36
2ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

FUNDAMENTOS BASICOS DE CONECTIVIDAD EN INTERNET

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRISISTA

P R E S E N T A

DANIEL RAMON ELORREAGA MADRIGAL

ASESOR: ING. JOSE J. CONTRERAS ESPINOSA
CO-ASESOR: LIC. VALENTIN ROLDAN

CUAUTITLAN IZCALLI, EDO. DE MEX. 1998

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS

DR. JAIME KELLER TORRES
DIRECTOR DE LA FES-CUAUTITLAN
P R E S E N T E .

AT'N: Ing. Rafael Rodríguez Ceballos
Jefe de: Departamento de Exámenes
Profesionales de la F.E.S. - C.

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:
"Fundamentos Básicos de Conectividad en Internet".

que presenta el pasante: Daniel Ramón Elorreaga Madrigal
con número de cuenta: 8840342-5 para obtener el TITULO de:
Ingeniero Mécanico Electricista.

Considerando que dicha tesis reúne los requisitos necesarios para ser discutida en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E .
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Edo. de Méx., a 19 de Enero de 1998

PRESIDENTE	Ing. José Juan Contreras Espinosa	28/01/98
VOCAL	Ing. Antonio Trejo Lugo	28/01/98
SECRETARIO	Ing. Margarita Lopéz Lopéz	2-2-98
PRIMER SUPLENTE	Ing. Juan Gonzalez Vega	28/1/98
SEGUNDO SUPLENTE	Ing. Victor Hugo Landa Orozco	28/I/98

AE/DEP/VAP/01

Esta tesis está dedicada a todos aquellos que un día comenzaron un gran sueño
Con muchos anhelos y esperanzas.
Conscientes de que siempre será mejor
lo uno desea en la vida

25 años me lo han enseñado.

Gracias.

A todos los que creen y confían en mi.

A todos aquellos que de una manera desinteresada
Contribuyeron directa o indirectamente con este trabajo

A quienes hoy no están conmigo para compartir esto
Sin ustedes tal vez no lo hubiese logrado.

A la Universidad Nacional Autónoma de México

Por el gran desempeño dentro de su labor académica
a los profesores de
La Facultad de Estudios Superiores Cuautitlan.

INDICE DE CONTENIDOS.

INDICE DE ILUSTRACIONES.-

INDICE DE TABLAS.-

INTRODUCCIÒN GENERAL

Por espacio de 15 años, ha evolucionado una tecnología que hace posible interconectar físicamente muchas redes de computadoras diferentes y hacerlas funcionar como una unidad coordinada. Esta tecnología llamada *Internetworking*, unifica diferentes tecnologías de *Hardware* subyacentes al proporcionar un conjunto de normas de comunicación y una forma de interconectar redes heterogéneas. La tecnología de red de redes oculta los detalles del *Hardware* de red y permite que las computadoras se comuniquen en forma independiente de sus conexiones físicas de red.

A nuestros días, la comunicación de datos se ha convertido en parte fundamental de la computación, el Internet es una red mundial de 200,000 redes de computadoras hoy utilizadas por más de 60 millones de gentes. Es un medio donde los elementos multimedia entrelazan todos los medios básicos de comunicación — Televisión, periódicos y revistas, radio, cine, y telefonía — innovando cada uno de estos. A través de él, la gente puede transmitir y recibir documentos, imágenes, sonido, vídeo y datos. Todo en igualdad de 0s y 1s de comunicaciones digitales. Las comunicaciones pueden ser tan modestas como 2 vecinos intercambiando mensajes e-mail o una extensa transmisión real-time de un concierto de rock alrededor del mundo.

El Internet forma parte de la tecnología emergente del área de comunicaciones con una trascendencia sin precedentes. Y rápidamente se ha desarrollado desde las redes locales interconstruidas (LANs) a las redes amplias de interconexión global.

A mediados de 1997, se tienen "conectadas" 23 millones de computadoras al Internet. A estas computadoras se les nombra "host" porque, históricamente, muchas aplicaciones eran puestas en grandes computadoras a las que se les nombraba "hosted" de varios servicios. Hoy los "hosts" pueden ser clientes o servidores, o ambos a la vez. Las redes de Internet están interconectadas por computadoras especiales llamadas "routers" donde su trabajo es "rutear" el tráfico de un "host" fuente a un "host" destino pasando a través de un gran número de redes

De esta manera, la presente tesis describe los fundamentos básicos que debemos observar para tener una interconexión de redes bajo un sistema abierto, observando de primera instancia las funciones que presentan las sociedades del *IEEE* y el *CITT* que marcan los estándares más importantes para las comunicaciones electrónicas en el mundo y que permiten la globalización de los medios de comunicación, en este caso la comunicación de computadoras.

El modelo *OSI* presenta las posibilidades infinitas que posee un sistema abierto de comunicaciones de computo a diferencia de los sistemas privados, los cuales sólo permiten la disponibilidad de comunicación por medio de vendedores particulares, las especificaciones aquí mostradas están disponibles públicamente. Por lo tanto cualquier persona puede desarrollar el software y hardware necesario para comunicarce a través de una red de redes.

Algo muy importante es que toda la tecnología diseñada sobre la base de este modelo permite la comunicación entre maquinas que tengan arquitecturas diferentes de hardware,

para utilizar cualquier hardware de red de paquetes conmutados y para incorporar muchos sistemas operativos de computadoras.

Para familiarizar al lector con las redes de comunicación de datos, es importante tener una reseña de las tecnologías subyacentes de red, este es el caso del capitulo de *Redes Locales (LAN)* donde presentamos las arquitecturas más conocidas en el ámbito comercial: *Ethernet,* y *Token Ring,* así como las *Topologías* de extensión más comunes para las comunicaciones en una área geográficamente confinada moderadamente como lo son edificios de oficinas y áreas administrativas de algún corporativo.

Bus Lineal, Anillo (simple y compuesto), y *Estrella* (simple y compuesta) son algunas de las *Topologías* analizadas en este capitulo. Cabe mencionar que se presenta una sección sobre la *Evolución De La Topología* donde se aplican los requerimientos funcionales de los *Protocolos De Acceso Al Medio* (MAC) tales como *Aloha* y *CSMA/CD* que son propiedades de la tecnología de bus en difusión en una red *Ethernet.*

Medios de Transmisión (MT), es un capitulo donde se exponen las diversas propiedades de los elementos físicos que conforman una red local; tal es el caso de los tipos de cable que utilizan: *Coaxial, Par Trenzado, BNC, y FDDI.* Los *Medios De Comunicación* para efectuar enlaces por medio de *Antenas Directas, Satélites,* y *Red Telefónica* (POST). *Modos De Transmisión* que presentan los medios a través del cableado y las *Técnicas De Interconexión* básicas que se efectúan dentro de los *Equipos De Interconexión: Repetidores, Concentradores, Puentes, Ruteadores, y Conmutadores;* cabe mencionar que estos dispositivos interconectan las redes entre sí, lo cual crea el concepto de *Internetworking,* esta sección provee las bases de la tecnología para la cual fueron diseñados en un esquema generalizado de interconexión y así también se manejan sus *Aplicaciones Y Productos* dentro de un mercado cautivo de tecnologías y arquitecturas de redes.

En él capitulo de *Tecnología Y Arquitectura De Un Backbone,* representa la topología esquemática para la migración de una red local a un enlace de redes metropolitanas y consecuentemente su proyección a redes de banda ancha lo que nos permite observar los conceptos básicos de un *Backbone Colapsado* sobre el cual se centralizan todas las comunicaciones con conexiones de *Fibra óptica* para *Redes De Alta Velocidad.* Uno de los puntos más interesantes de este capitulo es el ejemplo del cableado estructurado realizado a principios de 1994 en el edificio Agustín De Betancurt del Campus Laganes de la Universidad Carlos III en Madrid, España. Este ejemplo práctico fue desarrollado por el Centro De Calculo de dicha institución, y lo selecciones debido a que la arquitectura de red y la tecnología que presenta su topología es muy parecida a la mayoría de las redes locales que hoy existen en los campus universitarios de la UNAM y sirve de base para los desarrollos futuros sobre la migración de redes locales a redes metropolitanas y su enlace a los servicios digitales que presentan las redes publicas en México (Telmex, At&T, Avantel-MCI, etc.) e incorporarse a los enlaces directos del backbone de Internet. De esto hablaremos en el apéndice C – *Enlaces Digitales en México.* –

Una vez conocidas las bases de las redes de comunicación locales, antes de adentramos a la migración de redes familiarizaremos al lector con él capitulo de *Arquitectura De Redes De Alta Velocidad* para definir las características que prestan las arquitecturas basadas en el

Ethernet para redes conmutadas, ganando confiabilidad y velocidad de respuesta en las transmisiones de datos en manera local. Y manejar el novedoso concepto que presenta la tecnología *100 VG-Anylan* como parte de las IVD LANs que integran los servicios voz y datos a para interconectarse a redes metropolitanas (MAN) o a redes de banda ancha (WAN) prestando así el soporte de servicios en voz, datos, facsímiles, y otros tipos de información digital codificada.

En él capitulo de *Migración De Arquitecturas* se resumen las posibilidades de ampliar la red local, mejorando la gestión de administración y tráfico de datos e incrementando las dimensiones geográficas y los múltiples servicios que estas puedan presentar; aquí presentamos las migraciones de las redes *Ethernet* con 10Mbps base a redes de alta velocidad. En primer lugar trabajamos la conmutación de datos en *Switches Ethernet* con conexiones de FDDI, lo cual presta ganancias de velocidad en la transmisión de datos a bajo costo pasando por las configuraciones de bus y anillo analizando sus costos, ventajas y desventajas como se viene haciendo y terminamos con la conexión a 155Mbps de una red ATM Local de grandes prestaciones y costos.

A estas alturas nuestro trabajo esta cubriendo las infinitas posibilidades de comunicación entre computadoras para efectuar el *Internetworking* pero faltan las bases que describen el manejo de estas en el ámbito de datos; para tal efecto se presenta él capitulo de *Redes De Banda Ancha* donde abarcamos la codificación de datos, la manera de transpórtalos, la verificación y corrección de errores dentro de los *Protocolos De Retransmisión* y *Protocolos de Ventana Deslizante.*

Una vez revisado lo anterior entramos a manejar el concepto de redes virtuales, lo cual representa la existencia de interconexión en el ámbito lógico de datos y no en el ámbito físico determinando para esto el uso de dispositivos de interconexión especiales para efectuar el enlace mediante *Brinding* y el ruteo por Routing o ambos a la vez en redes metropolitanas y publicas de banda ancha; analizando sus prestaciones, ventajas y desventajas, así como las aplicaciones y productos disponibles en los mercados para su interconexión.

Protocolos Ruteables Y No Ruteables capitulan el conocimiento general de múltiples maneras de interconectar redes de una manera fiable y consistente en el ámbito lógico; una vez determinada la arquitectura existente y el tipo de enlace físico que predomine en sus instalaciones. Permitiendo reafirmar los conocimientos obtenidos hasta el momento sobre el modelo *OSI* en interconexión de redes en el ámbito de datos.

Y al fin se llega al capitulo pináculo de esta tesis: *Protocolos TCP/IP* este resume bajo una estructura objetiva, la descripción de la tecnología *TCP* e *IP* como parte del estudio realizado para el *Internetworking* por la Agencia De Proyectos Avanzados De Investigación (ARPA) de la defensa de los Estados Unidos De Norteamérica.

La cual habla de un conjunto de estándares de red que especifican los detalles de como se comunican las computadoras, así como un grupo de reglas para interconectar redes y para rutear el tráfico en forma general. En primer termino analizamos el *Ruteo En Ambiente IP* y sus *Protocolos De Ruteo Interno*: RIP, IGPR, OSPF, e Integración IS-IS; *Protocolos De*

Ruteo Exterior: *EGP, y BGP*. Que surgen ante la necesidad de un sistema de comunicación interoperable para el ruteo de enlaces entre redes.

En la sección de *Mecanismos De Operación TCP/IP* comparamos el modelo *OSI* con *El Modelo De Referencia De Internet* analizando las capas de *Acceso*, de *Internetworking*, de *Transporte* y *Aplicación*; cotejando su trabajo por medio de los protocolos *IP, ICMP, UDP,* y *TCP;* pasando por la revisión de las *Operaciones IP*: *Mascaras De Red, Búsqueda De Direcciones IP, Operación De Tablas De Ruteo Y Servidores*; terminando por analizar su desempeño en las partes criticas de la operación de redes: *Ancho De Banda, Usos De Memoria, y Procesos de CPU.*

Todo lo anteriormente visto, no cumpliría su propósito si faltase él capitulo dedicado exclusivamente a la *Administración De Redes* donde se exponen los conceptos de costos, configuración, seguridad, rendimiento y fallas; a las cuales esta expuesta una red de computadoras no importando el área que abarque, siempre será indispensable manejar administración por medio de computadoras remotas o de escritorio ayudados por la creación e implementación de los protocolos de administración que poseen los componentes de interconexión de redes; analizando los más importantes hoy en día.

Y finalizamos este trabajo es el de *Firewalls Y Seguridad En Internet.* Si bien una red incorporada al Internet proporciona servicios a nivel aplicación y en el ámbito de red, el crear nuevas herramientas de trabajo y grupos trabajo con computadoras en dominios públicos y privados, surge la necesidad de desarrollar diversas tecnologías para resguardar en forma segura las fuentes de información corporativas y publicas, con lo cual se asegura que siempre existan comunicaciones fiables e información real dispuesta en una serie de servicios a los usuarios.

Al final de la tesis encontraremos la *Conclusión* y adicionalmente se presentan tres apéndices, el primero es el *Apéndice A,* es un proyecto de conectividad, el segundo es el *Apéndice B* que presenta ejemplos prácticos para la creación de Firewalls, el tercero es el *Apéndice C*, que trata sobre conexiones en Internet y enlaces digitales disponibles en México. Y finalizamos con el *Apéndice D* que comprende un Glosario de abreviaturas y términos de enlace de redes.

OBJETIVOS

OBJETIVO GENERAL:

- Conocer los diversos aspectos sobre las tecnologías que permiten la creación de redes de telecomunicación para equipos de cómputo en Internet.

OBJETIVOS PARTICULARES:

- Definir el desarrollo de un proyecto de conectividad basados en el uso de redes locales para computadoras de arquitectura Ethernet y la familia IEEE802.
- Conocer las prestaciones, aplicaciones y productos de las tecnologías de alta velocidad para la migración de arquitecturas de red.
- Conocer los diversos protocolos de comunicación de computadoras para compartir recursos a través de la red global del Internet.
- Dominar los conceptos del TCP/IP para lograr la conectividad de redes locales, metropolitanas, y de banda amplia al Internet.
- Configurar, administrar y optimizar las conexiones de red basadas en la suite del protocolo IP.

1. Estándares y el Modelo OSI

1.1. Estándares

Existen dos organizaciones internacionales de estándares para redes:

El Comité Consultivo Internacional de Telégrafos y Teléfonos (CCITT) y la Organización de Estándares Internacionales (OSI).

En México y algunas partes del mundo se utilizan dos estándares americanos de red, éstos son:

El Instituto Nacional Americano de Estándares (ANSI) y el Instituto de Ingeniería Eléctrica y Electrónica (IEEE); ambos de sus siglas en inglés.

El trabajo de ambas organizaciones ha sido a marchas forzadas, debido a la rápida expansión en el uso de las redes locales, a tal efecto que las dos poseen una serie de estándares desarrollados en redes.

En el ámbito internacional éstas desempeñan el papel de Comité Consultivo para el CITT y el ISO, desarrollando ambos, numerosos estándares para facilitar la operación de redes locales y de banda ancha.

El ANSI y el IEEE trabajan en conjunto con el ISO para estandarizar las tecnologías de redes locales.

Ejemplo:

El ISO delega la estandarización de las tecnologías LAN al ANSI. El ANSI, en turno, delega los estándares de baja velocidad en LAN - inicialmente definida para una operación en rango por y debajo de 50 Mbps - para el IEEE. Resultado del desarrollo estándar para 100-Mbps del ANSI en Interfaces de Datos Distribuidos por Fibra (FDDI); debido a que el IEEE desarrolló el estándar para *Ethernet*, *Token-Ring*, y otras redes de área local. Desde que el IEEE desarrolló el estándar para *Ethernet* de 10-Mbps, esta organización es responsable de las modificaciones a la tecnología de redes de área local. Como resultado de esto la IEEE será responsable para la estandarización del *Ethernet* de Alta Velocidad[1] a incluir isoENET, 100BASE-T, y 100VG-AnyLAN, que más tarde las dos representarán la operación del rango a 100Mbps. En redes locales como sé vera más adelante.

Una vez que el IEEE desarrolla y aprueba el estándar, éste es enviado al ANSI para ser revisado. Si el ANSI aprueba el estándar, se envía al ISO. Entonces el ISO solicita a los países miembros, que analicen que tan seguro es el estándar para trabajar en el ámbito internacional, resultado del desarrollo estándar del IEEE o ANSI para un estándar ISO

[1] Ver. Arquitectura de redes de alta velocidad, Cap 5; Pag. 71

1.1.1. ANSI (American National Standard Institute).

El instituto se localiza en Nueva York, el cual es una organización no-lucrativa y no-gubernamental fundada en 1918, y es el representante de los Estados Unidos de Norteamérica ante el ISO.

Los estándares del ANSI son desarrollados a través del trabajo de 300 comités, y de la asociación de la industria electrónica (EIA). Reconocida por la importancia de la industria en cómputo. El ANSI estableció el comité estándar del X3 en 1960, consistiendo en 25 comités, cada uno asignado a desarrollar una área técnica. Uno de estos comités es el X3S3, más formalmente conocido como el Comité Técnico de Datos y Comunicaciones (DCTC)[2]. Este comité es responsable del ANSI X3T9.5 que gobierna las operaciones *FDDI*, y esta reconocido como el estándar ISO9314.

