switches en el backbone y aumentando el ancho de banda disponible en el ambiente de usuarios LAN, mas trabajo puede completarse en la misma cantidad de tiempo. Esto se traduce en verdaderos ahorros de costo.

4.4.4..-SOPORTE.

Una vez que la compañía ha decidido implementar backbone Switching, necesita mantenimiento y soporte confiable. El mantenimiento y programas de soporte de una fuente competente puede ser invaluable y puede ahorrar dinero.

Un diseño de red debe reflejar el nivel de competencia de la gente que labora en su empresa; de otra manera, outsourcing debe evaluarse como opción. Si outsourcing se requiere para experiencia técnica, se debe de escoger alguien que tenga la experiencia y el conocimiento requerido y que haya trabajado con los productos que tiene su red. En México las compañías que ofrecen outsourcing son: IBM, TELMEX, AT&T e INTERSYS.

Existen otros aspectos que deben ser considerados en la implementación de el backbone de Switches.

- Presupuesto de la compañía.
- Competencia y presión de otras compañías.
- Cultura corporativa.
- Experiencia interna.
- Infraestructura de cableado estructurado existente.
- Expectativas del usuario en la red.
- Arriesgo en la inversión.
- Seguridad.

4.5.-CONSIDERACIONES QUE DETERMINAN LA ELIMINACIÓN.

4.5.1.-DE LOS RUTEADORS

Cuando se utilizan múltiples protocolos en la red, los Ruteadores no son capaces de manejar todos con la misma eficiencia, lo que genera colisiones dentro de la red y a su vez deteriora la velocidad de transmisión en la red.

Las redes que utilicen protocolos no ruteables, generan una limitante para los Ruteador.

4.5.2.-DE LOS SWITCHES.

Cuando se tiene un número excesivo de saltos entre dos estaciones que deseen comunicarse, los Switches provocan que se deteriore la velocidad de la red debido a que ellos solo envían la información a los Switches vecinos sin importarles si es el camino más optimo para enviar la información.

Cuando se envían datos que están erróneos, el Switch no tiene manara de saberlo, ya que el análisis que él hace de las tramas no es tan a fondo como el que realizan los Ruteadores.

Otra de las desventajas que presentan los Switches es que, debido a que ellos están diseñados para trabajar a grandes velocidades, solo se dedican a recibir e inmediatamente reenviar la información, y no pueden retenerla mucho tiempo sino solo el necesario para desencapsular el número MAC, esto provoca que cuando exista alguna colisión o alguna caída de la red, o que por algún motivo el Switch no pueda enviar la información, pero si sigue recibiendo mas tramas, entonces el Switch opta por el método mas simple "tira a la basura" las tramas que no pueda enviar, esto provoca que se tenga que reenviar la trama y a su vez es perdida de tiempo.

4.6.-CONSIDERACIONES DE RENDIMIENTO.

4.6.1.-LA LATENCIA

La latencia es otra de las consideraciones que debemos tomar en cuenta en la conexión de algún dispositivo de internetworking.

La latencia depende básicamente del tipo de protocolo que se este utilizando en la red, a esto nos referimos a, que si es orientado a conexión u orientado a no conexión, ya que si se utiliza un protocolo orientado a no conexión, prácticamente la latencia desaparece en la red, porque el dispositivo que envió la trama, no necesita

obtener una respuesta de que si llego o no correctamente, sino que el sigue enviando las tramas restantes.

Pero cuando se utilizan protocolos orientados a conexión, ya sean Ruteables o no Ruteables , la latencia si juega un factor importante en la red, además de que se puede llevar un mejor control del envío de la información, y esto no es básico del Hardware sino del Software que se este utilizando, por lo que los dispositivos solo intervienen o se ven involucrados en cuanto a la velocidad con que ellos hagan llegar la trama a su destino.

4.6.2.-LOS VOLUMENES DE TRANSFERENCIA. (Throughput)

Este rubro puede generar una gran confusión en cuanto a cual es el dispositivo que mejor maneje el Throughput, que como ya se menciono es la relación que existe entre la cantidad de datos enviados y el tiempo que se tomo en enviarlos, si nos basamos literalmente en el concepto, no hay duda de que los Switches ofrecen un mejor manejo del Througput debido simplemente a la velocidad de transferir información, pero la confusión empieza cuando se analiza que tan correctos son los datos enviados ya que los Switches debido a su arquitectura tienen un menor control de la información enviada, por lo que es mas susceptible a enviar información errónea quizás ocasionada por alguna colisión.

En cambio los Ruteadores como llevan un mayor control de los datos que envían pueden evitar enviar información que no sean realmente lo que se esta transmitiendo, y así lograr que el Throughput no solo se enfoque a que tantos datos pueden enviar en un tiempo determinado, sino a que tantos datos correctos pueden enviar en el mismo tiempo.

4.7.-CRITERIOS PARA LA COMPRA DE PRODUCTOS DE INTERNETWORKING.

4.7.1.-EL PRECIO.

Sin duda el precio es un factor importante cuando se va a decidir comprar un articulo cualquiera, y mucho más lo es cuando se va a decidir entre comprar un Ruteador o un Switch debido a que de ello dependerán las comunicaciones en la empresa.

En este capítulo mostramos algunos artículos y sus precios estimados .

4.7.2.-POLITICAS EMPRESARIALES.

Puede existir la posibilidad de que la empresa tenga algún convenio con alguna empresa que venda estos productos, por lo tanto se tiene que apegar a las condiciones o a los productos que esa empresa ofrezca, sin tener la posibilidad de conocer otros proveedores.

4.7.3.-SOPORTE DEL PROVEEDOR .

El soporte técnico que ofrezca el proveedor es importante debido a que este tipo de tecnología se mantiene con una constante evolución, y es difícil que en la empresa tenga gente capacitada para resolver los problemas que se puedan generar con estos productos, aun cuando los administradores de red tienen la obligación de estar actualizándose día a día, siempre existirá un problema que no se pueda resolver ni con los manuales de usuario que el mismo proveedor ofrezca.

4.7.4.-EXPERIENCIA DEL VENDEDOR.

La experiencia a la que nos referimos no es a la experiencia que tenga como vendedor, sino a la experiencia que tenga en cuanto a las normas y estándares internacionales y que tanto se apegue a ellos, también se debe tomar en cuenta en que comités de normalización pertenece y cual es su influencia en ellos.

Esto nos dará la seguridad necesaria para saber si los productos que deseemos adquirir serán compatibles con los de cualquier otra empresa y así logremos la comunicación con quienes nosotros quisiéramos sin preocuparnos de la compatibilidad y sobre todo sin importar el que exista la posibilidad de que no se puedan comunicar con nosotros.

4.7.5.-INTERFACES REQUERIDAS

Es necesario conocer si los proveedores soportan las interfaces que nosotros requerimos, para conectar el nuevo dispositivo a nuestra red.

4.7.6.-PROTOCOLOS SOPORTADOS

Como ya se vio en los capítulos anteriores, existen un gran número de protocolos y es importante saber que tipo de protocolo soporta el dispositivo que vamos a adquirir, porque no se puede cambiar toda la arquitectura ya instalada solo porque el dispositivo no soporta el protocolo que ya esta implementado, es mas fácil comprar un dispositivo que soporte lo que ya tenemos.

4.7.7.-SEGURIDAD.

La seguridad es uno de los puntos más delicados a estudiar, ya que tenemos que ver que tan segura quedará nuestra red en cuanto a las opciones de que alguien se filtre a la red sin que se de cuenta el administrador, y no solo que ocupe los recursos, sino que pueda entrar a información confidencial, o que provoque cualquier cosa que pueda dañar la integridad de la red, por eso es que la seguridad en todo tipo de redes juega un papel importante.

4.7.8.-INTERFACE PARA EL USUARIO.

En el caso de los dispositivos de internetworking, el usuario realmente es la red, pero a esta interface para el usuario a la que nos referimos, es a que tan amigable es la forma de programar el dispositivo para los administradores, ya que entre mas complejo sea la forma de programar los dispositivos serán mas propensos a errores.

4.7.9.-DOCUMENTACIÓN.

Es de vital importancia que el proveedor ofrezca manuales de instalación, manuales de mantenimiento y sobre todo manuales de usuario, y que además sean claros y concisos ya que sin ellos no podremos saber como hacer funcionar correctamente el aparato que vayamos a adquirir.

4.7.10.-SOFTWARE

El software de equipo se carga a través de la red, o se tiene que cargar manualmente a cada equipo, ya que estas son características que el administrador tendrá que tomar en cuenta para cargar el software, también se puede cargar remotamente.

4.8.-CARACTERISTICAS PRINCIPALES DE ALGUNOS DE LOS PRODUCTOS.

Existe una infinita gama de productos así como de marcas, por lo que nos resultaría imposible mencionarlos a todos, debido a esto, solo ponemos algunos ejemplos de los productos, y si se requiere de una mayor información, en la bibliografía informamos de las direcciones de Internet en donde se podrá adquirir mayor información de los productos que se requieran.

4.8.1.-PLATAFORMA ESCALABLE DE SWITCHES (CISCO).

El primer nivel de bloques para la edificación de la interconexión de redes switcheadas es la plataforma física del Switch. Cisco ofrece un amplio y óptimo rango de plataformas con Switches que son diseñadas para el desarrollo a través de el amplio rango de aplicaciones, desde los grupos de trabajo de un backbone trabajando juntos.

La Familia de Switches Catalyst.

La familia Cisco Catalyst es una línea de Switches diseñados para ofrecer una alto rendimiento para ayudar a los usuarios a emigrar fácilmente desde la tradicional LAN's compartidas hasta unas redes completamente Switcheadas. Un elemento integral en la familia Cisco es la arquitectura escalable, la familia Catalyst libera los variantes niveles de flexibilidad y costo/eficiencia para los requerimientos actuales, como en las aplicaciones de los grupos de trabajo, el área de trabajo y el Backbone, mientras se habilita la interconexión de redes de área amplia.

La marca de dispositivos Cisco a puesto en el mercado una infinidad de productos para la interconexión de redes, por lo cual sería imposible mostrarlos todos, es por eso que solo mencionaremos las características principales de algunos de la familia Catalyst.

El Switch Catalyst 5000 soporta altas densidades de Ethernet, Token Ring, FDDI, ATM y Fast Ethernet, en un único chasis modular. Además con la utilización de la arquitectura VLAN, un futuro opcional al Switchear diferentes niveles y al aumentar las capacidades de tráfico, el Catalyst 5000 es optimo para un alto rendimiento en las aplicaciones de la empresa.

El Catalyst 3000 ofrece capacidades VLAN y tolerancia a la falla de Switcheo utilizando una única arquitectura escalable de Software/Hardware. La arquitectura apilable del Catalyst 3000 acomoda aplicaciones crecientes del Switch para conectar

grupos de trabajo a servidores o a Backbones de Fast Ethernet o ATM. El Catalyst 3000 es perfecto para grupos de trabajo y gabinetes de cableado que tiendan a crecer.

El Switch Catalyst 2000 combina alta velocidad y flexibilidad en la configuración de los puertos con excepcional productividad para las aplicaciones de los grupos de trabajo Ethernet y usuarios individuales que requieran incremento en el rendimiento y conectividad con los servidores o con el Backbone 100 base T, FDDI, o ATM.

El Catalyst 1000 libera el mejor valor de costo/rendimiento de la industria, este Switch provee 10 Mbps Ethernet dedicados a cada usuario y provee 100 Mbps al conectarse a los servidores o Backbones y además para una un mayor rendimiento y una mejor productividad provee una alternativa para medios compartidos con la utilización de Hubs 10 Base T.

El Catalyst 1200 es el mas "inteligente" de Cisco, este Switch multinivel soporta la adición de Multicast IP, VLAN, Funciones de ruteo IP, además los administradores no tendrán que usar aplicaciones de control tan sofisticadas.

4.8.2.-LA FAMILIA DE ATM SWITCHES LIGHTSTREAM.

Esta familia de Switches ATM ofrece un completo rango de soluciones para el Switcheo ATM, por ejemplo: La utilización de Switches ATM para el área de trabajo de los grupos, para interconectar diferentes campus que utilicen LAN Switches, para interconectar servidores y Ruteadores compartidos con ATM, además soportando protocolos de WAN, tráfico de voz y vídeo a través de un Backbone común de ATM.

El LightStream 1010 es un sistema de Cisco de la próxima generación de Switches ATM para grupos de trabajo y el despliegue de Backbones.
Incorporando más tarde el soporte para las especificaciones del ATM Forum y construyendo el Software Cisco IOS. El LightStream ofrece el más completo y sofisticado rendimiento, escalabilidad y robustez requeridos para el desarrollo de la producción ATM.

El LightStream 1010 ha sido desarrollado para soportar un amplio rango en el Backbone, en la manera modular para un cambio rápido, en el ambiente de trabajo y también para soportar las interfaces ATM para WAN. Estas características también son flexibles y se desarrollan bajo un ambiente costo-efectividad en una variedad de escenarios, desde alta densidad como 155 Mbps usando UTP nivel 5 para grupos de trabajo, hasta alto rendimiento en los Backbones.

El LightStream 1010 también ofrece la sofisticación y profundidad de la funcionalidad verdadera requerida para el desarrollo de la producción ATM, ventajas en los mecanismos de administración del tráfico, permitiendo el soporte de la corriente, un mejor contacto con el tráfico, mientras también reflexiona acerca de la calidad de servicio (Quality of Service QoS) y las garantías requeridas para las aplicaciones del futuro, permite también un soporte en el control de las ráfagas disponibles.