1.1.2. IEEE (Institute of Electrical and Electronic Engineers).

El instituto está formado fundamentalmente por la sociedad de ingenieros americanos, siendo la más activa en el desarrollo de los estándares en comunicación de datos; por lo cual es una organización prominente en el desarrollo de los estándares de redes locales, comenzando en 1980 por el subcomité 802 después que ellos establecieran un mercado viable para la tecnología LAN.

El proyecto IEEE 802 se esfuerza por concentrarse entre la interfaz física de las partes de red y los procesos de funcionamiento requeridos para establecer, mantener, y actualizar las conexiones de ésta.

Los procedimientos de este proyecto incluyen la definición para los formatos de datos, procedimientos para el control de errores y el control de otras actividades derivadas por el flujo de información, representádolo bajo los niveles del modelo ISO, que son la capa física y de enlace

1.1.3. CITT (Consultive Committe for International Telephone and Telegraph).

La CITT como es conocida por todo el mundo es la responsable directa del desarrollo de estándares en comunicación de datos en conjunto con la Unión Internacional de Comunicaciones que tiene sus instalaciones en Ginebra, Suiza. Y ésta formada por 15 grupos, cada uno responsable de una área específica.

El CITT fue renombrado ITU en 1994. Sus últimas sesiones plenarias fueron, sobre la ley de uso y venta de servicios de carriers (compañías de telecomunicaciones) norteamericanos en Europa Occidental (1992), y las recomendaciones del CITT V-series, el cual describe la operación de diferentes

[2] Data Communications Technical Committee; de sus siglas en inglés.

características en *módems* - por ejemplo, compresión de datos, transmisión, detección y corrección de errores ISO (International Standard Organization) -.

Es una organización no-gubernamental, la cual posee el rango consultivo conjunta con el concilio de la ONU para la economía y sociedad. La participación del ISO es promover el desarrollo para la creación de los estándares mundiales con vista a facilitar el intercambio de bienes y servicios.

La más notable actividad del ISO en el campo de comunicaciones es el desarrollo de las siete capas de los Sistemas Abiertos de Interconexión (OSI), por sus siglas en inglés.

1.2. Modelo OSI

En 1977 la ISO (Organización Internacional para la Estandarización), organismo formado por representantes de la industria, creó un comité para desarrollar estándares para la comunicación de datos y con esto lograr la interoperabilidad entre sistemas heterogéneos. El resultado de este esfuerzo fue un modelo de referencia conocido como el Modelo de Referencia OSI o el modelo de referencia para la interconexión de sistemas abiertos.

El modelo OSI sirve como una guía o serie de lineamientos para las tareas de comunicación, más no especifica un estándar de comunicación, sin embargo, muchos estándares y protocolos cumplen con lo que establece el modelo.

Las comunicaciones están divididas de acuerdo al modelo OSI en siete partes o capas, cada una de las capas destinada a una tarea específica.

7	APLICACIÓN
6	PRESENTACIÓN
5	SESIÓN
4	TRANSPORTE
3	RED
2	ENLACE DE DATOS
1	FISICA

Tabla 1-1Modelo OSI.

Las capas del modelo OSI se pueden agrupar en categorías de acuerdo a su funcionalidad:

Conexiones Físicas (capas 1 y 2): Estas capas proveen la conexión física a la red y son responsables de mover la información sobre el medio de transmisión.

Comunicaciones (capas 3 y 4): Estas capas son responsables de que la información sea transportada de manera confiable desde el dispositivo transmisor hasta el receptor, independientemente del medio físico.

Servicios (capas 5, 6 y 7): Estas capas tienen como responsabilidad ofrecer servicios de red al usuario, por ejemplo servicios de impresión, emulación de terminal, validación de acceso, traducciones de formato, entre otros.

Cada capa ofrece o solicita servicios de las capas adyacentes. La capa 3, por ejemplo utiliza servicios de la capa 2 y ofrece servicios a la capa 4.

Cada capa se comunica con su igual en el dispositivo receptor; es decir, la capa 4 de la computadora A sólo se puede comunicar con la capa 4 del dispositivo B.

Este proceso es probablemente similar al envío de mensajes en la edad media; los reyes usaban uno o más mensajeros para comunicarse con otros reyes, la comunicación final era entre reyes, pero antes de que el mensaje llegara al rey, ya había habido comunicación entre mensajeros o emisarios al mismo nivel.

Cada capa agrega al mensaje original cierta información de control conocida como "**encabezado o header**". En el equipo receptor, cada capa va quitando el Header para que el usuario reciba el mensaje original[3].

Dependiendo de la capa de OSI de la que estemos hablando es como referirnos a la unidad de información, aunque esta nomenclatura no es un estándar:

CAPA	UNIDAD DE INFORMACIÓN	ANALOGÍA
7. Aplicación	Mensaje	Conversación
6. Presentación	Mensaje	Dialogo
5. Sesión	Mensaje	Párrafo
4. Transporte	Datagrama	Oración
3.Red	Paquete	Frase
2. Enlace de datos	Frames	Palabras
1. Física	*Bits*	Letras

Tabla 1-2 Modelo OSI, unidades de información y analogía.

El modelo OSI no es tangible, sólo especifica que tareas deben llevarse a cabo en cada capa, mas no se dice cómo se deben realizar. El modelo OSI hay que verlo como un marco de referencia sobre la base de la cual se desarrollan los protocolos que posteriormente implementan los fabricantes.

En las siguientes secciones se revisa la función de cada una de las capas del modelo OSI.

1.2.1. Capa 1; Física

La capa física se ocupa de la transmisión de *bits* a lo largo de un canal de comunicación y describe las especificaciones físicas del medio, como son: el tipo de cable, las propiedades eléctricas y funcionales de las señales de transmisión y recepción, entre otras. Esta capa es la responsable de transmitir y recibir *bits* a través del medio de transmisión.

[3] Ver. Conmutación de paquetes, Cap. 6.1.2; Pag. 92

1.2.2. Capa 2; de enlace de datos

La capa de enlace de datos es responsable de organizar los *bits* que llegan de la capa 1 en frames. Esta capa agrega cierta información de control al mensaje original, tal como la dirección física (MAC address o dirección de *hardware*) del emisor al destinatario, longitud del frame y un indicador del protocolo superior involucrado. Controla además el acceso al medio.

Esta capa se subdivide en dos subcapas:

LLC (Logical Link Control; control de enlace lógico) que ofrece 2 tipos de servicios: Servicios orientados a conexión (Connection Oriented) y Servicios no orientados a conexión (Connectionless).

MAC (Media Access Control; Control de acceso al medio) que controla el acceso al medio, maneja las direcciones físicas o de MAC, forma los frames.

1.2.3. Capa 3; de red

El objetivo principal de la capa de red es el de mover información a través de varias redes interconectadas entre sí, o sea una red de redes. Esta capa se encarga de colocar el paquete en la red destino, basándose en direcciones lógicas o direcciones de red.

Es como una agencia de viajes: la agencia hace todos los trámites necesarios para que yo llegue a Hawai, pero una vez ahí, alguien más me tendrá que llevar a la dirección exacta. Al igual que la agencia de viajes, la capa 3 no se preocupa de verificar si la información llegó o no llegó, sólo la envía.

A esta capa también se le conoce como capa de ruteo, pues sus funciones principales son la de ruteo y conmutación de la información; es en esta capa donde residen los protocolos como IP e IPX, quienes se encargan de encontrar el camino óptimo para que el mensaje viaje de la red origen a la red destino.

1.2.4. Capa 4; de transporte

La capa de transporte funciona a la mitad del modelo OSI. Esta capa asegura una entrega confiable de información entre el emisor y el receptor. La palabra "Confiable" no quiere decir que la información siempre va a ser entregada, si se rompe el cable de la red, la información nunca llegará a su destino. Sin embargo, la capa 4 sabe que la información no llegó y avisa a las capas superiores para que retransmitan el mensaje e implementen un mecanismo comparable con el correo certificado.

Para ser confiable, esta capa implementa varios mecanismos como el manejo de confirmaciones o acuse de recibo por cada datagrama que se envía llevando una secuencia de cada datagrama entregado, establece circuitos virtuales, etc.

Ejemplo de protocolos[4] de capa 4 son TCP y SPX.

1.2.5. Capa 5; de sesión

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. Una sesión podría permitir al usuario acceder a un sistema de cómputo distante o transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sección consiste en administrar y controlar el diálogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo o bien, en una sola dirección en un instante dado. Si el tráfico sólo puede ir en una dirección en un momento dado, la capa de sesión ayudará en el seguimiento de quién tiene el turno.

La capa de sesión negocia el establecimiento de conexiones, autentifica el acceso (validación del "login"), coordina y sincroniza el diálogo y provee la administración de la sesión.

1.2.6. Capa 6; de presentación

La capa de presentación realiza las funciones de un traductor. A diferencia de las capas inferiores que únicamente están interesadas en el movimiento fiable de *bits* de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

Un ejemplo típico de las funciones de esta capa es la traducción entre formatos diferentes de archivos (ASCII - EBCDIC). El trabajo de manejar estas estructuras de datos abstractas y la conversión de la representación utilizada en el interior de la computadora a la representación normal de la red, se lleva a cabo a través de la capa de presentación. Otros ejemplos de funciones de la capa de presentación son la compresión de datos y el encriptamiento.

1.2.7. Capa 7; de aplicación

En esta capa NO residen las aplicaciones con las que trabaja el usuario. Aquí residen los protocolos necesarios para ofrecer los servicios de red, un ejemplo es el correo electrónico. En la capa 7 reside un protocolo para correo electrónico con la función de que un mensaje de correo llegue del emisor al destinatario, pero no es lo que ve el usuario. El usuario utiliza una interface para crear el mensaje y para enviarlo. Distintas interfaces de usuario (de varios fabricantes) pueden utilizar el mismo protocolo de mensajería.

1.2.8. Modelo, protocolo e implementación

A menudo existe confusión en la industria de las comunicaciones de redes sobre las diferencias entre el modelo OSI, protocolos de red y la implementación de un protocolo.

[4] Ver. Protocolos ruteables, Cap. 8 1; Pag. 105.

Al empezar a trabajar en la selección y diseño de dispositivos, servicios y productos de administración de LAN/WAN resulta de mucha ayuda el entender cómo difieren los conceptos antes mencionados.

Un modelo representa conceptos generales y guías de como se debe mover la información de un lugar a otro. Describe ciertos servicios qué deben ser proporcionados y que capa es responsable de hacerlo.

Un protocolo es un conjunto de reglas concernientes al *hardware*, procedimientos y estructuras de datos. Es el "**plano**" que siguen los desarrolladores para crear productos de *hardware* y *software* que sean capaces de mover información a través de una red o proveer servicios de red. Típicamente un protocolo trata con sólo una capa del modelo.

Una implementación es la forma en que un fabricante crea un producto basado en un protocolo. Por último, cabe mencionar que una arquitectura específica en forma exacta, los servicios y protocolos que se utilizarán en cada una de las capas de un modelo.

2. Redes locales (LAN)

Al instalar una red de computadoras surgen una serie de preguntas pero la cuestión más importante es: ¿Dónde se coloca una estación en relación con el resto de la red?. ¿Al final de una rama que está conectada al cable?. ¿En el punto de unión de dos o más cables?. ¿Al final del cable? O ¿en todos los anteriores?.

Hay tres formas posibles de conexión:

- Punto por punto, en la que sólo se unen dos estaciones adyacentes, sin pasar a través de una estación intermedia.
- Multipunto, en la que dos o más estaciones comparten un sólo cable.
- Lógica, en la cual las estaciones se pueden comunicar entre sí, haya o no-conexión física directa entre ellas.

Así las estaciones de una red local se comunican entre sí mediante una conexión física (punto a punto o multipunto) o lógica.

2.1. Arquitecturas

2.1.1. IEEE 802.3: *Ethernet*

Es un algoritmo CSMA/CD 1 - persistente, con una tasa de 10 Mbps (ahora está de moda una nueva versión a 100 Mbps: Fast *Ethernet*).

Para poder escribir bytes en el cable, debemos codificarlos y darles trama (encapsularlos). El tramado (framing) es típicamente tarea del MAC. En *Ethernet*, el paquete puede verse en la Ilustración 2-1:

Ilustración 2-1 Paquete *Ethernet*

El Preámbulo (Preamble) sirve para sincronizar los relojes del emisor y receptor. Luego viene un comienzo de paquete (Start) y las direcciones de origen (Source) - destino (Destination). Las direcciones *Ethernet* son de 48 *bits*, y son asignadas por convenio entre los fabricantes para evitar dos iguales en la misma red local. Se usan direcciones de grupos (multicasts) y la dirección con todos los *bits* en 1, que es para todos (broadcast). Los paquetes son de tamaño variable, con máximo 1500 bytes (Data).

El campo de PAD, sirve para los paquetes de datos menores de 46 bytes, que son rellenados para dar un largo total al menos de 64 bytes, para evitar que pueda ser transmitido antes de llegar al final del cable. Al final, se agrega una verificación de suma (checksum), que permite validar que todos los *bits* del paquete llegaron sin alteración (CC).

Si se produce una colisión, el emisor espera un tiempo aleatorio antes de reintentar. El tiempo se divide en espacios (slots) de 512 *bits*. Con probabilidad 1/2 se transmite en el slot 0 ó 1. Si vuelve a ocurrir una colisión, con probabilidad ¼ se transmite en el slot 0, 1, 2 o 3. A la tercera, se espera un número aleatorio de slots entre 0 y 2^3 -1. Luego, al ocurrir la colisión i, se sigue esperando entre 0 y 2^i - 1. Después de 10 colisiones, se espera entre 0 y 1023 slots. Después de 16 colisiones se aborta la transmisión.

Este algoritmo se conoce como *binary exponential backoff*, y es muy interesante porque intenta evitar sobrecargar la red con retransmisiones una vez que ésta se encuentra saturada.

Ethernet muestra en la práctica un factor de utilización cercano al 50%. En teoría el mejor caso es alrededor del 80%.

2.1.2. Token Ring

El problema con *Ethernet* es que la distribución del acceso al medio es aleatoria, por lo que puede ser injusta, perjudicando a la computadora durante un periodo de tiempo.

En algunos casos es muy importante garantizar un acceso igualitario al medio, de manera que podamos asegurar que siempre podremos transmitir, independientemente de la carga. El clásico esquema utilizado para esto es el paso de una ficha (Token) entre los participantes. Quien posee la ficha, puede transmitir. Quien quiere transmitir, debe esperar a recibir la ficha.

Por razones de justicia en el acceso, típicamente estas redes se organizan en anillo, de modo de que el *Token* pueda circular en forma natural.

Un ejemplo bastante difundido de estas redes es FDDI (Fiber Distributed Data Interface) que utiliza fibra óptica (aunque también existe sobre cobre) en un doble anillo a 100 Mbps (4 fibras múltimodo).

El MAC *layer* usa direcciones *Ethernet* y permite el broadcast (un paquete que da la vuelta completa al anillo).

Al emitir un paquete, se espera a recibirlo por el otro lado para descartarlo. Al terminar de emitir un paquete, se escribe el *Token* en la red para señalar que está disponible. El *Token* es un paquete físico especial, que no debe confundirse con un paquete de datos. Ninguna estación puede retener el *Token* por más de un tiempo dado (10 ms).

Al estar la red bajo carga, siempre habrán paquetes encolados en las computadoras esperando ser enviados. El protocolo es tomar el *Token*, transmitir un paquete y escribir el *Token*, permitiendo un acceso igualitario a la red, y un uso del ancho de banda de casi un 100%.

Para mantener el anillo funcional, el MAC *layer* es bastante complejo. En todo momento existe una computadora que ha sido elegida como monitor de la red. Ésta se encarga de revisar si el anillo está funcional, si existe un *Token* en él, la existencia de direcciones duplicadas, etc. En *FDDI*, es incluso capaz de recuperarse de fallas en segmentos del anillo, utilizando el anillo secundario (Ver, Ilustración 2-2).

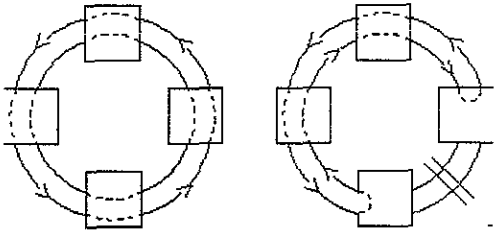


Ilustración 2-2 Reconfiguración del Anillo *FDDI*

2.2. Topologías

La Topología de una Red es la forma física que adopta la misma, junto con el modo de transmisión y la codificación eléctrica de las señales que emplea (Arquitectura).

Cuando se diseña una red, para un entorno de trabajo determinado, la topología que se utilice nos va a definir multitud de parámetros que deben ser tomados en cuenta en otras fases del diseño.

La Topología está en función del:

- Entorno físico en el que nos vamos a mover
- Tráfico que va a soportar nuestra red
- Tipo de servicios que se pretenden ofrecer
- Tipo de protocolos que van a correr
- Tipo de conectividad que queremos tener.

La topología elegida va a influir de forma considerable en las labores posteriores de administración y gestión de la red, como:

- Maniobra rápida de cambio de usuarios (el menor tiempo posible)
- Detección y solución de fallas en cualquiera de los diferentes niveles lógicos que forman la torre de protocolos.
- Crecimiento de la red manteniendo el entorno existente (la buena interconexión de los segmentos que componen la red), etc.

2.2.1. Topología externa (nivel físico).

Es la forma física que adoptan (topología en estrella, en bus, en anillo,...) los medios de transmisión empleados (el cableado), los equipos de interconexión y los equipos interconectados.

Se denomina topología a la forma de conectar los nodos de una red, es decir, la forma que adopta el flujo de información. Dicho de otro modo, la topología es la figura geométrica que forman los nodos y las conexiones que las unen.

Puede ser de tres tipos:

En bus o en árbol.-

Todas las estaciones (también llamadas nodos) comparten un mismo canal de comunicaciones. Las estaciones utilizan este canal para comunicarse con el resto.

En anillo.-

Las estaciones se conectan formando un anillo. Ningún nodo controla totalmente el acceso a la red.