El LightStream permite una disminución en la velocidad de la fuente de tráfico antes de que la congestión llegue a ser excesiva.

El valor adicionado a las capacidades para el acceso a ATM, hace que se cargue a través de enlaces redundantes compartidos.

Todas estas sofisticaciones están ocultas por la verdad basada en los estándares y en las capacidades plug and play del LightStream 1010.

El LightStream 2020 es un multiservicio de alto rendimiento para la empresa , es un Switch ATM que reúne las demandas de las más exigentes redes. El LightStream 2020 perfectamente complementa el LightStream 1010, expandiendo el rango desde el más lejano campus de la empresa hasta las aplicaciones en redes privadas para el desarrollo de multiservicios de redes publicas. En algún escenario de desarrollo la definición valor agregado se le asigno al LightStream 2020 ya que tiene la habilidad de integrar múltiples paquetes, circuitos , interfaces ATM y servicios en una común y homogénea infraestructura ATM, estos avances pre-estandarizan la administración del tráfico aseguran con los protocolos de ruteo la máxima utilización del ancho de banda del Backbone.

4.8.3.-ACCESO CON RUTEADOR DE LA FAMILIA CISCO.

Cisco construye la más alta calidad en soluciones de "internetworking" para la empresa, que permite un excepcional rendimiento, escalabilidad y estabilidad. El Cisco 7000 y el Cisco 4000 son Ruteadores multiprotocolo que son particularmente bien situados para una interconexión con Switches, en particular, el primero, nativo de la interfaz de Ruteador ATM es una llave fundamental para la integración existente entre LAN y WAN con la posibilidad de evolucionar a ATM basada en redes Switcheadas.

La sofisticada señalización ATM, las capacidades de administración del tráfico y las interfaces ATM permitirán también que jueguen un papel importante en el desarrollo de nuevos servicios como VLANs.

4.8.4.-EL MPRUTEADOR DE MOTOROLA

El Motorola 6520 Multimedia Periphery Ruteador (MPRUTEADOR) es un producto para acceso a WAN optimo para oficinas de mediano tamaño que dependan de la eficiente integración del tráfico SNA/SDLC etc. Con el tráfico de LAN en X.25, Frame Relay, PPP, y circuitos ISDN.

Con el mas fuerte multiprotocolo soportado, la mas avanzada prueba de cliente en capacidades SNA y el más amplio rango de optimización del ancho de banda para WAN, el 6520 MPRUTEADOR minimiza el costo para ambientes de comunicación de datos únicamente mientras provee un alto grado de caminos para el desarrollo de ambientes multimedia.

El 6520 MPRUTEADOR ofrece soporte a cada LAN Ethernet o Token Ring e incluye soporte para mas de cinco puertos seriales con dos de ellos soportando una velocidad síncrona arriba de 1.544 Mbps. El MPRUTEADOR puede ser expandido para soportar 19 puertos seriales. Este es uno de los productos que tienen la capacidad de soportar ISDN

4.8.5.-CATALYST 5000

El sistema de switcheo Catalyst 5000 de Cisco permite a los usuarios construir redes partiendo de un sistema basado en un chasis modular y flexible a un costo razonable y con un alto nivel de rendimiento. Como un elemento integral de CiscoFusion, el equipo Catalyst 5000 provee una alta densidad de puertos y VLANs ya que integra la funcionalidad del Cisco Internetworking Operating System (CISCO IOS). La arquitectura del Catalyst 5000 soporta conexiones switcheadas a 10 Mbps Ethernet, 100 Mbps Fast Ethernet, CDDI/FDDI y ATM.

El chasis modular provee la flexibilidad de acomodar todas las topologías dinámicas existentes hoy en día, y la escalabilidad de enfrentar las demandas de ancho de banda, velocidad y todos los avances en aplicaciones. Los módulos de interface soportan una gran variedad de interfaces, velocidades, densidades con una gran opción de conectores. Cada modulo de interface ocupa un solo slot de expansión en el chasis, el cual cuenta con 5 slots. El modulo de Supervisory Engine, un requerimiento del sistema, también ocupa un slot. El chasis completamente lleno soporta una gran variedad de combinaciones: hasta 98 interfaces Ethernet switcheadas y hasta 50 interfaces Fast Ethernet (100 Mbps).

El Supervisory Engine permite en si que se lleve a cabo el switcheado y la administración de la red, además de ofrecer dos interfaces 100 Base TX Fast Ethernet para conexiones a servidores o al backbone.

A continuación se listan los diferentes tipos de interfaces existentes para el equipo Catalyst 5000.

- 24 interfaces 10 Base T (10 Mbps Ethernet, full o half dúplex)
- 12 interfaces 10 Base FL (10 Mbps Ethernet, full o half dúplex)
- 12 interfaces 100 Base TX (100 Mbps Fast Ethernet, full o half dúplex).
- Una dual Attached station 100 Mbps FDDI/CDDI.
- Una interface ATM a 155Mbps.

El Catalyst 5000 ofrece un backplane del tipo Synergy Switching Backplane el cual ofrece un throughput de 1.2 Gbps lo cual permite cableado de 10 y 100 Mbps Ethernet, entregando un "low latency" (baja latencia) y alrededor de un millón de Bps. El backplane recibe el nombre de Synergy Switching Backplane debido a que se trata solo de un single-backplane el cual acomoda de manera simultánea todos los tipos de medios existentes (Ethernet, Token Ring, FDDI y ATM) deliberando una solución bajo el mismo sistema para todas las necesidades de switcheo con una migración directa a ATM. Otra característica que ofrece este backplane es que cuenta con tres prioridades de que es en el backplane de switcheo de datos; de esta manera los usuarios pueden configurar niveles de alta o baja prioridad en cualquier interfaz de switcheo para, de esta manera, acomodar tráfico lento y pesado.

El Catalyst soporta la formación de grupos de trabajo, tanto en el mismo equipo como entre otros Catalyst 5000 extendiendo redes virtuales (VLANs) entre plataformas a través de conexiones CDDI/FDDI, Fast Ethernet y ATM. ATM soporta VLANs multiplexando LANs en circuitos virtuales.

El Catalyst 5000 cuenta con un soporte para entradas estáticas así como auto aprendizaje para un máximo de 16,000 direcciones activas MAC en su tabla. También cuenta con soporte al algoritmo Spanning Tree. Una característica importante es que cuenta con un soporte completo e integrado para VLANs.

4.8.5.1.-ADMINISTRACIÓN DE TRÁFICO.

El Catalyst 5000 soporta tres niveles de prioridad dentro del Synergy Switching Backplane. Dos niveles de prioridad son definidos por el usuario. Cada interface puede ser configurada como Alta prioridad o Baja prioridad (prioridad baja es el default status). El bus mantiene colas (queues) lógicas separadas para cada clase de prioridad, esto garantiza que las colas con prioridad alta serán atendidas primeramente, reduciendo latencia causado por el retraso en el buffer.

La latencia, en esta arquitectura, es no determinística ya que depende del número de dispositivos que accesan simultáneamente el backplane así como de la prioridad asignada a es puerto.

4.8.6.-KALPANA PROSTACK 16

Así como los Switches de la familia Catalyst pueden ser comparados con los concentradores modulares e inteligentes, la familia Kalplana puede ser comparada con los concentradores apilables (Stackable hubs). Con un tiempo de latencia cercano a cero, eficiencia de 100% en cuanto a forwarding, tecnología full dúplex y conectividad de alta velocidad, la familia de Kalpana eleva el throughput por mas de diez veces. Todos los productos Kalplana soportan el Simple Network Managemente Protocol, la cual permite a los usuarios monitorear estos Switches desde cualquier sistema de administración.

La familia Kalplana es mas apropiada para elevar el performance existente en la red o aplicaciones departamentales que están experimentando congestionamiento. La naturaleza de plug and play de los productos Kalplana los convierten en equipos de muy fácil instalación y mantenimiento.

Basado en su experiencia, Kalplana desarrolló el sistema ProStack, plataforma de switcheo apilable. El Etherswitch pro 16. de la familia ProStack, permite a los usuarios expandir la capacidad de su red conforme los requerimientos de ancho de banda lo exijan sin la necesidad de migrar a una nueva plataforma. El equipo básico EtherSwitch Pro 16 soporta 16 puertos Ethernet, con dos slots de expansión para dos módulos de alta velocidad. Cada puerto de expansión puede ser "llenado" con una amplia variedad de módulos para satisfacer las necesidades del cliente. En caso de necesitarse colectividad a alta velocidad los puertos de expansión pueden ser cubiertos con módulos de Fast Ethernet o ATM.

De dos a ocho EtherSwitch Pro 16 pueden apilarse para lograr un sistema de hasta 192 puertos switcheados con una capacidad de switcheo de 4.8 Gbps.

A continuación se muestra una lista con las características más relevantes de este equipo:

* Puertos:
Cada equipo de switcheo cuenta con 16 puertos 10 Base T (RJ-45) y un puerto AUI.
Modulo de expansión PRO 16: RJ-45.

- **Módulos de Expansión:**

  Modulo con 4 puertos 10Base T.
  Módulo con un puerto 100Base TX.
  Módulo con tres puertos 10Base FL.
- **Software Upgrades:**
  Vía flash EPROM.

Conclusiones.

La elaboración de estos apuntes ha constituido un problema estructural, debido a que la mayor parte de la información recopilada en ellos ha sido extraída de los mismos documentos elaborados por los fabricantes de los aparatos por lo que resultó un tanto complejo redactar, analizar y enfocar el punto de vista de cada uno, hacia un punto de vista imparcial y que realmente enfoque al funcionamiento real de los aparatos sin tomar en cuenta las estrategias de mercadotecnia de cada fabricante para vender sus productos. Con lo cual podemos decir que se logró dar a conocer de una manera bastante amplia, el funcionamiento de cada aparato así como la tecnología empleada actualmente en materia de redes digitales y las expectativas a futuro. Quizás nuevas tecnologías modifiquen algunos aspectos, pero consideramos que las bases están dadas y con ello logramos cumplir el objetivo de este documento.

Con la elaboración de éste trabajo hemos logrado enfocar los conocimientos, que teníamos de una manera abstracta, adquiridos en la escuela y los hemos podido llevar a una forma de conocimientos aplicados a la industria, lo cual consideramos que es muy importante debido a que la mayor parte de lo que aprendemos en la escuela siempre se queda en el aire, es decir, sabemos que existe, pero no sabemos como aplicarlo a una manera práctica.

Consideramos que el presente trabajo aporta un "Valor agregado" , ya que hemos hecho una recopilación de información dispersa en libros, cursos de empresas, revistas y muy considerablemente en internet, lo cual facilitará al lector, la consulta de información específica en un tema, sin tener que consultar en todas las fuentes mencionadas anteriormente. También creemos en este valor debido a que los alumnos de la UNAM, podrán contar con información de la tecnología de punta y con ello aprender de la tecnología nueva, con la que realmente se van a encontrar en su área laboral.

En este trabajo no solo hacemos un análisis comparando los Ruteadores con los Switches, sino que también da pie a nuevas ideas para aprovechar mejor la infraestructura y de hecho permite tener parámetros de evaluación para iniciar el diseño conceptual de una red.

Después de todo el análisis, información recopilada y conocimientos adquiridos podemos concluir que nunca un Ruteador va a ser mejor que un Switch o viceversa, sino que cada uno aporta condiciones o características diferentes, por lo que la conveniencia de instalar uno u otro será dependiendo de las redes que queramos interconectar, pero después de leer este trabajo y conociendo las necesidades de su red, un administrador o diseñador de redes podrá saber con exactitud que le conviene instalar, pero el trabajo no solo está enfocado a ellos, sino que cualquier persona ajena al tema, después de estudiar este trabajo conocerá y aprenderá todos los conceptos básicos que se necesitan saber para comprender el funcionamiento de una red, hasta la capacidad de tomar las decisiones de instalar un Ruteador o un Switch.

PROTOCOLOS IEEE 802.

La IEEE (Institute of Electrical and Electronics Engeneers) es una organización profesional Americana que define los estándares relacionados con la interconexión de redes así como de otras áreas de la electrónica y de las comunicaciones. Los estándares IEEE 802.X son estándares que se refieren a la interconexión de redes, los cuales son también recomendaciones y documentos informativos acerca de las redes y las comunicaciones.

Las publicaciones de la IEEE son el producto de varias técnicas, estudios y grupos de trabajo, algunos de estos grupos de trabajo han sido reunidos a lo largo de una década mientras otros solo en algunos meses.

Las recomendaciones de la IEEE son principalmente referidas a los niveles mas bajos del modelo de referencia OSI los cuales son el nivel Físico y el nivel de Enlace. La IEEE reconoce dos subniveles en el nivel de enlace del modelo OSI, uno más bajo que es el nivel MAC (Media Access Control) y uno superior que es el subnivel LLC (Logical Link Control).

Note que varios de los estándares, como el 802.1 y el 802.11 han sido adoptados y supervisados por las nuevas versiones del modelo OSI como la 8801-1 ó la versión 8802-11cuyos estándares son aceptados internacionalmente. La literatura todavía no alcanza éstas revisiones, por lo que vera referencias a IEEE 802.3, por ejemplo, en lugar de ISO/IEC 8802-3.

Las siguientes son las normas IEEE 802.X.

802.1.- Especifica los estándares para la administración de la red utilizando el subnivel MAC, incluyendo el algoritmo "spanning tree", este algoritmo es usado para asegurarse que una sola ruta ha sido seleccionada para pasar mensajes entre redes usando puentes y para encontrar otra ruta en caso de que la primera se caiga, este documento también maneja los sistemas de direcciones.