En Estrella.-

Todas las estaciones están conectadas por separado a un centro de comunicaciones o nodo central, pero no están conectadas entre sí.

Hay aún otra topología, la topología en malla, muy común en las redes de larga distancia y en las redes de grandes servidores, pero ésta no se usa en las redes locales de microcomputadoras.

Las redes en bus son multipunto, es decir, las estaciones están conectadas a un único canal de comunicaciones por medio de líneas secundarias individuales. Las redes en anillo y en estrella usan una topología punto a punto; cada segmento físico de cable conecta únicamente dos estaciones, sin pasar a través de ninguna otra estación intermedia. Las combinaciones de estas topologías no sólo son posibles, sino que se están haciendo cada vez más populares.

2.2.2. Factores de evaluación de la topología

La topología tiene una gran importancia en el diseño de una red local, puesto que afecta al rendimiento de la misma. A continuación, después de la definición de cada una de las topologías, se incluye una lista de factores que son de gran ayuda para seleccionar la topología más adecuada a las necesidades particulares.

Los factores que se han de tener en cuenta son los siguientes:

- Aplicación. El tipo de instalación en el que es más apropiada la topología.
- Complejidad: La complejidad técnica de la topología. Este factor afecta a la instalación y mantenimiento de todo el cableado.
- Respuesta: El tráfico que puede soportar un sistema.
- Vulnerabilidad: Lo susceptible que es la topología a fallos o averías.
- Expansión: La posibilidad de ampliar la red cuando sea preciso, así como la facilidad que hay para añadir los dispositivos necesarios para cubrir distancias más grandes.

La importancia de los últimos factores es relativa cuando se selecciona una determinada red local, ya que resultan afectados por las necesidades de los usuarios.

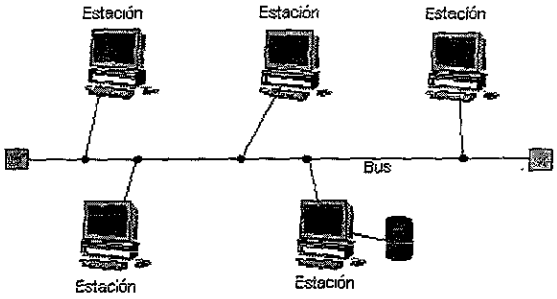
2.2.3. Control de la red

El control de la red también afecta a la topología. El control y la topología están tan relacionados que a veces se define a la topología como el medio de implementar el protocolo de control.

El control puede estar centralizado, en cuyo caso el acceso a la red y la asignación de canal los determina un nodo. La "inteligencia" también puede estar concentrada en el nodo central, quedando las estaciones como terminales no inteligentes.

O puede estar distribuido, en cuyo caso las estaciones pueden acceder independientemente a los canales de la red, dependiendo esto siempre de un conjunto compartido de protocolos. En este caso, la "inteligencia" de la red está distribuida por todas las estaciones conectadas.

2.3. *Bus lineal*



Si falla una estación, las comunicaciones continúan

Ilustración 2-3 Red en Bus de Datos.

En una configuración en bus, todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades de interfaz y derivadores. Los mensajes se envían por todo el canal de distribución. Para que una estación pueda recibir un mensaje, ésta ha de reconocer su propia dirección. Por tanto, los dispositivos conectados a un bus han de disponer de un alto nivel de inteligencia o, de no ser así, la ha de proporcionar la unidad de interfaz.

Puesto que las estaciones más cercanas a la estación emisora reciben una señal más fuerte que las que se encuentran en el extremo más alejado del bus, los transmisores y los receptores utilizados por la red han de tolerar una amplia gama de señales. Los problemas relacionados con la intensidad de las señales se solucionan normalmente limitando la longitud de los segmentos de cable y el número de las estaciones conectadas. En algunas redes se pueden utilizar amplificadores (o repetidores) para mantener la intensidad de la señal. Los conectores y derivadores utilizados no han de reducir demasiado las señales.

Técnicamente, un árbol es una red que cuenta con un cable principal al que hay conectadas redes individuales en bus.

Esta topología se utiliza para conectar redes individuales en bus. Esta topología se utiliza para conectar las estaciones de un edificio de varios pisos. Consiste en un cable principal que conecta los buces (a los que hay conectados estaciones) de cada piso del edificio.

La red está dividida en segmentos diferentes. En esta topología de red se usa normalmente cable coaxial de banda ancha En una red en bus normal se suele usar cable coaxial de banda base.

2.3.1. Factores de evaluación de la topología en bus lineal

⇒ Aplicación: Las redes en bus se usan normalmente en redes muy pequeñas o que tienen muy poco tráfico.

⇒ Complejidad: Las redes en bus suelen ser relativamente sencillas.

⇒ Respuesta: La respuesta es excelente cuando hay poco tráfico, pero a medida que aumenta la carga, la respuesta disminuye rápidamente.

⇒ Vulnerabilidad: El fallo de una estación no afecta normalmente a la red. Las redes en bus son vulnerables a los fallos del canal principal y a otros problemas que afectan al bus. Cuando se producen problemas, éstos son muy difíciles de localizar; sin embargo, una vez localizados son bastante fáciles de reparar

⇒ Expansión: La expansión y reconfiguración de una red en bus son muy sencillas. Cualquier dispositivo que se desee instalar o cambiar de lugar se puede conectar en el punto más adecuado sin tener que cambiar nada en el resto de la red, aunque resulta difícil conectar microordenadores y dispositivos de fabricantes diferentes, puesto que todos los dispositivos conectados han de poder aceptar los mismos tipos de dirección y de datos.

2.3.2. Ventajas e inconvenientes

Ventajas:

◊ El medio de transmisión es totalmente pasivo.

◊ Es sencillo conectar nuevos dispositivos.

◊ Se puede utilizar toda la capacidad de transmisión disponible.

◊ Es fácil de instalar.

◊ Es particularmente adecuada para tráfico muy alto.

Inconvenientes:

◊ La red en sí es fácil de intervenir con el equipo adecuado, sin perturbar el funcionamiento normal de la misma.

◊ La interfaz con el medio de transmisión ha de hacerse por medio de dispositivos inteligentes.

◊ Los dispositivos no inteligentes requieren unidades de interfaz muy sofisticadas a veces, los mensajes interfieren entre sí.

◊ El sistema no reparte equitativamente los recursos.

◊ La longitud del medio de transmisión no sobrepasa generalmente los 200 metros.

2.4. *Anillo*

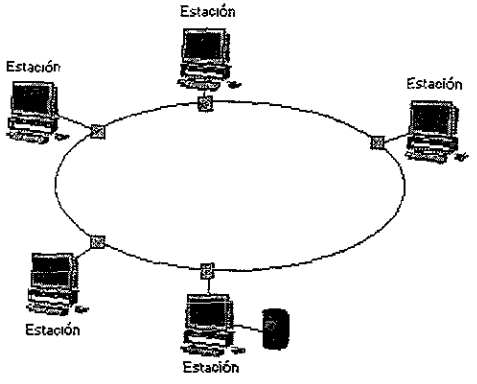


Ilustración 2-4 Red en Configuración de Anillo.

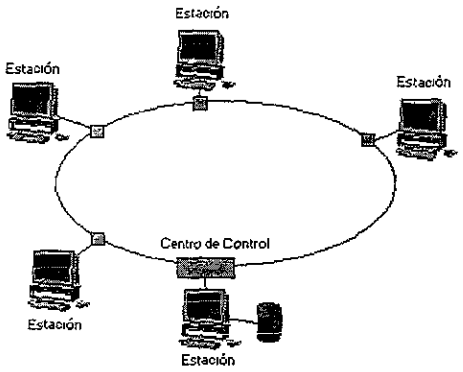
La red en anillo forma un círculo de conexiones punto a punto de estaciones contiguas. Los mensajes van de una estación a otra hasta llegar a la estación adecuada. Las estaciones están conectadas al cable por medio de una unidad de acceso que, a su vez, está conectada a un repetidor, el cual transmite los mensajes que van dirigidos a otras estaciones.

Para poder recibir mensajes, cada estación ha de ser capaz de reconocer su propia dirección; sin embargo, no es necesario desviar los mensajes, ya que éstos van automáticamente a la siguiente estación de la red. En las primeras redes de este tipo, el flujo de la información se movía en una sola dirección. Las redes más modernas disponen de dos canales y transmiten la información en direcciones opuestas por cada uno de ellos.

Cuando se usa una topología en anillo para distribuir el control en redes locales, el protocolo utilizado ha de evitar situaciones conflictivas a la hora de acceder a un canal compartido.

2.4.1. Bucle

Una red en bucle es una red en anillo en la que todas las estaciones están conectadas a un centro de control, que es el que controla las comunicaciones. Una de las estaciones funciona como centro de control y es la responsable del acceso del resto de las estaciones al canal.



Red en Bucle

Ilustración 2-5 Red en Bucle.

Últimamente está adquiriendo auge un nuevo tipo de conexión en anillo en el que el cable que conecta las estaciones pasa a través de un centro de conmutación formado por diversos relees. De esta forma, si falla una estación, ésta se desconecta y el resto de la red puede seguir funcionando. Este tipo de red en anillo facilita además el mantenimiento, puesto que proporciona un punto de control y reconfiguración centralizado. En teoría, es posible conectar varias redes en anillo para formar una red en anillo compuesta.

2.4.2. Factores de evaluación de la topología en anillo

⇒ Aplicación: Una red en anillo es interesante en situaciones en las que se ha de asignar la capacidad de la red de forma equitativa, o cuando haya que conectar un pequeño número de estaciones que funcionen a velocidades muy altas en distancias muy cortas.

⇒ Complejidad: Una red en anillo requiere *hardware* relativamente complicado. El desvío de mensajes es en gran medida sencilla, puesto que el mensaje solamente se mueve en una dirección, la estación emisora sólo necesita saber la dirección de la estación de destino.

⇒ Respuesta: Con tráfico muy alto, la respuesta del sistema permanece bastante estable. El aumento del tiempo de espera es menor que en otros tipos de red; sin embargo, el tiempo de espera medio es bastante alto incluso cuando la carga del sistema es baja.

⇒ Vulnerabilidad: El fallo de una sola estación o de un canal puede hacer que falle todo el sistema. Esto es debido a la interdependencia de las estaciones. En este tipo de topología resulta bastante difícil localizar un fallo; en un sistema muy amplio puede no ser posible reparar inmediatamente el problema. Sí se desea mantener la red en funcionamiento, es necesario duplicar los recursos o utilizar un método para evitar los puntos en los que se ha producido el fallo.

⇒ Expansión: En una red de anillo equipada con centros conectores apropiados es bastante sencillo añadir o suprimir estaciones sin tener que hacer un gran número de conexiones; Por tanto, los costos de modificación del sistema son relativamente bajos. Para hacer modificaciones no se suele interrumpir el sistema, aunque en ocasiones puede ser conveniente y, a veces, necesario.

2.5. Anillo Compuesta

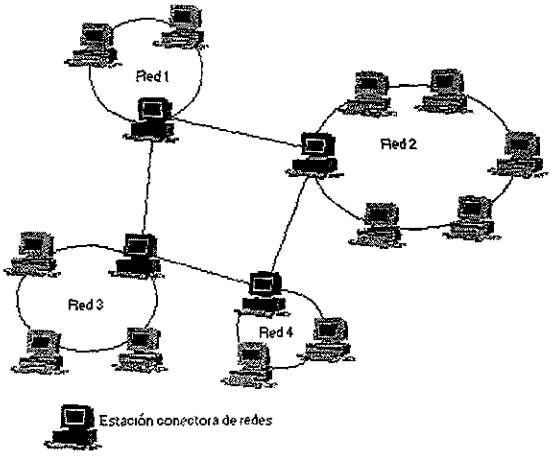


Ilustración 2-6 Red en Anillo Compuesta.

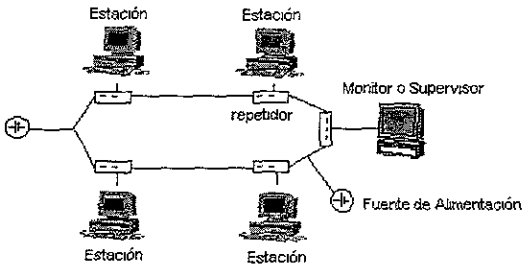
2.5.1. Ventajas E Inconvenientes

Ventajas:

- ◊ La capacidad de transmisión se reparte equitativamente entre todos los usuarios.
- ◊ La red no depende de un nodo central.
- ◊ Es fácil localizar los nodos y enlaces que originan errores.
- ◊ Se simplifica al máximo la distribución de mensajes.
- ◊ Es fácil comprobar los errores de transmisión.
- ◊ Resulta sencillo enviar un mismo mensaje a todas las estaciones.
- ◊ El tiempo de acceso es moderado, incluso en situaciones de mucho tráfico.
- ◊ El índice de errores es muy pequeño.
- ◊ Se pueden conseguir velocidades de transmisión muy altas.
- ◊ Permite utilizar distintos medios de transmisión.

Inconvenientes:

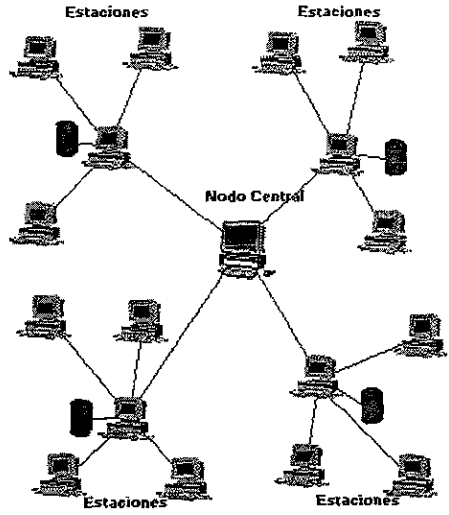
- ◊ La fiabilidad de la red depende de los repetidores.
- ◊ Es necesario un dispositivo monitor.
- ◊ Es difícil incorporar nuevos dispositivos sin interrumpir la actividad de la red en el caso de que ésta no disponga de centros conectores.
- ◊ La instalación es bastante complicada.



Red en Anillo

Ilustración 2-7Red en Anillo.

2.6. Estrella



Topología en Estrella

Ilustración 2-8 Topología Estrella.

En una configuración en estrella cada estación de trabajo está conectada a un nodo central por medio de un canal punto a punto dedicado. Las estaciones pasan los mensajes al servidor central, y éste lo transmite a la estación a la que vaya dirigido.

El control de la red se puede asignar de cualquiera de las tres formas siguientes:

1) El control reside en el nodo central, el cual efectúa la retransmisión de los mensajes. Los datos recibidos en la estación central pueden ser procesados dentro de la misma estación o pueden ser enviados a otra estación para que los procese. En este caso, el nodo es el que proporciona la potencia principal de cálculo.

2) El control puede estar a cargo de una de las estaciones exteriores, en vez de la estación central. El gestor actúa de conmutador, estableciendo conexiones entre las distintas estaciones.

3) El control puede estar distribuido entre todas las estaciones. El nodo se usa para enviar mensajes a sus destinos y resolver las solicitudes de conexiones conflictivas entre estaciones de trabajo.

En los tres casos el nodo central es la estación principal; si ésta fallase para toda la red.

El nodo central proporciona el punto lógico para conectar directamente los recursos compartidos más importantes.

Generalmente, las estaciones no tienen que tomar decisiones en cuanto a cómo y cuando transmitir los mensajes, puesto que todas las comunicaciones han de pasar a través de la estación central antes de llegar a sus destinos. Las "redes en estrella compuestas" son aquellas en las que una estación de la red puede actuar como gestor y/o controlador de una red secundaria.

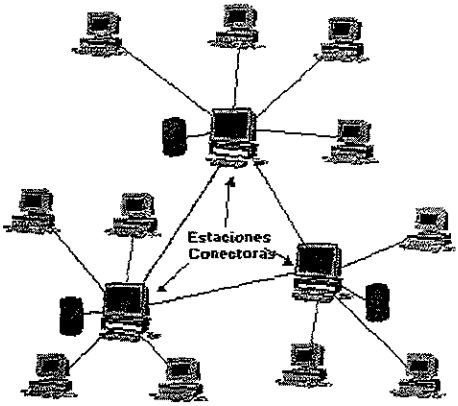
A veces, para referirse a una red en estrella compuesta se utiliza el término "copo de nieve", por su similitud a éste.

El tamaño y capacidad de la red están directamente relacionados con la potencia de la estación central. La carga que conlleva todo lo relacionado con la compatibilidad la soporta el nodo central.

La topología en estrella elimina la necesidad de que cada estación de la red efectúe sus propias decisiones de transmisión. Toda la retransmisión de mensajes se efectúa en el nodo central.

Conceptualmente, la topología en estrella es compatible con los servicios telefónicos básicos, y a menudo se utilizan las mismas líneas mediante un sistema *PBX* de datos.

2.7. *Estrella Compuesta*



Red en Estrella Compuesta o " Copo de Nieve"

Ilustración 2-9 Red en Estrella Compuesta.

2.7.1. Factores De Evaluación De La Topología En Estrella

⇒ Aplicación: Actualmente, la red en estrella es la mejor forma de integrar servicios de datos y voz. Una red de datos en estrella que utilice los nuevos sistemas *PBX* digitales ofrece las ventajas y el ahorro de los servicios informáticos.

⇒ Estaciones conectadas a la estación central pueden, a su vez, actuar de nodo central para otras estaciones, o pueden estar conectadas a enlaces de comunicaciones remotos.

⇒ Respuesta: La respuesta es buena para una carga moderada del sistema. Sin embargo, el tamaño y la capacidad de la red, y, por tanto, la respuesta, están directamente relacionados con la potencia del nodo central. La dependencia de la red es muy alta: normalmente la estación (nodo central) no se puede usar para ninguna otra cosa mientras está actuando como controlador de la red. El número de líneas separadas es también muy alto.

⇒ Vulnerabilidad: La fiabilidad de la red depende completamente del nodo central. Si éste falla, cesa toda la actividad de la red. El fallo de una sola estación no afecta al funcionamiento del sistema. En cualquier caso, la identificación y separación de problemas quedan simplificadas por el control centralizado.

⇒ Expansión: La expansión del sistema es muy restringida; la mayoría de los nodos centrales sólo pueden soportar un número limitado de interfaces de red. A menudo, al usuario se le imponen las limitaciones de ancho de banda y de velocidad de transmisión. Estas limitaciones son necesarias para proteger de sobrecarga las funciones de proceso del nodo central.

2.7.2. Ventajas E Inconvenientes

Ventajas:

◊ Es ideal en configuraciones en las que hay que conectar muchas estaciones a una central de administración y gestión de red.

◊ Se pueden conectar terminales no inteligentes.

◊ Las estaciones pueden tener velocidades de transmisión diferentes.

◊ Permite utilizar distintos medios de transmisión.

◊ Se puede obtener un alto nivel de seguridad.

◊ Es fácil detectar y localizar averías.

◊ La transmisión de los mensajes está controlada por el nodo central.

Inconvenientes:

◊ Es susceptible de averías en el nodo central.

◊ Elevado precio debido a la complejidad de la tecnología que se necesita en el nodo central.

◊ La instalación de los cables resulta bastante cara.

◊ La actividad que debe soportar el nodo central hace que normalmente las velocidades de transmisión sean inferiores a la que se consiguen en la topología en bus y en anillo.

2.7.3. Evolución De La Topología.

La Topología de una Red, tanto física como lógica, puede variar a lo largo del tiempo. Normalmente aparecen nuevos usuarios que quieren conectarse y se introducen nuevos nodos.

Este incremento de equipos conectados supone una disminución del ancho de banda - menos velocidad de transmisión y peor rendimiento de la red (aumento de las colisiones) -.

Frente a eso, los administradores de las redes deben conseguir más ancho de banda, modificando el entorno de la red:

* Segmentando la Red de forma lógica en el *hub* y/o en el ámbito de la base.
* Segmentándola de forma física.
* Instalando *bridges* y/o *routers* (ruteadores) en los puntos críticos para reducir el tráfico segmentado.
* Añadiendo más adaptadores a los servidores, etc.

En definitiva, deben adoptar tecnologías que permitan soslayar los cuellos de botella.

2.7.4. Topología Interna (Nivel De Control De Acceso Al Medio)

Es la topología sobre la que trabaja el protocolo de acceso al medio. Es como va el tráfico por la red a ese nivel, es decir, la forma que adopta el flujo de información (En Bus, En Anillo,) al seguir un determinado protocolo de acceso al medio (MAC) dependiendo de la arquitectura: *Ethernet*, o *Token Ring*.

Una Red *Ethernet* trabaja sobre un bus.

Una Red *Token Ring* trabaja sobre un Anillo.

Luego podemos decir que ambos aspectos constituyen la topología de una red.

Físicamente la Ilustración 2-10 de la red formada por los equipos de usuarios (A, B, C, D y E), por los medios de transmisión (en este caso los cables de par trenzado 1, 2, 3, 4 y 5) y por el equipo de interconexión (el concentrador) es una estrella. Pues claramente adopta esa forma.

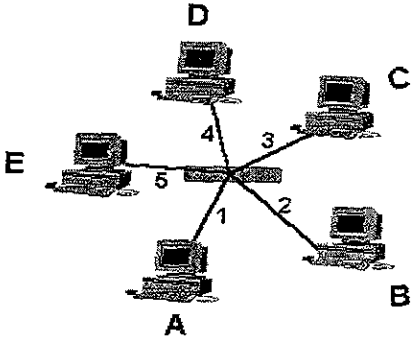


Ilustración 2-10 Interconexión Básica de una Red.

Sin embargo internamente es un bus:

Ejecuta el protocolo de acceso al medio *CSMA/CD* o *Ethernet*, sobre cable de par trenzado sin apantallar (*UTP*), lo que se conoce como entorno 10BaseT, y dicho protocolo trabaja en un bus.

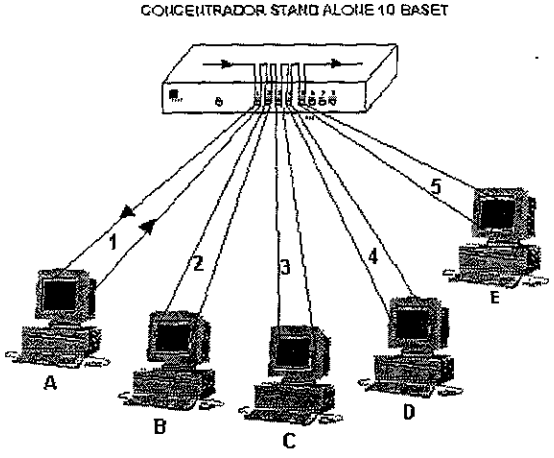


Ilustración 2-11 Interconexión de un HUB en una Red de Computadoras.

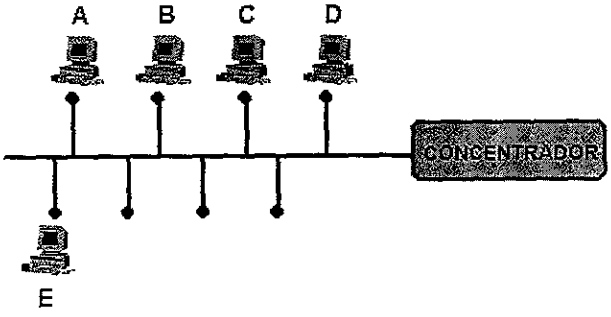


Ilustración 2-12 Conexión Estrella a Bus a través de un Hub.

La ventaja de tener una estrella, es que si se estropea algún nodo (en nuestro caso cada equipo de usuario con su correspondiente cable), los demás pueden seguir funcionando (FIGURA 1). Sólo si se estropea el nodo principal (el concentrador) deja de funcionar la red. Sin embargo, si físicamente tuviéramos un bus (un único cable), al estropearse el cable todos los nodos dejarían de funcionar (FIGURA 2).

FIGURA 1

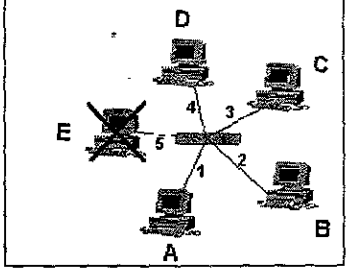
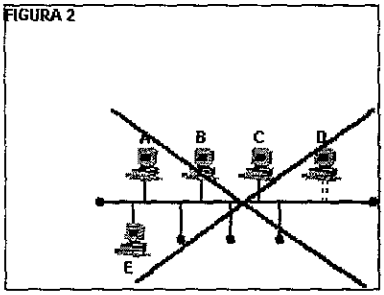


FIGURA 2



2.8. *Protocolos de control de acceso al medio (MAC)*

Las redes locales típicamente se organizan en base a un esquema de red de broadcast (difusión). Es decir, múltiples computadoras se conectan a un medio común, que permite difusión (radio en el aire, coaxial, etc.).

Los protocolos utilizados para compartir este medio entre todos los participantes, son conocidos como MAC (Medium Access Control).

El modelo es simple: un medio compartido donde todos pueden escribir y leer. Si dos o más computadoras transmiten al mismo tiempo se produce una colisión, que es detectable (y distinta a cualquier dato posible).

2.8.1. Aloha

Este es el protocolo que dio origen a muchos en uso hoy en día. La idea es muy simple, cuando se desea transmitir se transmite. Habrá colisiones, y tanto los emisores como el resto detectarán eso. La colisión destruye los paquetes emitidos, los que deberán ser re-emitidos. Los protocolos entonces deben determinar cuándo hacerlo (por ejemplo, no sirve esperar un tiempo fijo, puesto que ambos transmitirán juntos). Una alternativa es esperar un tiempo aleatorio antes de retransmitir.

Si suponemos paquetes de largo fijo a transmitir y que cada estación transmite en cuanto tiene datos, la probabilidad de colisión en redes cargadas es muy alta puesto que basta con que el último *bit* de un paquete se transmita junto con el primer *bit* de otro para que ambos colisionen y se destruyan.

Un dato importante en estas redes compartidas es cuánto es el factor máximo de utilización que se puede lograr del medio. Es decir, si tengo un *UTP* de capacidad total 10 Mbps, cuánto puedo ocupar realmente entre todos los participantes. Esto no es trivial, porque requiero que haya mucha carga de tráfico para utilizar más ancho de banda, pero al aumentar el tráfico aumentan las colisiones.

En el caso del protocolo *ALOHA* puro, se tiene que el máximo factor de utilización es 18%, lo que dista mucho de ser razonable.

Una optimización al protocolo es dividir el tiempo en *slots* fijos sincronizados (slotted ALOHA). Una computadora sólo puede transmitir en un comienzo de *slot* (que dura justo el tamaño de un paquete). Esto disminuye la probabilidad de colisiones, permitiendo un factor de utilización máximo de 37%.

2.8.2. CSMA/CD

Una optimización importante a *ALOHA* puro es no transmitir si el canal está ocupado, lo que implica escuchar antes de hablar (Carrier Sense). Si el canal está ocupado, puedo quedar escuchando hasta que se desocupe y ahí transmitir (CSMA1-persistente).

Esto no es muy bueno, porque al aumentar la carga, aumenta la probabilidad de que más de una computadora esté escuchando el canal ocupado, esperando transmitir, y por lo tanto habrá una colisión cuando ambos intenten. Para evitar esto, en vez de esperar que el canal se desocupe, esperamos un tiempo aleatorio antes de volver a intentar (CSMA no persistente).

3. Medios de transmisión (MT)

El propósito fundamental de la estructura física de la red consiste en transportar, como flujo de *bits*, la información de una máquina a otra. Para realizar esta función se van a utilizar diversos medios de transmisión. Estos se pueden evaluar atendiendo a los siguientes factores:

∴ Tipo de conductor utilizado.

∴ Velocidades máximas que pueden proporcionar (ancho de banda).

∴ Distancias máximas que pueden ofrecer.

∴ Inmunidad frente a interferencias electromagnéticas.

∴ Facilidad de instalación.

∴ Costo.

∴ Capacidad de soportar diferentes tecnologías de nivel de enlace.

3.1. Principales mt's usados en redes de área local

Los principales soportes físicos de la transmisión para redes de área local son cables de los siguientes tipos: par trenzado, apantallado o sin apantallar, coaxial y fibra óptica. Vamos a dar una pequeña descripción de cada uno de ellos.

3.1.1. Cable coaxial

Se ha venido usando ampliamente desde la aparición de la red *Ethernet*. Consiste básicamente, en un hilo de cobre rodeado por una capa de aislante que a su vez esta recubierta por un apantallamiento. Todo el conjunto está envuelto por un aislante exterior.

Se suele suministrar en distintos diámetros, a mayor diámetro mayor capacidad de datos, pero también mayor costo. Los conectores resultan más caros y por tanto la terminación de los cables hace que los costos de instalación sean superiores. El cable coaxial tiene la ventaja de ser muy resistente a interferencias, comparado con el par trenzado, y por lo tanto, permite mayores distancias entre dispositivos.

Existen distintos tipos de cables coaxiales, entre los que destacan los siguientes:

* Cable estándar *Ethernet*, de tipo especial conforme a las normas IEEE 802.3 10BASE5. Se denomina también cable coaxial "grueso", y tiene una impedancia de 50 Ohmios. El conector que utiliza es del tipo "N".
* Cable coaxial *Ethernet* delgado, denominado también RG58, con una impedancia de 50 Ohmios. El conector utilizado es del tipo BNC.
* Cable coaxial del tipo RG 62, con una impedancia de 93 Ohmios. Es el cable estándar utilizado en la gama de equipos 3270 de IBM, y también en la red ARCNET[5]. Usa un conector BNC.
* Cable coaxial del tipo RG59, con una impedancia de 75 Ohmios. Este tipo de cable lo utiliza, en versión doble, la red WANGNET, y dispone de conectores DNC y TNC.

Sin embargo, la forma de conectar computadoras al cable es delicada: una T debe insertarse en el cable y conectarlo directamente a la interfaz de comunicación. También existen los vampiros (adaptadores), que sólo sirven para cable coaxial grueso que es menos manipulable. Esto genera múltiples problemas en instalaciones de tamaño medio, puesto que el coaxial es muy estable si no se toca, pero no soporta bien los tirones y movimientos. Un trozo de coaxial con problemas impide la comunicación en toda la red.

3.1.2. Par trenzado

El Par Trenzado es el medio más usado de comunicación por el sistema telefónico. Dos cables de cobre telefónicos trenzados en forma helicoidal (para evitar que hagan de antena) permiten tasas de transferencia punto a punto de varios Mbps, dependiendo del largo y del grosor.

3.1.3. Par trenzado sin apantallar (UTP)

Es el soporte físico más utilizado en las redes de área local, pues es barato y su instalación es barata y sencilla. Por él se pueden efectuar transmisiones digitales (datos) o analógicas (voz). Consiste en un mazo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía. Un cable de pares trenzados puede tener pocos o muchos pares; en aplicaciones de datos lo normal es que tengan cuatro pares. Uno de sus inconvenientes es la alta sensibilidad que presenta ante interferencias electromagnéticas.

[5] Sistema de Red de área local (LAN) desarrollada por Datapoint Utiliza las técnicas de pasa fichas ('token') pero no es una anillo ('ring') sino que sigue la topología física de estrella y permite un máximo de 256 nodos en la red.

En noviembre de 1991, la EIA (Electronics Industries Association) publicó un documento titulado "**boletín de especificaciones técnicas adicionales para cables de par trenzado sin apantallar**", Documento TSB-36. En dicho documento se dan las diferentes especificaciones divididas por "**categorías**" de cable *UTP* (Unshielded Twisted Pair).

También se describen las técnicas empleadas para medir dichas especificaciones. Por ejemplo, se definen la Categoría 3 hasta 16MHz, la Categoría 4 hasta 20 MHz y la Categoría 5, hasta 100 MHz.

Los cables de categoría 1 y 2 se utilizan para voz y transmisión de datos de baja capacidad (hasta 4 Mbps). Este tipo de cable es el idóneo para las comunicaciones telefónicas, pero las velocidades requeridas hoy en día por las redes necesitan mejor calidad.

Los cables de categoría 3 han sido diseñados para velocidades de transmisión de hasta 16 Mbps. Se suelen usar en redes IEEE 802.3 10BASE-T y 802.5 a 4 Mbps.

Los cables de categoría 4 pueden proporcionar velocidades de hasta 20 Mbps. Se usan en redes IEEE 802.5 *Token Ring* y *Ethernet* 10BASE-T para largas distancias.

Los cables de categoría 5 son los *UTP* con más prestaciones de los que se dispone hoy en día. Soporta transmisiones de datos hasta 100 Mbps para aplicaciones como *TPDDI* (FDDI sobre par trenzado).

Cada cable en niveles sucesivos maximiza el traspaso de datos y minimiza las cuatro limitaciones de las comunicaciones de datos: atenuación, *Crosstalk*, capacidad y desajustes de impedancia.

La atenuación es un descenso en el nivel de señal, causado por imperfecciones en el cable. Se mide en decibelios por cada cien metros (dB/m). El mínimo valor de dB/m significa mejor cable.

Crosstalk o paradiafonía (medido en decibelios) es el ruido eléctrico en el cable, causado por las luces fluorescentes o señales inducidas por cables cercanos.

La capacitancia (medida en picofaradios por metro [pf/m]) es la distorsión de las señales eléctricas causada por cables de pares cercanos. A menor valor de pf/m, mejor será el cable.

Los desajustes de impedancia ocurren cuando la impedancia de una señal no se ajusta a la del dispositivo de recepción.

Es una medida de cómo las señales pueden pasar fácilmente a través de un circuito. Para comunicaciones más claras, la impedancia de la señal transmitida y recibida debe ser igual. La impedancia para los cables *UTP* debe ser de 100 ohms. ±15.

3.1.4. Par trenzado apantallado (STP)

Suele denominarse STP (Shielded Twisted Pair) y tiene en IBM a su principal promotor. Como inconveniente tiene que es más caro que el *UTP*, pero tiene la ventaja de que puede llegar a superar la velocidad de transmisión de 100 Mbps.

Se diferencia del *UTP* en que los pares trenzados van recubiertos por una malla, además del aislante exterior que poseen tanto los cables STP como los *UTP*. Los conectores que se suelen usar con los cables de par trenzado son RJ-45 o RJ11.

Su interés es tan alto, que hoy día se usan para reemplazar cableado de coaxial, haciendo una estrella del bus (o estrellando el bus). Para esto se usa un concentrador, donde llegan todos los pares trenzados, y que repite los datos hacia todos los cables. Esto disminuye las colisiones, evita los puntos de falla globales (salvo por el concentrador mismo) y permite usar el cableado telefónico normal para redes locales.

3.1.5. Fibra óptica

Se utiliza, en los últimos años, cada vez más como soporte físico en las redes locales y públicas. De todas formas su costo sigue siendo demasiado elevado para que se utilice de forma generalizada. En la actualidad se utiliza principalmente para conexiones entre edificios. Está compuesta por un hilo de vidrio (fibra óptica), envuelto por una capa de algodón y un revestimiento de plástico (ver Ilustración 3-1). Es necesaria la existencia de un dispositivo activo que convierta las señales eléctricas en luz y viceversa.

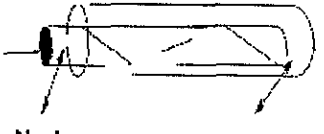


Ilustración 3-1Esquema de una Fibra Optica.

La luz tiene una frecuencia del orden de los $10^{8\ Mhz,}$ lo que permite un ancho de banda enorme. El sistema de transmisión se basa en un emisor de luz, un receptor y un medio de transmisión: fibra de vidrio o de sílice.

Gracias a los coeficientes de refracción de la luz, se puede enviar luz sin perder nada de un punto al otro. Incluso, varios rayos pueden viajar al mismo tiempo usando diferentes ángulos de refracción (fibras múltimodo). Una fibra que es del largo de onda de la luz usada puede utilizarse como fibra monomodo, sin refracción, lo que permite mejores tasas de transmisión por mayor distancia (pero con equipamiento más caro).