802.2.- Define el funcionamiento del subnivel LLC de la capa de enlace del modelo OSI. El LLC provee una interfaz entre los métodos de acceso al medio y el nivel de red, las funciones que provee el LLC son transparentes para las capas superiores, estas funciones incluyen el direccionamiento y el control de error. Este subnivel es usado por las especificaciones Ethernet 802.3 pero no son usadas por las especificaciones Ethernet II.

802.3.- Describe el nivel físico y el subnivel MAC para redes de banda base que usen topología de BUS y CSMA/CD como esquema para el acceso a la red, éste esquema fue desarrollado en conjunción con Digital, Intel y Xerox, para que fuera

totalmente compatible con Ethernet. Ethernet II e IEEE 802.3 no son idénticos, sin embargo es permitido que ambos tipos de nodos coexistan en la misma red. IEEE 802.3 también gobierna las tecnologías de Fast Ethernet tales como 100 base Tx, 100 base Fx y 100 base Fl.

802.5.- Describe el nivel físico de la red y el subnivel MAC que usen topología de anillo y "Token Passing" para el acceso a la red. La línea de productos de IBM para Token Ring que corre a 4 MBPS puede correr a 16 MBPS usando este estándar.

802.8.- Este es el reporte de un TAG en redes de fibra óptica, el documento discute el uso de la fibra óptica para redes definidas del 802.3 al 802.6 y también provee recomendaciones para la instalación de la fibra óptica.

802.9.- Este es el reporte de un grupo de trabajo refiriéndose a la integración de la voz con los datos (IVD). Este documento especifica la arquitectura e interfaces para los dispositivos que puedan transmitir ambos, voz y datos, por las mismas líneas. El estándar 802.9 fue aceptado en 1993, es compatible con ISDN, utilizando el subnivel LLC especificado en 802.2 y también soporta cable UTP.

802.10.- Este es el reporte de un grupo de trabajo refiriéndose a la seguridad de las redes LAN, incluyendo "Data Exchange" , encriptamiento, administración de las redes y seguridad en las arquitecturas que son compatibles con el modelo de referencia OSI.

International Communications Union (ITU).

La ITU es un cuerpo de estándares internacionales bajo el auspicio de las Naciones Unidas dentro del gobierno y coordinado por el sector privado para el establecimiento de las telecomunicaciones, redes y servicios. La ITU ejecuta la tarea de regulación, estandarización y desarrollo de las telecomunicaciones para armonizar las políticas de las comunicaciones internacionales.

La ITU tiene tres subagencias, las cuales son:

El Consultative Committe for International Telephony and Telegraphy (CCITT) El cual es el responsable de múltiples normas para las comunicaciones y es mucho más activo en cuanto a las comunicaciones de datos en la red.

El Consultative Committe on International Radio (CCIR) encargado de las comunicaciones de radio.

El International Frequency Registration Board (IFRB) el cual asigna bandas de frecuencia para las comunicaciones.

Las Siguientes normas fueron remitidas por la CCITT y adoptadas por la ITU.

V.11.- Características eléctricas de un circuito balanceado para transmitir datos a 10 Mbps. Compatible con RS-422.

V.22.- Funcionamiento de modems asíncronos y síncronos para velocidades de 1200 Bps.

V.22 bis.- Operación de modems asíncronos y síncronos para velocidades de 2400 Bps.

V.24.- Los circuitos de intercambio físico para interconectar equipo de computación. RS 232 D es un subconjunto de V.24 y V.28 que define las propiedades eléctricas del circuito.

V.25 bis.- Procedimientos de auto llamada y auto respuesta implementando un protocolo de comandos conceptualmente similar a los comandos HAYES AT pero específicamente orientados a los circuitos de telefonía Internacional.

V.28.- Las características eléctricas de un intercambio de circuitos desbalanceados, usados en conjunción con los circuitos físicos V.24, definiendo de 5 a 15 volts para un bit "0" y de -5 a -15 para definir un bit "1" .

V.32.- Operación de modems sincronos y asincronos para enlazar o conectar líneas a velocidades de 9600 y 4800 Bps.

V.32ter.- Revisión de la AT&T de la V.32 con velocidades de 19200 bps con la opción de que se incremente esa velocidad.

V.32bis.- Operación de los modems sincronos o asincronos para operar a velocidades de 14.4 Kbps con la opción de negociar ráfagas de datos a velocidades mayores.

V.35.- La interfaz física de circuitos para interconectar equipos y computadoras a velocidades de 48 Kbps (pero es obsoleto por la aparición de la V.36 y la V37. Ahora solo se usa como termino genérico para describir el conector físico y la interfaz eléctrica usada para la transmisión a velocidades de 1544 Kbps.

V.42 Es un estándar de CCITT para un protocolo de corrección de errores para modems que usan conversión de asincrono-a-sincrono definida como LAP-M Protocol.

V.34 .- Operación de modems sincronos o asincronos para el enlace con líneas telefónicas a 28800 bps.

Otras organizaciones de estándares son:

ANSI (American National Standards Institute) .- Instituto Nacional de Estándares Americanos.

El estándar más importante de la ANSI, representando a los EUA ante la ISO es el estándar FDDI.

ATM Forum.

Es un consorcio industrial internacional no lucrativo, el cual constituye una acelerada convergencia de los estándares de la interoperabilidad, basándose en los estándares internacionales y promueve en la industria la cooperación.

Sus estándares importantes son:

ATM LAN Emulation
Especificación de la Frame Based User-to-Network (FUNI).

Y por último la EIA Electrical Industries Association.

Sus estándares importantes son:

La interfax RS-232D.
EIA/TIA-568 (secuencia de cables).

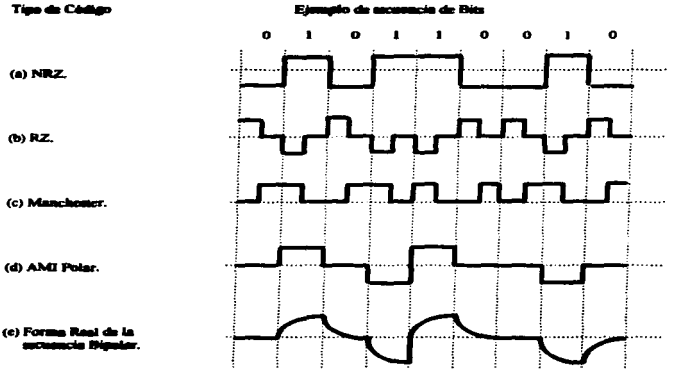
CÓDIGOS DE LÍNEA.