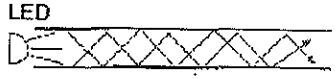


Ilustración 3-2 Esquema de Difracción Con LED.

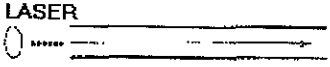


Ilustración 3-3 Esquema de Difracción con Láser.

Las ventajas de la fibra óptica residen en la resistencia total que ofrece a interferencias electromagnéticas, en ser un soporte físico muy ligero y, sobre todo, a que ofrecen distancias más largas de transmisión que los anteriores soportes. Sus inconvenientes se encuentran en el costo (sobre todo en los acopladores) y en que los conectores son muy complejos.

Existen tres tipos de fibra óptica:

∴ F.O. múltimodo con salto de índice. La fibra óptica está compuesta por dos estructuras que tienen índices de refracción distintos. La señal de longitud de onda no visible por el ojo humano se propaga por reflexión. Así se consigue un ancho de banda de 100 MHz.

∴ F.O. múltimodo con índice gradual. El índice de refracción aumenta proporcionalmente a la distancia radial respecto al eje de la fibra óptica. Es la fibra más utilizada y proporciona un ancho de banda de 1 GHz

∴ F.O. monomodo. Sólo se propagan los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo (en concreto un ancho de banda de 50 GHz).

Para terminar con los medios de transmisión nos vamos a referir brevemente a los modos de transmisión. Existen dos modos de transmisión: banda base y banda ancha.

La banda base es la transmisión digital de datos a través de un cable. La codificación utilizada es normalmente de tipo Manchester, que permite combinar una señal de reloj con los datos. La transmisión en banda base implica que sólo puede haber una comunicación en el cable en un momento dado.

La transmisión en banda ancha es la transmisión analógica de los datos. Para ello se utilizan módems que operan a altas frecuencias. Cada módem tiene una portadora diferente, de forma que es posible realizar varias comunicaciones simultáneas en el cable.

Actualmente, 1 Gbps es normal en fibra óptica, pero en redes locales es bastante menos.

Aún no se dispone comercialmente de multiplexores en frecuencia de fibra óptica, pero ya existen en laboratorios. Esto permite pasar 10^8 señales con 1 MHz cada una a la vez por una sola fibra.

3.2. Medios de comunicación

3.2.1. Antenas directas

Existen varias maneras de conectar punto a punto lugares "visibles": por medio de infrarrojos, láser, UHF, microondas, debido a esto son definidas como tales.

3.2.2. Satélites

Los satélites de comunicaciones están en órbita geo-estacionaria, a 36.000 Km sobre el ecuador. Cada satélite posee varios Transponders, cada uno con capacidad de 50 Mbps (existen satélites experimentales para llegar a Gbps). Esta capacidad puede ser dividida en múltiples canales más lentos (800 64 Kbps por ejemplo).

El problema de los satélites es el retardo de la señal. La tasa de transferencia (*bits/s*) no indica cuánto demora la señal en llegar al otro lado. La órbita geo-estacionaria está tan lejos que en subir y bajar del satélite la onda demora unos 300 ms.

Esto implica una ida y vuelta de una señal de 600 ms (aproximadamente medio segundo).

En algunos casos (envío de archivo) esto no es relevante, pero en otros (comunicación interactiva) es desastroso.

3.2.3. Red telefónica

La red telefónica es probablemente el medio de transporte de datos más usado en el mundo, a pesar de que nunca fue diseñada para ello. Con sus más de 300 millones de suscriptores en el mundo, presente en todas partes, es demasiado atractiva para usarla, a pesar de sus limitaciones.

La red telefónica tradicional (que en lenguaje de telecomunicaciones se denomina POTS: Plain Old Telephone System) provee una línea de comunicaciones punto a punto que transmite entre 0 y 3000 Hz. Además, la calidad sólo concierne que las frases sean distinguibles, por lo tanto el nivel de ruido tolerable es enorme, y no todas las frecuencias intermedias pasan con la misma calidad. Aunque ya la mayoría de las centrales telefónicas son digitales (en México están aún en reestructuración) y las troncales son de fibra óptica, la mayoría del ruido se genera en el par trenzado que une el teléfono con la central más cercana.

La calidad del tendido es muy variable y depende de la época en que fue hecho. A pesar de las apariencias, en realidad la mayoría del capital de las compañías de teléfonos está en esos cables. Se estima que el total de cables a las casas (conocido como localloop) tendidos en el mundo rinden ir y volver a la luna unas 1000 veces.

Curiosamente, el par trenzado debería ser capaz de soportar 2 Mbps sin problemas, y las centrales digitales mucho más. Por lo tanto, disponemos de la infraestructura para obtener datos a velocidad más que razonables desde la casa. Lo que nadie descubre aún es cómo vender ese servicio. Algunos intentos se hacen con ISDN[6], que permite conexiones a 128 Kbps si ambos teléfonos tienen ese servicio. Sin embargo, mientras las estructuras de precio sean como el teléfono y los anchos de banda sean parecidos, nadie quiere pagar más por ello. En Estados Unidos de Norteamérica, el *ISDN* se ha vuelto una alternativa atractiva en algunos estados, en particular para accesar *Internet*.

Para poder transmitir datos por la línea telefónica tradicional, se usa un módem (Modulator/Demodulator). La idea es transformar la onda cuadrada digital en una onda sinusoidal análoga. Inicialmente, los *módems* usaban modulación en frecuencia (un tono=0 otro tono=1) y operaban a 300 bps, que obedecen a los 300 bauds de la línea. Luego, usando múltiples tonos, 1.200 y 2.400 fueron comunes. Usando modulación de fase y luego técnicas sumamente avanzadas de adaptación dinámica de frecuencias, se pasó a 4.800, 14.400 y 28.800 bps. Ahora utilizando módems con sistemas Analógico/Digitales y bases ISND, se paso de 36.600 hasta un Troughtput[7] de 57.400 bps.

3.2.4. Modos de transmisión

3.2.4.1.Half-Duplex

Es una forma de transmisión exclusiva de dos direcciones por la que dos nodos en una red que desean hablar entre ellos pueden estar mandando o recibiendo en cualquier momento, pero no realizando ambas cosas a la vez.

3.2.4.2.Full-Duplex

Significa que cada nodo de la red puede estar simultáneamente transmitiendo y recibiendo en el mismo momento. Esto se consigue utilizando dos pares de alambres en el cable *Ethernet* para la transmisión de datos, mientras que normalmente uno de estos cables se usa para el informe de colisiones.

---

[6] Conexiones digitales que forman parte de la RDSI (Red Digital de Servicios Integrados) cómo parte de los servicios telefónicos locales.

[7] Transmisión a Banda Completa

3.3. Técnicas de interconexión

En redes de área amplia (WAN) donde deben interconectarse múltiples puntos unos con otros, es imposible pensar en conexiones físicas punto a punto, por lo que se utilizan varias técnicas para compartir troncales entre varias comunicaciones simultáneas.

- Multiplexión
- Conmutación

3.3.1. Multiplexión

Dos técnicas clásicas se utilizan para multiplexar una línea (o sea simular varias líneas lógicas sobre una línea física): multiplexión en frecuencia y multiplexión en el tiempo.

Al multiplexar en frecuencia, se asignan rangos de frecuencias a cada conexión, dividiendo la línea en segmentos reservados exclusivamente para cada canal lógico. Según la cantidad de Hz disponibles en la línea puedo multiplexar más o menos.

Al multiplexar en tiempo, los canales lógicos ocupan la línea completa (con todas las frecuencias disponibles) por turnos.

Estos turnos son típicamente *slots* de tiempo predefinidos, garantizando entonces un ancho de banda disponible para cada canal lógico.

Estas dos técnicas pueden mezclarse típicamente haciendo multiplexión en Frecuencia y luego cada canal lógico puede ser multiplexado en tiempo.

Ambas técnicas adolecen de un problema: reservan el ancho de banda aunque no se use. En el caso de redes de computadoras esto es un gran pecado, puesto que muchas conexiones permanecen sin transmitir largos períodos de tiempo.

3.3.2. Conmutación

Como no existen líneas directas punto a punto entre todos los participantes de una red como la red telefónica, además de multiplexar las troncales, debe existir una forma de establecer una conexión virtual punto a punto. Existen dos métodos clásicos para esto: conmutación de circuitos y conmutación de paquetes.

3.3.2.1.Conmutación de circuitos

La conmutación de circuitos es el paradigma de las redes telefónicas Básicamente, al pedir una conexión, se realiza una reserva de recursos desde el origen hasta el destino Originalmente, se reservaban pares de cobre entre los *switches* que físicamente se iban cerrando para establecer una línea entre origen y destino.

Hoy en día todo se basa en multiplexión en frecuencia y tiempo, pero la idea es la misma: una vez establecida la conexión existe un canal lógico reservado entre ambas partes. Si después no hablo durante dos minutos, el costo de recursos es el mismo que si hablo.

- Una ventaja de este esquema es que nunca hay congestión en las conexiones, puesto que los recursos están reservados: el retardo es siempre el mismo. La congestión se maneja en base a tonos ocupados al pedir realizar la llamada.

3.3.2.2.Conmutación de paquetes

La otra alternativa es conmutación de paquetes. En este caso, no se reservan recursos para las conexiones, sino que se simulan sobre paquetes de datos (con un formato muy bien definido). Estos paquetes deben ser ruteados uno por uno hacia su destino, multiplexando en forma natural las troncales (es una multiplexión en el tiempo, pero sin slots pre-asignados). En este caso, el uso de los recursos es optimo, puesto que si no transmitió, no gastó nada. Sin embargo, son de naturaleza muy dinámica, presentando problemas de congestión y de retardo variable. Por otro lado, los paquetes pueden perderse, desordenarse, etc.

3.4. Equipos de interconexión

3.4.1. Repetidores(Repeats).

Un repetidor es la expresión mínima de un concentrador, o dicho con más propiedad, un concentrador es un repetidor multipuerto. Los repetidores, con sólo dos puertos - se denomina puerto a cada conexión con la red o segmento de la misma -, diseñados según las especificaciones IEEE 802.3, actúan como parte del cableado de la red, ya que transfieren los paquetes recibidos de un extremo al otro, independientemente de su contenido, origen y destino; es decir, de un modo totalmente transparente e indiscriminado.

Permiten interconectar dos o más - según sean puros repetidores o concentradores, respectivamente - segmentos incluso con diferentes tipos de cableado, permitiendo, de este modo, sobrepasar el número máximo de nodos o la longitud máxima permitidas por segmento. Se encargan de regenerar las señales y resincronizar los segmentos e incluso de desconectar "**segmentar o particionar**" aquellos que funcionan inadecuadamente, permitiendo así que el resto de la red siga trabajando.

Por supuesto, el uso de repetidores esta también limitado, ya que generan un pequeño retraso, que en caso de prolongarse por varios repetidores consecutivos, impediría el adecuado funcionamiento de la red y la pérdida de los paquetes que circulan por la misma; entre dos nodos cualesquiera de la red pueden existir un máximo de cuatro repetidores, lo que equivale a cinco segmentos, y además en un máximo de tres de ellos pueden conectarse otros

nodos - dos de los cinco segmentos pueden emplearse sólo en la interconexión entre repetidores -

La velocidad a la que transmiten los paquetes es siempre la misma que la de la propia red. Los repetidores actúan, según el modelo OSI, a nivel físico (Capa I).

3.4.2. Concentradores. (Hubs)

Los *hubs* permiten la interconexión de diferentes tipos de cableados, añadiendo la ventaja de utilización de máquinas como puentes o ruteadores sobre una misma caja. Desde los primeros *hubs*, que aparecieron como meros repetidores para cableado estructurado, hasta los actuales, la evolución que han seguido es enorme en comparación con las que han tenido los otros equipos de interconexión. Se diseñaron inicialmente para aprovechar las ventajas del cableado estructurado; pero, al llegar al mercado unos diez años después de que se instalaran las primeras redes comerciales, tuvieron que dar soporte a la tecnología existente además de estar preparados para el futuro.

Los primeros *hubs* eran meros repetidores 10BaseT que permitían la conexión de un determinado número de máquinas a la red principal, utilizando para ello una conexión 10Base5 o 10Base2. No incluían funciones de gestión.

Posteriormente aparecen los *hubs* multimedia, que permiten la conexión a diferentes medios físicos:

10BaseF, Foirl, 10BaseT, 10Base2, 10Base5, etc., añadiendo una función mínima de gestión para el control del *hub.*

Por último, aparecen los *hubs* de tercera generación capaces de mantener sobre una misma máquina un determinado número de redes, de tipo *Ethernet, Token Ring* y *FDDI*, con posibilidad de encaminamiento entre cada una de ellas (utilizando *bridges* y/o *routers*), con diferentes tipos de medios físicos, y añadiendo una gestión mucho más potente, basada en protocolos estándar de gestión, para su control. La arquitectura empleada en ellos difiere, aunque se pueden considerar tres tipos diferentes:

Arquitectura multicanal. Emplea varios canales que definen como redes diferentes, tipo *Ethernet, Token Ring* o *FDDI*.

Arquitectura monocanal. De alta velocidad, con comunicación síncrona o asíncrona.

Arquitectura mixta. Soporta los dos tipos de arquitecturas anteriores.

En el futuro cercano soportarán servicios de tipo multimedia. vídeo, voz, datos, etc., así como ATM (modo de transferencia asíncrono).

3.4.3. Tecnología de HUB´S

3.4.3.1.Arquitectura Tricanal.

Tienen tres canales donde se pueden configurar tres o más redes lógicas Básicamente, se trata de un bus o backplane integrado en un chasis que permite la coexistencia de *Ethernet, Token Ring* y *FDDI.* El máximo número de redes soportadas para cada protocolo es de tres, siete y cuatro respectivamente Nosotros por tanto podemos tener 3.

Se observa que el número máximo de redes de un determinado tipo que pueden configurarse en un único backplane excluye la utilización de redes de otro tipo en el mismo backplane.

Los chasis pueden tener diferente número de slots, de los cuales dos suelen estar ocupados por un módulo de control del *hub* y por otro módulo de gestión (que tiene implementado un agente SNMP), respectivamente. El resto de los slots están ocupados por módulos *Ethernet*, módulos AUI, módulos de Fibra Optica, puentes, repetidores, bridges, ruteadores, etc., cada módulo que insertemos en el *hub* puede ser asignado a una de las redes de que dispongamos, dependiendo de la configuración que hallamos escogido. Los módulos también se pueden dejar aislados sin asignar a ninguna red.

El *hub* está formado por componentes pasivos. Y como el *backplane* síncrono permite al *hub* estar conectado a otros sin necesidad de utilizar repetidores internos, podríamos salvar las limitaciones de la regla de cuatro repetidores de *Ethernet*, pudiendo conectar hasta 23 *hubs* en serie, sin utilizar puentes o repetidores (usando módulos de fibra).

Alta disponibilidad y tolerancia a fallos.

Todos los *hubs* de la última generación tienen una serie de características para proporcionar redes de alta disponibilidad y tolerantes a fallos. Éstas son, principalmente:

- Fuentes de alimentación redundantes. Pueden incorporar una segunda fuente de alimentación de backup, que entra en funcionamiento en caso de que la principal se estropee. Se puede reemplazar la fuente principal mientras sigue funcionando la de backup, sin que se tenga que apagar el equipo.
- Módulos de control redundantes. De la misma forma podemos instalar un módulo de control redundante, que sustituirá al principal en caso de avería de éste.
- Enlaces redundantes. Las roturas o fallos en los cables suelen ser problemas comunes en una red. Si se usan enlaces redundantes en las conexiones (suelen estar disponibles para módulos de fibra), evitaremos las consecuencias de estos problemas. Si el puerto de un enlace falla o el cable se rompe, el puerto redundante entra en funcionamiento entre 100ms.

y 1.1 sg Después, dependiendo del tipo de problema. Para tener un enlace redundante necesitamos una nueva conexión física.

- Port Switching. Esta característica permite que los puertos de un módulo puedan ser asignados dinámicamente a cualquiera de los tres canales disponibles en el backplane. Sólo está disponible para módulos de *Ethernet*. De esta manera, en un mismo módulo podemos tener sus puertos asignados a tres redes *Ethernet* diferentes, pudiendo realizar reasignaciones a una u otra con la simple ejecución de un comando, sin necesidad de tocar el cableado. También tienen la función de switching de módulos, permitiendo asignar dinámicamente un módulo al canal que se desee.
- Concentradores redundantes. Si instalamos concentradores redundantes, podemos asegurar las partes críticas de la red (aquellas que siempre deben funcionar) contra el fallo de los hubs que se encuentran instalados en esas partes.

Para llevar a cabo esto deberíamos usar la redundancia de enlaces.

- Inserción de módulos en caliente. Permiten añadir o quitar módulos sin necesidad de apagar el *hub*.

Sólo existe una excepción: cuando quitamos el módulo de control del *hub*.

- La Gestión SNMP. Está integrada en el módulo de gestión del *hub*.

3.4.4. Puentes (Bridges).

Los puentes (bridges) fueron diseñados, según la normativa IEEE 802.1d, para la conexión de redes diferentes. Igual que los repetidores, son independientes de los protocolos y retransmiten los paquetes a la dirección adecuada basándose precisamente en ésta, en la dirección destino (indicada en el propio paquete). Su diferencia con los repetidores consiste en que los puentes tienen cierta lactancia, que les permite reenviar o no un paquete al otro segmento; cuando un paquete no es retransmitido, decimos que ha sido filtrado. Además esos filtros pueden ser automáticos, en función de las direcciones de los nodos de cada segmento, que los puentes retengan al observar el tráfico de cada segmento, o pueden ser filtros definidos por el administrador de la red, en función de razones de seguridad, organización de grupos de trabajo en la red, limitación de tráfico innecesario, etcétera.

Otra diferencia importante es que con los repetidores, el ancho de banda de los distintos segmentos es compartido; mientras que con los puentes, cada segmento dispone del 100% del ancho de banda o, en otras palabras, el ancho de banda total de la red se multiplica por el número de puertos de los que dispone el puente.

En el caso de una red *Ethernet*, un puente (dos puertos), el ancho de banda disponible entre dos segmentos seria de 20 Mbps, y si se dispone de un puente multipuerto, por ejemplo con tres puertos, el ancho de banda total será de 30 Mbps, y así sucesivamente.

Su filosofía impide que las colisiones se propaguen entre diferentes segmentos de la red, algo que los repetidores son incapaces de evitar Los puentes pueden llegar, según sus prestaciones, a transmitir los paquetes a la misma velocidad a la que circulan por la red. Los puentes de una red se enlazan habitualmente entre sí con topología de bus y a su vez se combinan con concentradores o repetidores multipuerto para extender la red de un modo eficaz, mediante una topología de estrella. Los puentes funcionan en la capa 2 del modelo OSI (enlace).

Una característica muy importante de los puentes es el algoritmo para enlazar protocolos (spanning tree), un mecanismo del *software* de un puente, por el cual se impide que se creen bucles dentro de una red donde haya varios puentes, al intercambiar constantemente entre ellos unos paquetes denominados BPDU que les permiten reconfigurar dinámicamente, los caminos a seguir por el tráfico de la red, sirviendo así incluso de medida de seguridad en caso de fallo de algún puente, al poder establecer, automáticamente, una ruta alternativa.

3.4.5. Ruteadores (Routers)

Los ruteadores (routers) son dependientes del protocolo, y de modo similar a los puentes tienen la capacidad de filtrar el tráfico de un modo inteligente. Su funcionamiento esta basado en gran medida en la información del protocolo contenida en cada paquete. Igual que los puentes, impiden la propagación de las colisiones de unos segmentos a otros de la red; es más, en realidad separan totalmente los segmentos convirtiéndolos en redes lógicas totalmente diferentes, que se denominan dominios, y modifican incluso el contenido de los paquetes retransmitidos. Como en el caso de los puentes, pueden llegar a transmitir los paquetes a la misma velocidad a la que circulan por la red.

Los ruteadores se sitúan en la capa de red del modelo OSI (nivel 3); sin embargo, la realidad es que en la mayoría de los productos actuales, hay una gran mezcla entre puentes y ruteadores, lo que se denomina brouters, que realizan funciones de puentes a nivel 3, y tienen la capacidad de comportarse como puros puentes o como puros ruteadores.

3.4.6. Conmutadores (Switches)

Los conmutadores (switches) son, en cierto modo, puentes multipuerto, aunque pueden llegar a tener funciones propias de ruteadores. Incrementan la capacidad total de tráfico de la red dividiéndola en segmentos más pequeños y filtrando el tráfico innecesario, bien automáticamente o bien en función de filtros definidos por el administrador de la red, haciéndola, en definitiva, más rápida y eficaz.

Cuando un paquete es recibido por el conmutador, éste determina la dirección fuente y destinataria del mismo; si ambas pertenecen al mismo segmento, el paquete se descarta; si son direcciones de segmentos distintos, el paquete se retransmite (a no ser que los filtros definidos lo impidan). En teoría, la diferencia fundamental entre puentes y conmutadores es que los puentes reciben el paquete completo antes de proceder a su envío al puerto destinatario, mientras que un conmutador puede iniciar su reenvío antes de haberlo recibido por completo. Ello redunda, evidentemente, en una mejora de prestaciones.

Un conmutador mantiene internamente una tabla asociando los puertos físicos con las direcciones de los nodos conectados a cada puerto.

Las direcciones pueden haber sido introducidas de forma manual por el administrador de la red, o pueden haber sido aprendidas por el conmutador en su monitoreo continuo de los paquetes que le llegan por cada puerto. Utilizando esta tabla y las direcciones destino de los paquetes recibidos, el conmutador determina una dirección desde el puerto fuente al destino, y transfiere el paquete en función de la misma. Esta conexión virtual entre la fuente y el destino se establece sólo para cada paquete enviado.

Los conmutadores ofrecen además la posibilidad de realizar transferencias simultáneas entre distintos pares de puertos a la velocidad de la red. En cualquier caso, el número máximo de transferencias simultáneas que puede realizar un conmutador es una de las características fundamentales para determinar sus prestaciones reales. Así, un conmutador de 24 puertos puede simultáneamente trabajar con 12, y si estas son *Ethernet* (10 Mbps), su capacidad total será de 120 Mbps; en el caso de que la combinación de su *hardware/software* no permita dicha capacidad teórica se produce su bloqueo interno, y se podría hablar por tanto de un conmutador diseñado defectuosamente.

Por otro lado, si el tráfico se produce desde varios puertos fuente hacia un único puerto destino, lo que podría ser el caso de un servidor y múltiples clientes, las prestaciones del sistema no se incrementan de forma significativa más allá de la propia velocidad de la red, puesto que el tráfico desde/hacia el servidor es incapaz de superar el límite impuesto por su segmento.

Se produce entonces otro tipo de bloqueo interno, ya que el conmutador se ve obligado a almacenar temporalmente los paquetes que llegan cuando se ha establecido ya una conexión virtual, hasta que esta termina y puede establecerse una nueva, y así sucesivamente

Esto también tiene solución, ya que en el mercado están disponibles conmutadores que ofrecen conexiones, bien para el enlace con servidores o con el troncal de la red, o incluso para la intercomunicación con otros conmutadores, a mayores velocidades, con soporte de tecnologías como Fast *Ethernet* (100 Mbps), Full Duplex *Ethernet* (20 Mbps), Full Duplex Fast *Ethernet* (200 Mbps), *FDDI* (100 Mbps), e incluso *ATM* (155 Mbps). Se puede optar también por otra opción si el *software* del servidor lo soporta. Esta tarea consiste en conectar el servidor o servidores al conmutador de forma simultánea por varios puertos o segmentos de la red.

Ello requiere también un soporte especial por parte del *software* del propio conmutador para que identifique los diferentes puertos como correspondientes a un único nodo de la red y sea capaz de remitir el tráfico a uno u otro puerto en función de su ocupación.

Los conmutadores pueden realizar su función de dos modos diferentes:

3.4.6.1.Cortar-continuar

Dado que la dirección destino está en la primera parte del paquete, el reenvío del mismo puede iniciarse antes, incluso, de que el paquete entero haya sido recibido por el conmutador, y en ello se basa el método cortar-continuar (cut-through). Es decir, el paquete se examina tan pronto como se ha podido recibir la parte donde está la dirección de destino, al mismo tiempo que se continúa recibiendo el resto del paquete. En el momento en que se ha podido decidir si ha de ser reenviado o filtrado, se puede iniciar su transmisión, aunque no haya sido recibido en su totalidad.

La ventaja de este procedimiento es su baja latencia pero tiene por contra, el inconveniente de que al no ser examinado el paquete en su totalidad antes de su reexpedición se pueden propagar errores existentes en el mismo, e incluso fragmentos de paquetes con colisiones, lo que implicará un *slot* innecesario del ancho de banda del segmento receptor y, por tanto, una reducción en las prestaciones del conmutador.

Por otro lado, cuando se transmiten paquetes entre redes de diferentes velocidades, no es posible utilizar este método, ya que, por ejemplo, al enviar un paquete recibido a 100 Mbps, a una red de 10 Mbps, la red receptora no sería capaz de reducir a la suficiente velocidad el paquete y se generaría un error, y viceversa. Es de destacar que esta misma situación, sin necesidad de que exista diferencia de velocidades, se produce cuando la red destinataria esta congestionada o colapsada.

3.4.6.2.Almacenar-transmitir

Cuando se emplea la técnica de almacenar y transmitir (store-and-forward), el conmutador recibe el paquete completo, lo almacena en su memoria interna y lo examina por entero antes de decidir si debe de ser transmitido o filtrado.

El inconveniente teórico es que se requiere una memoria para almacenar los paquetes, así como procesadores y *software* más potente para evitar retrasos (disminuir la latencia), lo que supone un costo y complejidad de diseño mayores. Pero, obviamente, sus prestaciones son mejores al eliminar paquetes erróneos de la red e incluso permitir filtros más sofisticados al poder analizarse el paquete completo Además el argumento de que una latencia menor es mejor no es válido si se tiene en cuenta que muchos de los protocolos de transporte modernos (TCP, NFS e IPX en modo ráfaga) permiten el envío de secuencias de múltiples paquetes consecutivos antes de recibir el reconocimiento de que el primero ha sido recibido adecuadamente; y por lo tanto, no se produce ningún retraso en el envío del siguiente paquete, por no haber llegado la señal de reconocimiento del primero, puesto que el segundo y los sucesivos ya han sido re-emitidos.

Existe multitud de tipos de concentradores que pueden catalogarse como conmutadores, y cada uno de ellos puede decirse que resuelve problemas concretos de la red. Pero fundamentalmente, pueden clasificarse en dos grupos fundamentales: conmutadores de grupo de trabajo y conmutadores de red. Un conmutador de grupos de trabajo (workgroup switch) garantiza la velocidad de la red entre pares de estaciones o nodos. Si la velocidad de los puertos fuente y destinatario es igual, el destinatario debe de estar ocioso (idle) para evitar el bloqueo.

En este caso se soporta una única dirección por puerto, que a su vez es la unidad mínima de segmento; cada segmento tiene por tanto una conexión dedicada con todo el ancho de banda de la red. Por supuesto, se pueden ofrecer puertos con distintas velocidades, como se ha mencionado antes, por ejemplo para servidores y clientes. A los puertos que admiten sólo una única dirección punto final de la red se les denominan puertos privados (private ports). Para la conexión a troncales, en cambio, se requiere un puerto de red estándar, es decir, no limitado a una única dirección de red.

Un conmutador de red (network switch) tiene que garantizar la conectividad a la velocidad de la red entre pares de segmentos de red. Si las velocidades de los segmentos origen y destino son iguales, el segmento destino debe estar en desatento para evitar el bloqueo.

En este caso, a cada puerto del conmutador se suele asociar un grupo de trabajo, por lo general a través de un concentrador, y los nodos del mismo comparten el ancho de banda dentro del mismo segmento. La ventaja evidente, frente a un conmutador de grupos de trabajo, es su menor costo por nodo final, pero su desventaja es limitar el ancho de banda que queda

repartido entre todos los nodos de un segmento y, obviamente, su instalación es más complicada por la necesidad de equilibrar la carga de trabajo de la red en cada segmento

Muchos concentradores modulares de altas prestaciones ofrecen una característica singular, basada fundamentalmente en *software*, que se denomina conmutación de puertos (port switching), y que coincide en parte con la estrategia de conmutación de los conmutadores, aunque no necesariamente emplean la misma tecnología. El *hardware* está preparado para dividir el concentrador en varios segmentos *Ethernet* y asignar a cada segmento un puerto o grupo de puertos. La ventaja de estos dispositivos es evidente, dada la capacidad y flexibilidad que supone para el administrador del sistema poder administrar puertos mediante un *software* de control, en función de repartir la carga de trabajo de los segmentos de la red, cambiar a un usuario de grupo de trabajo, etcétera, todo ello sin necesidad de cambiar físicamente el cableado de la instalación.

3.4.7. Tecnología de Conmutadores

Los conmutadores son dispositivos sofisticados que permiten reducir la saturación de las redes a base de << segmentar>> las mismas, reduciendo el número de puestos o nodos conectados a cada segmento, y ampliando el ancho de banda disponible para cada uno de ellos.

Para lograr este objetivo se emplea un *hardware* complicado, acompañado de un *firmware* muy específico, capaces de procesar a gran velocidad todos los paquetes que pueden llegar por los diferentes puertos y evitar la pérdida de alguno de ellos, y al mismo tiempo reproducirlos sólo en los puertos destinatarios adecuados. Para ello, diferentes fabricantes emplean arquitecturas propietarias, a menudo con bastantes puntos de coincidencia, dado que los objetivos son idénticos, y a veces con características específicas que los hacen muy diferentes, y que marcan por tanto las diferencias de prestaciones entre unos y otros equipos.

En estas líneas se van a estudiar dos sistemas muy diferenciados, empleados por dos fabricantes de equipos muy diferentes entre sí, como ejemplos diversos de sofisticadas soluciones a idénticos problemas.

3.4.7.1.Arquitectura de memoria compartida

El primero de los sistemas, denominado arquitectura de memoria compartida (shared memory architecture), desarrollado por **Alantec**; se fundamenta en un diseño simple, eficiente, flexible, gestionable y, sobre todo, potente.

Alantec fue creada en 1987 con el objetivo claro de ayudar a las redes colapsadas a incrementar sus prestaciones sin modificar sus estructuras básicas ya existentes. Su producto, denominado PowerHub, consiste en una completa familia de conmutadores/concentradores inteligentes, basados

fundamentalmente en *software* con algoritmos de enrutamiento multiprotocolo. Además, una de sus características fundamentales es que permiten soportar gran variedad de redes: *Ethernet*, Fast *Ethernet*, Full Duplex *Ethernet*, Full Duplex Fast *Ethernet*, *FDDI* y *ATM*.

El modelo de conmutador empleado por **Alantec** implica que todos los paquetes recibidos, independientemente de su destino, se depositan en una memoria compartida, donde serán examinados por el procesador y desde donde se tomarán las decisiones de reenvío. Por lo tanto, el *software* **PowerHub** puede transmitir un paquete usando cualquier técnica de bridging, routing o filtrado que pueda ser expresada mediante un algoritmo de programación.

La simplicidad del esquema de memoria compartida incrementa la eficacia del *hardware* y el *software*, ya que facilita su estructura de pipeline y el método de conmutación de paquetes, en el que no se pierde ancho de banda a causa de tiempos asociados con arbitraje, carga de trabajo y similares, que con frecuencia van asociados a estructuras de bus compartido. Además, los paquetes recibidos en la memoria compartida pueden ser reenviados directamente hacia sus destinos, sin necesidad de copiarlos, aún en casos de paquetes broadcast y multicast.

La flexibilidad le es inherente por varias razones. La memoria compartida puede emplearse de forma jerarquizada para proporcionar inteligencia distribuida en sistemas de alto ancho de banda, lo que naturalmente soporta modelos de multiproceso que pueden ser construidos con una gran variedad de tecnologías de memoria, en función de puntos de vista de costo/prestaciones.

Las arquitecturas de memoria compartida son un camino directo para proporcionar muchas características de gestión de redes. Dado que cada paquete es examinado, y que cada decisión de transmisión es tomada por el propio *software*, se pueden establecer complejas estadísticas, filtros de seguridad y monitoreo de puertos, con suma facilidad. Además. Dichas características no se limitan al *hardware* diseñado, sino que pueden ser incorporadas con posterioridad en función de las nuevas necesidades y experiencias de los clientes.

Por último, la arquitectura de memoria compartida es poderosa: los diseñadores de *hardware* entienden la dificultad del ancho de banda compartido en un entorno determinado, además de su alto precio, por ejemplo en un cableado *Ethernet* o un anillo *FDDI*. Sin embargo, el ancho de banda es más barato en una, por ejemplo en el bus de un "**backplane o circuito impreso**". La arquitectura de memoria compartida de **Alantec** emplea este principio avanzado y da un paso más al respecto, proporcionando el ancho de banda compartido a nivel de circuitos integrados y empleando memorias cache de altas prestaciones.

Se puede reducir el costo de los sistemas al utilizar una interface que posea un procesador de paquetes inteligente, ya que se ganaría potencia en el proceso además de un ancho de banda favorable que se requiere en los buces y la memoria que necesitan los paquetes entre puertos, mientras que la potencia de proceso es fundamental para examinar y modificar las cabeceras de los paquetes transmitidos, uno a uno, permitiendo realizar estadísticas y proporcionar otras funciones de valor añadido.

La arquitectura de proceso de paquetes basado en *software* emplea CPU RISC de muy altas prestaciones, con la ventaja de su excelente escalabilidad y flexibilidad, a un valor efectivo costo/prestaciones

La solución en *software* conlleva ventajas añadidas importantes, como es la posibilidad de actualizar los protocolos, depurar errores, etcétera. El inconveniente puede ser su capacidad de proporcionar las prestaciones adecuadas, lo que se soluciona con un equilibrado y depurado diseño del *hardware*, con CPU distribuidas que suministren potencia en los puntos que lo requieren del dispositivo.

Es importante, como parte de ese diseño equilibrado, que el sistema no pueda ser bloqueado. Ello implica que sea capaz de suministrar un ancho de banda lo suficientemente elevado como para que puedan reenviarse todos los paquetes cuando todos los puertos suministran el máximo tráfico de que son capaces, en función del tipo de red al que están conectados. Este punto de tráfico ocurre por lo general cuando los paquetes son de la longitud máxima permitida, ya que en dicho caso la carga de protocolo es minimizada .

Los dispositivos de **Alantec** se han diseñado siguiendo la norma de que no sean configurables, aunque en algunos casos el propio usuario puede configurarlos para que lo sean, por ejemplo como una forma de reducir el costo del sistema por puerto cuando no se desea que todos los segmentos puedan operar a su velocidad máxima.

Todos estos dispositivos emplean el método *store and forward* forzosamente - ya que permiten conmutar tráfico entre puertos de diferentes velocidades -.

Además de la memoria compartida, es una característica importante de estos dispositivos el uso de unidades procesadoras distribuidas, diseñadas en función de las necesidades de cada tipo de interfaz física, con diferentes topologías y procesadores de diferente potencia, distinto ancho de banda o tamaño de la memoria compartida, lo que conlleva sus evidentes posibilidades de ampliación según las necesidades de cada caso. Se emplean varias unidades de procesadores de entrada/salida y varias unidades procesadoras que ejecutan los algoritmos de proceso de paquetes y de gestión *SNMP*.

En el caso de los productos **PowerHub** actuales, cada conmutador tiene un ancho de banda de 800 Mbps, con transferencias en modo de palabras o bloques, siendo el número de canales variable en función del modelo.