Cuando las distancias entre los ordenadores y terminales son grandes, resulta más económico incorporar la temporización a la propia señal que usar un canal de sincronismo aparte. Esto es lo que se conoce como un código de línea. Los códigos que no emplean esta técnica presentan el inconveniente de que el reloj y los datos pueden verse alterados de forma diferente al propagarse por canales distintos. La señal de sincronismo puede verse adelantada o retardada en relación con la señal de datos, lo cual puede provocar que el receptor tenga dificultad para "engancharse" a esta última.

Un código de línea es aquél que permite al receptor comprobar periódicamente si está muestreando la línea en el momento exacto en que llega un bit de datos. Ello exige (en condiciones ideales) que la línea cambie de estado muy a menudo. Los mejores códigos son aquellos en los cuales el estado de la línea cambia muy frecuentemente, ya que estos cambios de estado (por ejemplo, saltos de tensión) permiten al receptor seguir reajustando su propio funcionamiento de acuerdo con la señal.

Lo único que hace el "reloj" es proporcionar la referencia para los unos y los ceros individuales. La idea consiste en disponer de un código que presente transiciones regulares y frecuentes sobre el canal. Las transiciones se limitarán el tamaño de las divisiones correspondientes a los datos binarios (unos y ceros) en el receptor; la lógica de muestreo buscará constantemente las transiciones de estado para delimitar los bits que vayan llegando.

En la siguiente figura podemos ver varios ejemplos de algunos de los métodos de codificación binaria más empleados en la industria. Examinaremos cada uno de ellos brevemente, indicando sus ventajas e inconvenientes.



CODIGO UNIPOLAR.

La señal no toma nunca valores negativos o nunca valores positivos (es decir, su signo algebraico no cambia: 0 volts para el 1 y 3 volts para el 0, por ejemplo).

CODIGO POLAR.

La señal toma valores positivos y negativos (los signos opuestos identifican los estados lógicos: +3 y -3 voltios).

CODIGO BIPOLAR.

La señal varia entre tres niveles(ej.: +3,0 y -3 voltios).

CODIGO CON INVERSION ALTERNADA DE UNO (AMI).

Representa los unos mediante pulsos cuya polaridad va alternando de uno a la siguiente.

CODIGO NRZ.

En la figura (a) aparece un código sin retorno a cero (NRZ). Como puede verse, el nivel de la señal permanece estable durante todo el intervalo del bit. En este caso, la señal permanece a nivel bajo para representar un 1, y sube a nivel alto para expresar el 0. (Muchos dispositivos emplean tensiones opuestas.) El esquema NRZ es muy empleado en comunicaciones, por su relativa sencillez y su bajo coste. Además, un código NRZ emplea el ancho de banda con gran eficacia, puesto que es posible representar un bit con cada baudio (cambio de la señal). No obstante, carece de la posibilidad de autosincronización, ya que, por ejemplo, en una serie de unos o ceros seguidos no aparecerá transición alguna en el canal, lo cual puede ocasionar que el reloj del receptor se desplace con respecto a la señal entrante, con lo que los datos de la línea no se muestrearán en el instante correcto, y el emisor y el receptor perderán la sincronización mutua. Un código NRZ puede ser polar o bipolar, según la realización de que se trate. El sistema NRZ goza de una amplia difusión de los sistemas de comunicaciones, ya que no exige codificación o decodificación adicionales, y utiliza el ancho de banda del canal de forma muy eficiente.

CODIGO RZ.

Los códigos con retorno a cero (RZ) suelen introducir en la señal un cambio de nivel, al menos, en cada intervalo de bit. Este esquema es el que aparece en la figura (b). Un código RZ presenta una transición en cada intervalo de bit, por lo que posee unas buenas características de sincronización. Su principal desventaja radica en que exige dos transiciones de la señal por cada bit, lo cual significa que un código RZ necesitará un ancho de banda doble que el de los códigos NRZ convencionales. Este tipo de código se emplea en algunos de los más avanzados sistemas asociados con las redes locales, las fibras ópticas y las tecnologías relacionadas con la luz.

CODIGO MANCHESTER.

La figura (c) muestra otro tipo de código muy empleado en los sistemas modernos de comunicaciones: el código Manchester. Este código presenta un cambio de estado en cada intervalo. Es, por tanto, un código dotado de un buen sincronismo. Sin embargo, al igual que el código RZ, exige una velocidad binaria doble que la

velocidad de transmisión de bits. Además, los dispositivos de interfaz que se emplean para conseguir estas velocidades binarias son bastante más caros que la *interfaz* NRZ. El código Manchester se utiliza bastante en grabaciones en cinta magnética, enlaces de fibra óptica, líneas coaxiales y redes Ethernet.

CODIGO AMI BIPOLAR.

La figura (d) nos muestra un código empleado por muchas compañías telefónicas. Se trata del esquema llamado originalmente código PCM de Bell System, su estructura de señalización es un ejemplo de AMI bipolar, en el que se emplean pulsos de polaridad alternada para codificar los unos binarios. Este código en concreto presenta algunos problemas cuando aparece una larga serie de ceros durante una transmisión, esto se debe a que no se pueden sincronizar de ninguna forma los bits cero, ya que el estado de la línea no cambia.

GLOSARIO.

A.

AMI (Alternate Mark Inversion) - Sistema de codificación bipolar en el cual los unos (marcas) sucesivo deben alternar su polaridad (entre positiva y negativa).

Analógico/a (Analog) - Onda de señal continua (como p. ej. la voz humana).

Ancho de banda (Bandwidth)- gama de frecuencias que pasa por un circuito. Cuanto mayor el ancho de banda, más información puede enviarse por el circuito en un lapso determinado.

ACK- Abreviatura de acknowledgment (acuse de recibo). Normalmente se envían ACKs de un dispositivo a otro de la red para indicar que ocurrió algún suceso (por ejemplo la recepción del mensaje).

ANSI - American National Standards Institute: Instituto Nacional de Normasmericano de Estándares. Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos.

Atenuación- Diferencia entre la potencia transmitida y la recibida debido a pérdidas en los equipos, líneas u otros dispositivos de transmisión. Se mide en decibeles.

B.

Baudio (baud)- Unidad de velocidad de señalización equivalente al número de estados o eventos discretos por segundo.

BERT (Tester de Tasa de Error de Bits)- Dispositivo usado para probar la tasa de error de bits de un circuito de comunicaciones .

Broadcast- Difusión o mensaje público. Mensaje enviado a todos los destinos dentro de una red.

Broadcast storm- Disturbios por difusión. Acontecimiento indeseable en una red, en el cual se envían muchas difusiones a la vez, empleando para ello considerable ancho de banda y, normalmente, causando además interrupciones en la red.

Buffer- Dispositivo de almacenamiento. Usado corrientemente para compensar diferencias en la velocidad de transmisión de datos o temporización de eventos cuando se transmite de un dispositivo a otro.

Byte- Grupo de bits que una computadora puede leer (generalmente de longitud 8 bits).

C.

Compresión.- Paso de los datos por un algoritmo que reduce el espacio/ancho de banda requerido para almacenar/transmitir el conjunto de datos.