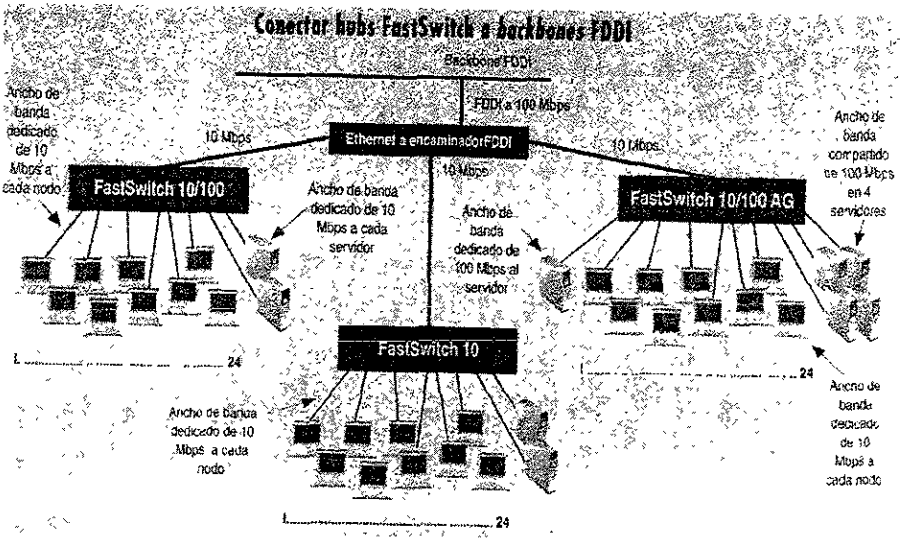


Ilustración 3-4 Esquematización Básica de Soluciones para Redes con Switches.

(Fuente: Alantec Tecnologies Corp.)

La arquitectura del *software*, o más bien el *firmware*, tiene que ser capaz de gestionar las diferentes fuentes de carga de trabajo.

3.4.7.2.Prestaciones de los conmutadores

Dado que un conmutador pretende solucionar los problemas de ancho de banda real disponible en la red y por tanto evitar sus congestiones importante determinar sus prestaciones, que se pueden analizar en función de tres parámetros fundamentales: ancho de banda puerto a puerto, ancho de banda total y latencia. Las redes *Ethernet* a 10 Mbps son capaces de transmitir 14 880 paquetes por segundo (PPS) para paquetes con un tamaño mínimo de 64 bytes. Esta velocidad, que se denomina velocidad de la red o velocidad del cable (wire speed), es teóricamente la máxima alcanzable.

Un conmutador, e incluso un puente o conmutador que sea capaz de sostener dicha velocidad en una conversación entre dos de sus puertos ofrece las máximas prestaciones posibles en este sentido. Nos indica que su combinación de *hardware* y *software* es capaz de ser tan eficiente como es el propio cableado en sí mismo.

Bien sea medida en Mbps o en *PPS*, el ancho de banda total es la máxima velocidad a la que pueden transmitirse los paquetes a través del conmutador y, por tanto, recibirse y enviarse por los puertos del mismo. En un conmutador con 24 puertos.

Ethernet (10 Mbps), su ancho de banda total debe de ser igual a la suma del máximo número de conexiones virtuales que pueda establecer a la velocidad de la red (o velocidad del cable), es decir 120 Mbps (10 Mbps x 12 conexiones virtuales), o bien 178.560 *PPS* (14.880 x 12 conexiones virtuales). Este seria el caso de un conmutador porteable internamente (non-blocking).

La latencia (latency) consiste en la demora en el tiempo transcurrido desde la recepción de los datos en un puerto y su reexpedición al puerto de destino. En general, se toma como punto de referencia el primer *bit* de cada paquete. La latencia depende fundamentalmente del tiempo requerido por el *hardware* y *software* del conmutador para identificar la dirección de destino.

Una baja latencia incrementa las prestaciones, especialmente en redes que utilizan protocolos de señalización y reconocimiento (handshaking), en los que todas las transferencias de datos se implementan en secuencias de transmisiones de paquetes individuales, cada uno de los cuales es reconocido (acknowledged) individualmente por el destinatario.

La baja latencia es menos importante en redes que emplean protocolos de *windowing* >> Ventana-Corredera <<, ya que implementan las transferencias de datos en secuencias de múltiples paquetes, reconocidos como un grupo por el receptor.

3.5. Aplicaciones y productos.

A lo largo de los párrafos anteriores ya se han esbozado las aplicaciones básicas de los conmutadores que se pueden sintetizar en: sustitutos de bridges y routers, sustitutos de concentradores en redes congestionadas, sustitutos de concentradores en grupos de trabajo, conexión de grupos de clientes a servidores, conexión de grupos de servidores a grupos de clientes e interconexión de múltiples concentradores. Los fabricantes que hoy en día ofrecen conmutadores en el mercado mexicano son: **Alantec**, **Artel**, **Cabletron**, **Cisco**, **Grand Junction**, **Networks**, **Interphase**, **Kalpana**, **Lannet**, **Lantronix**, **SMC**, **UB**, y **3Com**. El abanico de productos ofrecidos incluye una variedad imposible de enumerar en estas líneas.

Lo que sí cabe señalar es que algunos fabricantes ofrecen soporte en sus dispositivos de conmutación para redes *FDDI*, *ATM*, Fast *Ethernet*, Full Duplex *Ethernet*, Full Duplex Fast *Ethernet* y *Token-Ring*, entre otras, bien como puertos independientes, o incluso como conmutación de dichos tipos de redes.

Sin duda, el soporte multitecnológico y la modularidad primarán los futuros productos que adopte el mercado, aunque se puede afirmar que algunos de

ellos han hecho ya su aparición y están despuntando con fuerza frente a otros productos de gama baja y prestaciones inferiores.

Es fundamental destacar el hecho que existen en el mercado *bridges* y *routers* multipuerto cuyas prestaciones y funcionalidad pueden llegar a ser equivalentes a las de verdaderos conmutadores, especialmente para pequeños grupos de trabajo o redes no excesivamente grandes.

Se puede esquematizar las ventajas clave de la conmutación en los siguientes puntos: incremento de las prestaciones de la red, proporcionando conexiones de alta velocidad entre distintos segmentos y nodos de la red, sin límite a pesar del incremento en el número de usuarios; reducción de las colisiones, especialmente al existir la posibilidad de dedicar un segmento a cada nodo de la red; bajo costo, dado que no se requiere modificar el *hardware* y cableado de todos los nodos de la red; mejora en la seguridad de la red, al transferir los paquetes sólo a sus direcciones de destino y al poder establecer filtros más específicos; bajos tiempos de respuesta de la red, totalmente predecibles, lo que permite incluso aplicaciones multimedia en redes que inicialmente no estaban preparadas para ello.

Se puede predecir sin duda alguna el incremento en el uso de este tipo de dispositivos, cada vez más sofisticados y modulares en todo tipo de redes; e incluso para un futuro no muy lejano se puede avanzar la desaparición de *bridges y/o routers*, tanto locales como remotos, puesto que los conmutadores pueden cumplir perfectamente y con creces, todas sus funciones.

4. Tecnología y arquitectura de un backbone

4.1. Arquitectura de backbone colapsado.

El Backbone[8] Colapsado (o backbone concentrado) es un sistema para conectar diferentes segmentos de red.

Hoy en día al trabajar en la implementación de un nuevo sistema de redes inmediatamente nos percatamos de las limitaciones del cableado (500 metros en *ThickCoaxial*, 100 metros en par trenzado, etc.) y de los equipos. Siempre surge la necesidad de interconectar una red local de manera general, como las que aún existen en diversas instituciones de la UNAM, que requiere de interconectarse a los campus por diversos segmentos de la red a través de *ruteadores* no muy evolucionados se deben basar en conexiones a través de un Backbone colapsado.

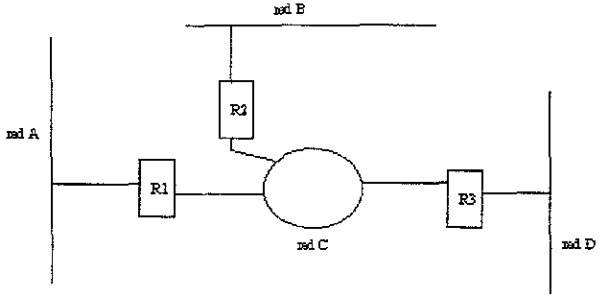


Ilustración 4-1 Backbone colapsado.

Los datos por medio de este sistema pasan a través de muchos *ruteadores* que se encuentran distribuidos físicamente, como lo podemos ver en la Ilustración 4-1

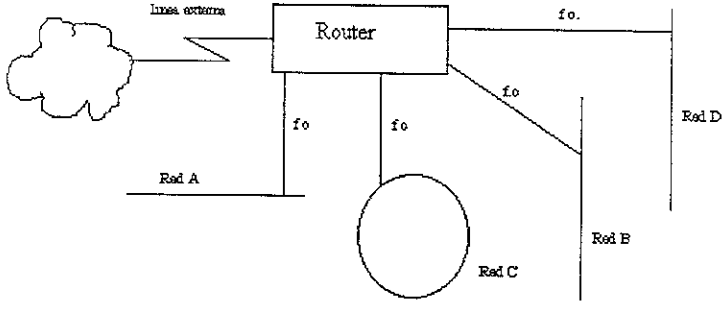
Para que un *host* de la red **A** mantenga una sesión con otro de la red **D**, los datos deben atravesar por dos ruteadores, se trata de un diseño descentralizado. En estos entornos, la detección de errores puede llegar a ser muy dificultosa

Así mismo estos diseños suelen estar orientados a conectar redes de un determinado ancho de banda (**A**, **B**, **D**) a otras con mayor ancho de banda (red **C**), p.e. *FDDI o Token Ring* a 16 Mbps, llamando a esta última *Backbone*.

[8] Columna Central de Red; aunque otros autores suelen definirlo como espina dorsal, de su traducción al español.

Con la llegada de los *hubs* de tercera generación, la fibra óptica y la gran evolución experimentada por los *ruteadores*, se llegó a una arquitectura de interconexión mucho más flexible: el *backbone concentrado* (C B.).

El C.B. consiste básicamente en un conjunto de segmentos de red interconectados mediante un *ruteador* de altas prestaciones que, además, se encarga de las conexiones externas Gracias a la flexibilidad del cableado estructurado, los *hubs* de tercera generación y las conexiones de fibra, ahora se evitará utilizar múltiples *ruteadores*. La figura del *Backbone* es sustituida por el *backplane* del *ruteador*.



fo.: fibra óptica

Ilustración 4-2 Ruteador en backplane.

Las principales ventajas del C.B. son:

* *Backplane* del *ruteador* de alto rendimiento: de 300-600 Mbps a 1 Gbps.
* Menor costo: sólo tenemos un *ruteador*, tenemos menos interfaces de red en total.
* Administración y control centralizados.
* Las sub-redes de computadorás se conectan al ruteador a través de fibra Esto hace que las distancias entre las sub-redes de computadoras y el *ruteador* puedan ser muy grandes.

Por otra parte al utilizar un *ruteador* multiprotocolo en el diseño de una red podemos tener.

* Soporte multiprotocolo, segmentación de la red en redes lógicas.
* Múltiples tipos de redes de área local (Ethernet, Token-Ring, FDDI).
* Interfaces de conexión al exterior.
* Segmentación de tráfico.
* Mecanismos sofisticados de filtrado de tráfico

Los *ruteadores* (**Cisco**, **Wellfleet**, etc) que se vienen fabricando desde el año 1991 cumplen con los dos requerimientos claves a la hora de construir *Collapsed Backbones*: disponibilidad alta (reconfiguración dinámica, cambio en caliente de interfaces, redundancia en el hardware, etc.) y rendimiento alto (soporte para un elevado número de conexiones, backplane de alta velocidad, arquitectura multiprocesador, etc.).

Dentro de esta arquitectura los *ruteadores* son los que proporcionan la conectividad entre los diferentes segmentos, mientras que los *hubs* proporcionan la conectividad del puesto de trabajo.

4.2. *Ejemplo - Topología de red en un Campus Universitario*[9]

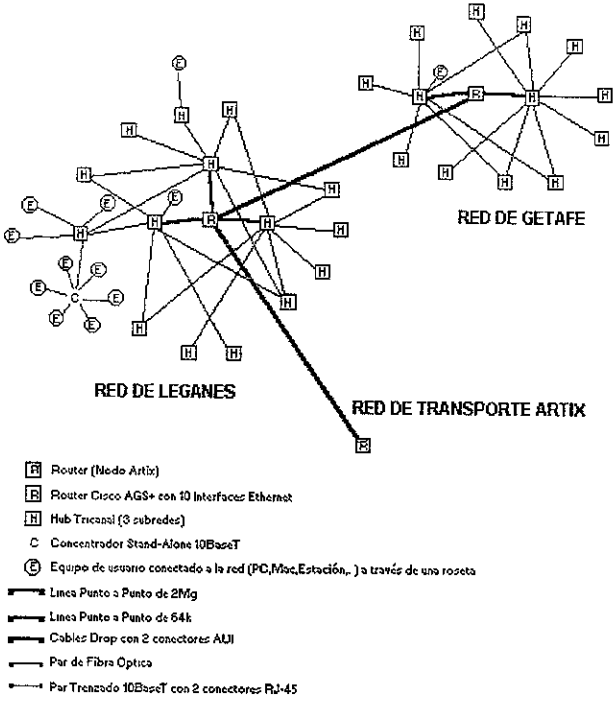


Ilustración 4-3 Nodos de la red de la Universidad Carlos III

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

Campus De Leganes

En Leganes, el repartidor principal y los secundarios se unen mediante cuatro pares de fibra óptica, se usa un par por cada segmento de red. Se podría llevar hasta cuatro segmentos *Ethernet* independientes desde el Centro de Cálculo, o bien usar algunos como enlaces de rescate. La capacidad de transmisión de Ethernet es de 10Mbps, el FDDI la supera con 100Mbps. Y está prevista una futura migración, la cual se puede implantar sobre un soporte de dos pares de fibra óptica en anillo, además cada estación se conectará a uno ó a los dos anillos a la vez.

[9] El Campus Leganes, corresponde a la Universidad Carlos III, en España La topología aquí presentada es parte de la redistribución efectuada a principios de 1994 en el edificio de Cálculo. El estudio presentado aquí fue realizado por el Centro de Calculo de dicha Universidad

En este caso habría que dejar instalado un anillo de fibra de dos pares y reconventir la estrella a anillo, haciendo los puentes convenientes. Con lo que se consigue el soporte físico para una o dos redes FDDI (dos anillos de dos pares cada uno).

Cada edificio tendrá una sub-red en Ethernet que accederá al anillo de fibra a través de un router a FDDI. El problema de esta reconversión es que las interfaces FDDI de los dispositivos que existen en el mercado son caras y escasas, y será mejor en este caso esperar a que la situación del mercado aconseje este cambio.

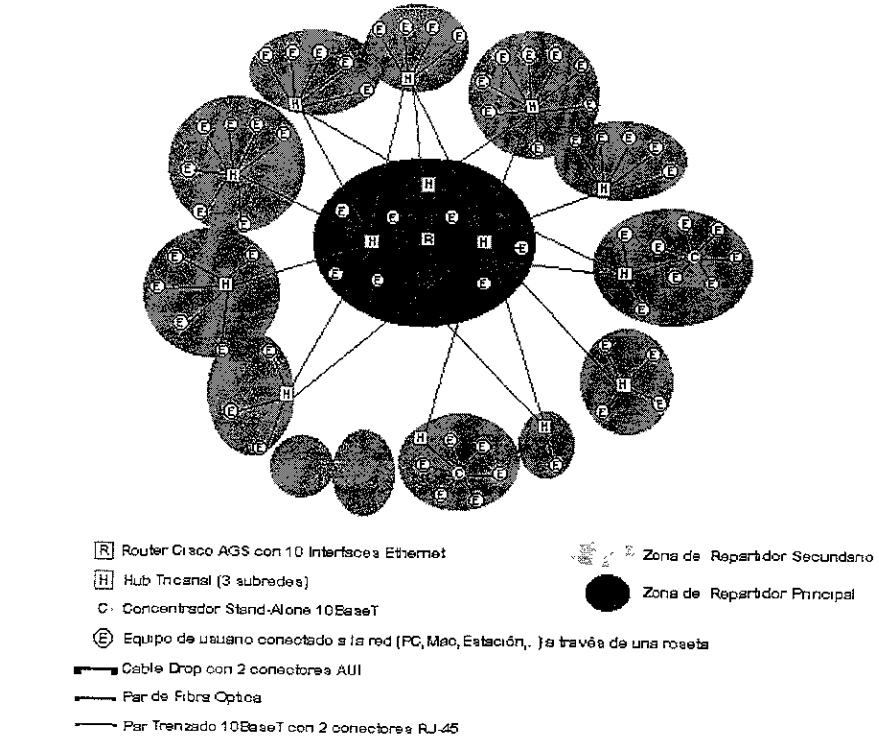


Ilustración 4-4 Nodos de la red del Campus Leganes.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

El equipo de interconectividad en Laganes consta básicamente de:

- 1 Repartidor Principal ubicado en el Centro de Cálculo (Unidad de Matemáticas).
- 13 Repartidores Secundarios distribuidos por todo el edificio (Unidad de Rectoría)
- Una roseta como mínimo por despacho.
- Tendido de Fibra Óptica del Repartidor Principal a los Secundarios
- Tendido de Par Trenzado 10BaseT de los repartidores secundarios a las rosetas

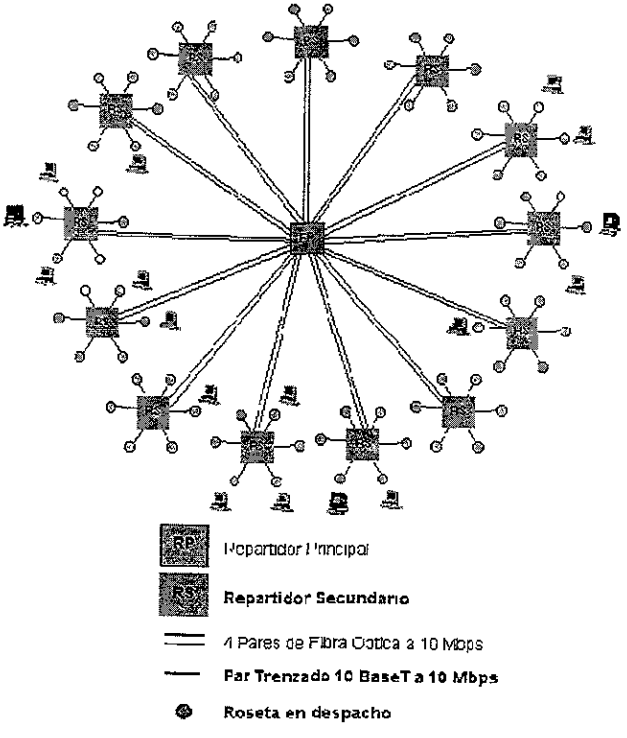


Ilustración 4-5 Esquema de Distribución de la Red.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

A Nivel Interno (Lógico)

Topología a nivel físico.