Convergencia.- Capacidad (y velocidad con la cual se logra) de un grupo de dispositivos de interconexión de redes que ejecutan un protocolo específico de enrutamiento, para coincidir en la determinación de la topología de las interconexiones luego de que está cambió.

Count to infinity-Cuenta hasta el infinito.- Problema que puede ocurrir en algoritmos de enrutamiento de convergencia lenta, donde los enrutadores incrementan secuencialmente la cuenta de trayectos (hop count) hacia algunas redes específicas hasta que (típicamente) se imponga un límite arbitrario.

CSMA/CD- (Carrier sense multiple access/ collision detection- Detección por portadora de acceso multiple/colisión). En este protocolo las estaciones escuchan al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete en transmitido tras un intervalo (time out) aleatorio. El CSMA/CD se usa en Ethernet.

CSU- (Unidad de Servicio de Canal)- Equipo de propiedad del usuario, instalado en la interface a las líneas de la empresa telefónica como terminación de una DDS (Servicio de Datos Digitales) o un circuito T1. Los CSU brindan protección a la red y capacidades diagnósticas.

D.

Decibel (dB)- Unidad que mide la intensidad relativa (razón) de dos señales.

DCE-(Data Communications Equipment) El equipo que brinda las funciones que establecen, mantienen y finalizan una conexión de transmisión de datos.

DSU- (Unidad de Servicio Digital) Dispositivo del usuario conectado a un circuito digital (tal como un T1 cuando está combinado con una CSU). La DSU convierte la corriente de datos del usuario a formato bipolar para su transmisión.

Dijkstra's algorithm. Algoritmo de Dijkstra. Algoritmo de enrutamiento de trayectoria mínima que itera sobre la longitud del camino para determinar el árbol abarcador (spanning tree) de trayectoria mínimas.

DTE (Equipo Terminal de Datos)- Dispositivo que transmite o recibe de un DCE (p. ej., una terminal).

DXI (Data Exchange Interface- Interfaz de Intercambio de Datos)- Protocolos utilizados entre ruteadores y DSUs en SMDS y ATM.

E.

E1- Sistema de portadora digital a 2.048 Mbps usado en Europa.

ECO- Distorsión de señal que ocurre cuando la señal transmitida es reflejada hacia la estación de origen.

Enrutado (Routing)- El proceso de selección de la vía circuital más eficiente para un mensaje.

Explorer Frame-Marco de Exploración. Marco que envía un dispositivo de la red en un entorno de puenteo de rutas fuente para determinar la ruta óptima hacia otro dispositivo de la red.

F.

Fast Switching- Conmutación Rápida.- Utilización de una memoria rápida caché de ruta para acelerar el paso del paquete a través del enrutador.

Flapping (Aleteo). Problema de enrutamiento en el que la ruta anunciada entre dos nodos alterna (aletea) de ida y vuelta entre dos trayectorias, debido a un problema que causa fallas intermitentes en la interfaz.

Flash EPROM- Nueva tecnología de PROM (Programmable Read- Only Memory) desarrollada por Intel y licenciada a otras compañías de semiconductores. Es un medio de almacenamiento no volátil que se puede borrar y reprogramar eléctricamente en el circuito. Se emplea en los enrutadores para lograr la carga inicial y la subsecuente retención de la información de configuración en forma no volátil.

Flash update- Actualización inmediata. Actualización de enrutamiento enviada asincronicamente en respuesta a un cambio en la topología de la red. Las actualizaciones de enrutamiento normales se envían a intervalos fijos.

Full duplex: Capacidad de transmisión simultánea de datos en ambas direcciones.

G.

G.703- Norma CCITT de características físicas y eléctricas de diversas interfaces digitales incluyendo las de 64Kbps y 2.048Mbps.

Group Address Dirección de grupo. Dirección única que se refiere a múltiples dispositivos de la red. Sinónimo de Multicast address.

H.

Half duplex- Circuito o dispositivo que permite la transmisión en ambos sentidos pero no simultáneamente.

Handshake- Secuencia de mensajes que dos o más dispositivos de la red intercambian para asegurar sincronización en la transmisión.

H channel- Canal ISDN primario full duplex que opera a 384 Kbps.

Header- Encabezado. Información de control que se añade a los datos antes de encapsularlos para su transmisión en la red.

Holddowns- Sajetones. Característica de algunos protocolos de enrutamiento en los que se impide que las actualizaciones regulares de rutas equivocadamente reinstalen una ruta que ha fallado.

I.

IAB-Internet Activities Board: Grupo de actividades de Internet. Investigadores de interconexiones entre redes que se reúnen regularmente para discutir asuntos de Internet.

Internet Address Dirección Internet. También llamada "dirección IP", es una dirección de 32 bits asignada a máquinas anfitrionas que emplean TCP/IP. La dirección se escribe como 4 octetos separados con puntos, formados por la sección de la red, una sección opcional de subred y una sección de anfitrión.

Internetwork- Redes interconectadas. Conjunto de redes interconectadas por enrutadores y que en forma genérica funciona como una sola. A veces se llama Internet. Lo cual no debe confundirse con la palabra Internet.

Internetworking- Término que surgió alrededor del problema de conectar redes. El término se puede referir tanto a productos como a procedimientos y tecnologías.

Isochronous transmission Transmisión Isocrónica. Transmisión asincrónica (start-stop) sobre un enlace de datos síncrónico.

J.

Jabber- Balbuceo. Condición de error en la cual un dispositivo de la red continuamente transmite "basura" a la red. En IEEE 802.3 se refiere a un paquete de datos cuya longitud excede a la prescrita en el estándar.

Jerarquía digital Síncrona (SDH, Synchronous Digital Hierarchy)- Norma europea para el uso de medios ópticos para el transporte físico en redes de larga distancia y alta velocidad.

Jitter- Leve desplazamiento de una señal de transmisión en el tiempo o en la fase. Puede introducir errores y pérdida de sincronización en las comunicaciones síncronicas de alta velocidad.

L.

LLC- Logical Link Control: Control lógico de enlace. Subcapa de la capa de enlace OSI definida por la IEEE. Se encarga del control de errores, control de flujo y creación de marcos. El protocolo LLC más usado es IEEE 802.2, que incluye variantes sin y con conexión.

Load Balancing- Balanceo de carga. En enrutamiento se refiere a la capacidad de un enrutador para distribuir el tráfico a todos sus puertos de la red que estén a la misma distancia de la dirección de destino. El balanceo de la carga incrementa la utilización de los segmentos de la red y aumenta el ancho de banda efectivo de la red.

Logical Channel - Canal lógico: Trayectoria de comunicaciones no dedicada, para conmutación de paquetes, entre dos o más nodos de la red . Mediante conmutación de paquetes pueden existir varios canales lógicos simultáneamente en un mismo canal físico.

M.

MAC -Medio Acceso Control: Control de Acceso al Medio. Protocolo que define las condiciones bajo las cuales las estaciones de trabajo acceden al medio de transmisión; su uso está más difundido en lo que hace a las LAN. En las LAN tipo IEEE, la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.

MIB- Base de Manejo de Información. Base de datos de información sobre manejo de objetos, a la que se puede tener acceso mediante protocolos de manejo de red tales como SNMP.

Multicast address Dirección Múltiple. Dirección que se refiere a múltiples dispositivos de la red. Sinónimo de group address (dirección de grupo).

N.

NetBIOS- Network Basic Input/Output System: Sistema básico de entrada/salida de la red. Interfaz de la capa de sesión para redes de PC, producida por IBM y Maicrosoft.

NetWare- Desarrollado y distribuido por Novell, Inc; se trata del sistema de archivos distribuidos más popular en la actualidad. Ofrece acceso transparente a archivos remotos y muchos otros servicios distribuidos de redes.

Network- Red. Conjunto de computadoras y otros dispositivos que son capaces de comunicarse entre sí empleando un medio reticular.

O.

OSI- Open Sistem Interconnection: Interconexión abierta de sistema. Programa internacional de estandarización, apoyado por ISO y CCITT, para desarrollar estándares para redes de datos. Facilita la interoperabilidad de equipos hechos por diversos fabricantes.

OSPF- Open Shortest Path First: La trayectoria abierta más corta primero. Algoritmo de enrutamiento jerárquico IGP de estado de enlace propuesto como sucesor de RIP en la comunidad Internet. A sus características incluyen enrutamiento de costo mínimo, enrutamiento de camino múltiple y balanceo de cargas.

P.

PAD- Packet Assembler/Disassembler: Ensamblador / Desensamblador de paquetes. Dispositivo usado para conectar dispositivos simples (como por ejemplo, terminales que trabajan en modo de caracteres) que no tienen capacidad de ensamblar ni desensamblar paquetes, a redes X.25. El PAD sirve como buffer para datos enviados entre las máquinas anfitrionas y las terminales en una red X.25.

Physical Address- Dirección Física. Término empleado algunas veces para referirse a la dirección de la capa de enlace (link-layer) de un dispositivo de la red.

Piggybacking- Aprovechar el viaje. Transporter acuse de recibo (acknowledgments) con el paquete de datos para ahorrar ancho de banda a la red.

Protocol.- Protocolo. Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en que los dispositivos de una red intercambian información.

Q.

QOS- Quality of Service: Calidad del Servicio. Medida del desempeño de un sistema de transmisión que considera la calidad de la transmisión y la disponibilidad del servicio.

Queue- cola. En forma genérica se refiere a una lista ordenada de elementos que esperan procesamiento. En enrutamiento indica un conjunto pendiente de paquetes que esperan ser enviados a una interfaz del enrutador.

R.

RARP- Reverse Address Resolution Protocol. Protocolo inverso de resolución de direcciones. El inverso lógico de ARP, que ofrece un método de encontrar direcciones IP basado en direcciones del medio.

Reloj maestro.- Master clock. Fuente de las señales de temporización (o las señales mismas) que todas las señales de la red usan para la sincronización.

RFC- Request For Comments. Solicitud de comentarios. Documentos empleados como el medio primario de comunicación de información sobre Internet. Algunos RFC son designados por IAB como Estándares Internet.

RMON- Remote Monitoring. El MIB de monitoreo remoto que permite que un dispositivo de monitoreo de red sea configurado y leído a distancia.

S.

SAP- Service Access Point: Punto de acceso al servicio. Interfaz entre capas OSI adyacentes. También se refiere a Protocolo de anuncio de servicios el cual es un protocolo Novell mediante el cual se hacen conocidos a los clientes recursos de la red tales como servidores.

Segmento de tiempo- Timeslot. Porción de un multiplex serie de información dedicado a un único canal. En T1 y E1 un segmento de tiempo representa típicamente un canal de 64 Kbps.

SNAP- Protocolo de Acceso a Subred. Protocolo Internet que opera entre una entidad de red en la subred y una entidad de red en el sistema final, y especifica un método estándar para encapsular datagramas IP y mensajes ARP en redes IEEE. Efectúa tres funciones claves: Transferencia de datos, manejo de conexiones y selección de QoS.

Source Address-Dirección fuente. Dirección de un dispositivo de la red que hace envíos.

Spanning Tree algorithm- Algoritmo de árbol Abarcador. Algoritmo usado para impedir ciclos de puenteo mediante la creación de un árbol abarcador.

T.

TCP/IP- Protocolo de Control de Transmisión/Internet Protocol. Los dos protocolos de Internet más conocidos, que erróneamente suelen confundirse con uno solo. TCP corresponde a la capa 4 del modelo OSI y ofrece transmisión confiable de datos. IP corresponde a la capa 3 de OSI y ofrece servicios de datagramas sin conexión.

Telnet. Protocolo estándar Internet de emulación de terminales.

Troncal - Trunk. Un único circuito entre dos puntos, cuando ambos son centro de conmutación de puntos de distribución individuales. Generalmente una troncal maneja simultáneamente.

U.

UDP- User Datagram Protocol. Protocolo de datagrama del usuario. Protocolo sin conexión de la capa de transporte que pertenece a la familia de protocolos de Internet.

W.

WAN- red de área amplia . Red que ocupa una área geográfica amplia.

X.

XNS- Xerox Network Systems. Sistemas de red xerox. Grupo de protocolos originalmente diseñados por xerox PARC. Muchas compañías de redes de PC, como Ungermann-bass, Novell, Banyan y 3Com, usaban o actualmente usan variantes de XNS como pila de protocolos primarios de transporte.

Referencias.

1) Douglas, E. Comer.
Internetworking With TCP/IP
Design, implementation and
Internals.

2) Novell Education, Course 205.
Fundamentals of Internetworking.
Design and Management.

3) Tanembaum,
Redes de Ordenadores.
Segunda edición.

4) Martin, P. Clark.
Network and Telecommunications.
Design and Operation.

5) Stallinga, Williams.
Local Networks.
Edi. McMillan Book 3° Edición,
1990.

6) Asesoría de redes de
telecomunicaciones S.A. de C.V.
(ASERCOM).
Apuntes del curso Redes LAN,
WAN, básico y avanzado.

7) Telecomunicación Corporativa S.A.
de C.V. (TELCOR).
Apuntes del curso de Ruteadores y
Compuertas.

8) ENEP Aragón
Apuntes del curso Redes Digitales
LAN / WAN
por el Ing. David Estopier B.

9) Intersys S.A. de C.V.
Apuntes del curso "El Catalyst
5000"

10) http://www.Anixter.com

11) http://www.Cisco.com

12) http://www.ATMforum.com

13) http://www.XYLAN.com

14) http://www.Bellcore.com

15) http://www.Motorola.com