Es una estrella *Ethernet* con arquitectura del *Backbone Colapsado.*

Cuenta con los siguientes equipos de interconexión: - un *ruteador* de altas prestaciones, que permite tener en lugar de un único segmento, tener un conjunto de segmentos de red (sub-redes). - una serie de *hubs* ubicados en los repartidores, etc.

Emplea dos tipos de cableado: Fibra Optica (FDDI) y Par Trenzado (UTP) 10BaseT. Utiliza el sistema de Cableado POUYET.

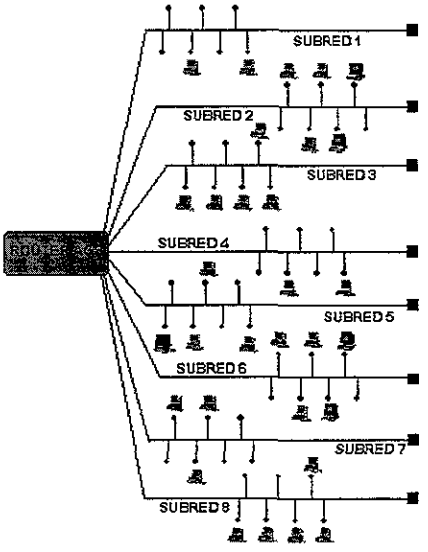


Ilustración 4-6 Sub-Redes que Integran al Campus.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

Es una red *Ethernet* a 10Mbps dividida en sub-redes, pero no es una *Ethernet Conmutada.*

Utiliza el protocolo *CSMA/CD.* Como es válido en la mayoría de las oficinas de un campus universitario, esto resulta adecuado en cierta forma, porque no existe simultaneidad en la red. Es decir, normalmente se tienen 100 maquinas con conexión a red, simultáneamente unas 20 se conectan a la vez. Debido a

que los usuarios se conectan a diferentes horas, y es casi imposible que se conecten a la vez en un nodo al mismo tiempo.

Actualmente la red general se conforma por 8 sub-redes. Esto implica que el ancho de banda real (el que se tiene en un instante determinado) ya no es de 10 Mbps, es de 10 Mbps en cada sub-red, y como podemos ver en la Ilustración 4-6, poseen 8 sub-redes x 10 Mbps = 80 Mbps. El ancho de banda que se demanda al *ruteador AGS* disponible es de 80 Mbps (esto es el ancho de banda a lo largo del tiempo, teniendo en cuenta las colisiones).

Si bien se puede notar que se recorta cuando los paquetes deben de ser encaminados por el *ruteador:* hay un tiempo de espera n en las colas, lo que mejora notablemente al disminuirse el número de colisiones.

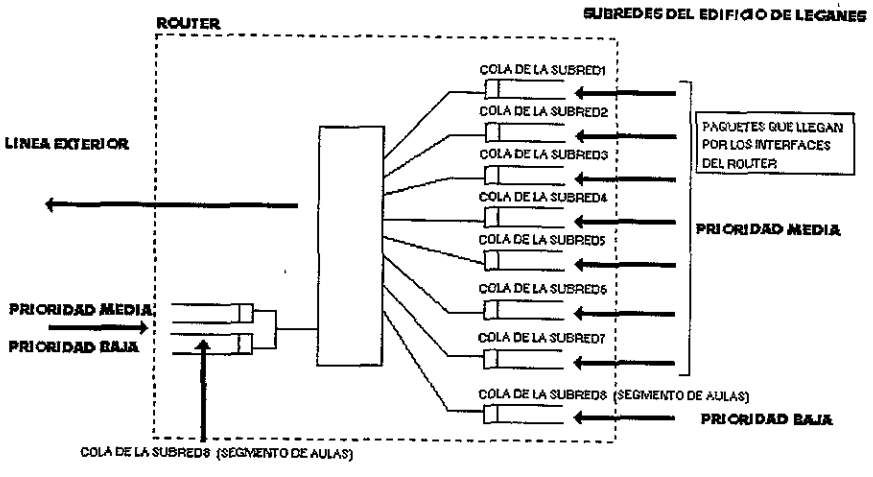


Ilustración 4-7 Esquema del Tráfico de Datos.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

El *ruteador AGS* tiene las siguientes características:

⇒ Posee una arquitectura multibus.

⇒ Está basado en un procesador 68040 de Motorola.

⇒ Incluye 16 Mb. De memoria. Esta memoria se encarga de la gestión de colas. Las colas se encargan de conmutar los paquetes *Ethernet.*

⇒ Utiliza el algoritmo de enrutamiento IGPR.

Puede utilizar dos criterios de prioridad:

⇒ Por Interfaces (Actualmente se emplea)

⇒ Por Protocolos.

4.2.1. Arquitectura de cableado polivalente (enrosetado)

Para instalar la red se necesita precablear[10] los edificios siguiendo un Plan de Distribución. Una vez efectuado el precableado, y sin ninguna operación adicional, se podrá:

- Conectar una terminal de cualquier tipo
- Uniformar, simplificar y sistematizar los modos de cableado.

El Plan de Distribución más común es el sistema SCP (Sistema de Cableado Polivalente).

El sistema SCP se basa en la existencia de locales de repartición en cada piso, pasillo, edificio, etc., cada uno de los cuales alojará un sub-repartidor. Estarán convenientemente situados, más o menos en el centro respecto a los despachos que tienen que dar servicio y próximos a las columnas verticales de distribución, de existir.

Todos los puestos de trabajo tendrán el mismo tipo de cableado, sin ninguna interrupción, y se montarán en topología de estrella, enlazándose al sub-repartidor a través de cables individuales.

4.2.2. Local de sub-repartición: repartidor

En él convergen todos los enlaces locales informáticos, ofimáticos, y los enlaces de la red telefónica (Dial-Up) que dan servicio a las oficinas situadas en un radio de 100 metros. En él se realizan la función de conexión y se establecen los enlaces con las redes de nivel superior. Pueden llegar a dar servicio a un máximo de 100 puestos de trabajo: su gestión será tanto más eficaz cuanto mayor sea el número de conexiones que soporte.

Los elementos del local de repartición se dividen en tres subconjuntos:

- Bastidores de Repartición. Sobre ellos se efectúa el montaje de los distintos tipos de módulos de conexión y se tienden los cables.
- Chasis de Repartición. Sirven de soporte para los distintos tipos de equipos electrónicos (repeats, hubs, gateways, bridges, switches).
- Módulos de Repartición. Son los módulos que se instalan en los *railes* de los chasis y bastidores de repartición. Se encuentran en los distintos locales de repartición y sirven para efectuar las conexiones de los cables procedentes de los puestos de trabajo, las interconexiones de los locales de repartición, y las conexiones de los equipos electrónicos.

[10] Precablear un edificio consiste en tender, en toda su extensión, una red de cables cuya disposición resulte suficiente en calidad, cantidad y flexibilidad.

Para diferenciar los distintos tipos de conexión están fabricados por código de colores:

- ◊ Módulos Azules. De conexión con los puestos de Trabajo (Vienen de las Rosetas)
- ◊ Módulos Amarillos. De conexión de equipos electrónicos, los cuales se agruparán en bloques independientes y se identificaran según el equipo al que pertenezcan (ejemplo: hub, repeat).
- ◊ *Módulos Verdes. De conexión con otros locales de repartición* (Por ejemplo: Conmutador Telefónico).

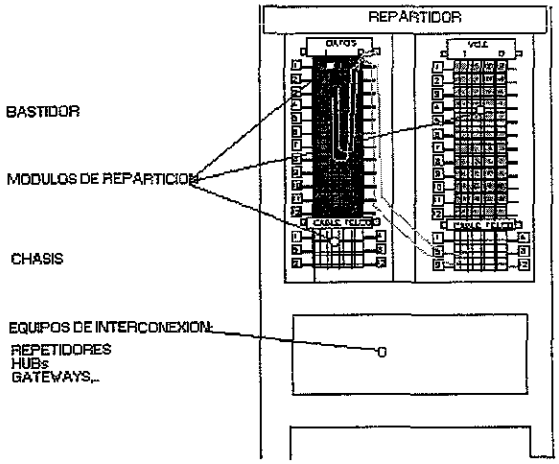


Ilustración 4-8 Código de colores para la unidad de repartición

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

5. Arquitectura de redes de alta velocidad

5.1. Ethernet conmutado

Cuando una red *Ethernet* empieza a presentar problemas de desempeño, una solución común es dividir la red en segmentos separados por puentes, procurando reducir el tráfico entre segmentos al mínimo. Entre más segmentada esté la red, mayor será su desempeño pues cada uno de los segmentos tendrá menos estaciones y, presumiblemente, menos colisiones. De esta manera, parece conveniente colocar los elementos más utilizados en la red (por ejemplo los servidores de archivos) en segmentos independientes[11].

El problema con esta solución es que para que sea óptima, se debe empezar por evitar el tráfico innecesario al cruzar segmentos intermedios, cada segmento en la red debería conectarse con todos los demás a través de un puente distinto. En esta configuración el número de puentes requerido crece de acuerdo a una función cuadrática del número de segmentos, resultando totalmente incosteable para redes medianas y grandes.

Debido a esto las redes *Ethernet* cuentan hoy con la tecnología de la arquitectura de *Ethernet Conmutado,* que forma parte de las actuales tendencias en tecnologías *LAN* de alta velocidad. No es tan nueva como *Fast Ethernet* o 100VG *AnyLan.* Simplemente es una forma de segmentar dinámicamente una *LAN.*

La distinción conceptual básica entre la *Ethernet* ordinaria y *Ethernet Conmutado* es que a diferencia del método CSMA/CD (Carrier Sense Multiple Access with collision Detection) de controlar el tráfico en la red entre los puntos A y B, el *Ethernet Conmutado* es un método de transmisión punto-a-punto que utiliza un dispositivo de conmutación para proporcionar vías dedicadas al tráfico sobre la marcha.

Este dispositivo de conmutación es un *EtherSwitch* que básicamente realiza los siguientes procesos:

- Convierte cada uno de sus puertos en un segmento de *LAN* dedicado
- Maneja el tráfico intersegmentos (inter-puertos) vía una matriz de Conmutadores (*Switches)*
- Realiza sólo una conexión entre los nodos de la red cuando es necesario

Un ejemplo de dispositivo *EtherSwitch* es el EtherSwitch EPS-2015RS de **Kaplana** distribuido por la empresa **ANIXTER**. Con 15 puertos, gestión *SNMP*, protocolo *Spaning Tree*[12], posibilidad de crear hasta 7 redes virtuales, filtraje de direcciones que permite a los administradores aislar determinados dominios o

[11] Glasgal, R., "Life in the Fast LAN", LAN Technology, Vol. 8, No. 9, July 1992, pp. 56- 68.
[12] V. Administración de redes, cap. 10 pag. 146

usuarios y *Etherchannel* que proporciona conexiones de hasta 140 Mbps. Cuesta cerca de 90,500 pesos. Se puede encontrar modelos más económicos cerca de los 39,600 pesos, con inferiores características: 7 puertos, *full duplex*, *SNMP*, etc.,

Para aprovechar las ventajas de la segmentación sin tener que introducir un número muy grande de puentes se creó el *Ethernet conmutado*, que ofrecerá una mejora de prestaciones en una *LAN* sólo en determinadas condiciones:

- Si el uso de la red es superior a un 35 por ciento.
- Si la respuesta de la red es lenta.
- Si en la red se utilizan dispositivos que demandan un amplio ancho de banda como estaciones de trabajo o servidores.

En esta tecnología la segmentación se realiza por software en un concentrador, sustituyendo los puentes por una matriz de conmutación de muy alta velocidad a la que se le da a veces el nombre de Arquitectura de backbone colapsado.

El *Ethernet conmutado* sustituye al *Hub*[13] de 10BaseT por un concentrador de conmutación que no envía las tramas recibidas hacia todos sus puertos, sino únicamente al puerto destinatario. A cada puerto del concentrador de conmutación, o conmutador *Ethernet*, pueden conectarse segmentos (compartidos) 10Base2, 10Base5 o 10BaseT, o conectarse estaciones de trabajo individuales.

Debido a que la conmutación se realiza a muy alta velocidad, se pueden tener comunicaciones entre distintos puertos simultáneamente, aumentando de esta manera el desempeño total de la red.

Un concentrador de conmutación con un *backbone* de 100 Mbps y 20 puertos puede en teoría ofrecer un desempeño muy cercano a 100 Mbps si consideramos que 10 de los puertos pueden estar enviando información a 10 Mbps hacia los otros 10 puertos simultáneamente.

El concentrador de *Ethernet conmutado* realiza funciones de puenteo (Brinding), incluyendo el aprendizaje de direcciones. Sin embargo, a diferencia de los puentes que almacenan las tramas y luego las reenvían, en los concentradores de *Ethernet conmutado* el inicio de una trama puede retransmitirse sobre el puerto de salida correspondiente antes de que se termine de recibir completamente la trama. Con esto, los conmutadores *Ethernet* pueden introducir retrasos de conmutación del orden de 40 microseg, que es mucho menor a los 1200 microseg. Introducidos por un puente típico[14].

[13] Repetidor multipuertos (concentrador)
[14] "Using the Model 3328 Ethernet Switch Engine", SynOptics Communications Inc, December 1993.

Con *Ethernet conmutado* se puede aprovechar toda la infraestructura de red instalada. Los fabricantes recomiendan utilizar el concentrador de conmutación separando en puertos distintos los nodos más utilizados.

Para conectarlo con 10BaseT se utilizan dos líneas UTP (par trenzado no blindado) entre el dispositivo y el puerto del concentrador; mientras se transmite sobre un par, se escucha en el otro para detectar colisiones. Si se conectara un único dispositivo a cada puerto de un concentrador de *Ethernet conmutado*, no existirían colisiones y se podría utilizar un par para transmitir y otro para recibir de manera simultánea. Esto es precisamente lo que hacen los productos full duplex de *Ethernet*.

Debido a que la operación de segmentación se realiza por software, así como por su capacidad de configurar los puertos para permitir o inhibir conexiones con otros puertos, varios fabricantes han llamado a estas arquitecturas Redes virtuales.

5.2. Ethernet isocrono

A diferencia de lo que ocurre en la transmisión de datos, la transmisión de voz o vídeo digitalizados a través de una red local puede verse seriamente afectada por la variabilidad con que pueden llegar mensajes sucesivos de una misma transmisión. Por ejemplo, el primer paquete puede tardar 200 ms en llegar a su destino, el segundo 20 ms, el tercero 130 ms, etc. Este efecto puede producir vibraciones en la imagen de vídeo o falta de sincronía entre la imagen y el sonido. Al tipo de información que no admite retrasos variables en su transmisión, se le llama tráfico isocrono.

El *Ethernet*, con un protocolo de acceso por competencia, no es una red adecuada para transmisión de tráfico isocrono. Ni siquiera lo son *Token Ring* o *FDDI* que tienen un protocolo determinista, pues éste sólo garantiza un retraso máximo y puede existir gran variabilidad en los intervalos de llegada de los datos.

Ante el auge informático que están despertando las aplicaciones multimedia, **National Semiconductor Corporation** desarrolló una solución conocida como *Ethernet isocrono* (isoENET o IsoEthernet) que consiste en añadir a *Ethernet* 10BaseT una red isocrona de 6.144 Mbps. Así, *Ethernet isocrono* puede verse como una red de 16.144 Mbps o como dos redes superpuestas, una no-determinista a 10 Mbps para transmisión de datos, y una isocrona a 6.144 Mbps para transmisión de tráfico sensible a retrasos. La parte isocrona puede dividirse en 96 canales B, de 64 Kbps cada uno, de la Red Digital De Servicios Integrados (ISDN).

Para poder aumentar el ancho de banda de la red utilizando el mismo cable de categoría 3 que puede usarse en 10BaseT, sin aumentar las emisiones

electromagnéticas, El *Ethernet isocrono* sustituye la codificación Manchester diferencial por la codificación 4B/5B y NRZI de FDDI[15]

Quizá la mayor virtud de Ethernet isocrono sea su total compatibilidad con la infraestructura de *LAN* (10BaseT) y *WAN* (ISDN) existentes[16]. Si se cuenta con una red 10BaseT, esta tecnología puede ser implantada gradualmente. Primero habría que adquirir el concentrador isocrono que sustituya al antiguo concentrador 10BaseT. Las tarjetas de red de las estaciones se pueden ir cambiando gradualmente conforme más estaciones vayan teniendo necesidades de tráfico isocrono. Además, si se cuenta con acceso a la red digital de servicios integrados por alguna compañía telefónica, el concentrador se podrá conectar a la red *WAN*, extendiendo los servicios multimedia de la red local a sitios geográficamente dispersos. El subcomité 802.9 de la IEEE, que estudia la integración de servicios en redes locales, ha adoptado Ethernet isocrono como una red multimedia para conectividad hasta el escritorio.

5.2.1.1.100BASE-VG o 100VG-AnyLAN

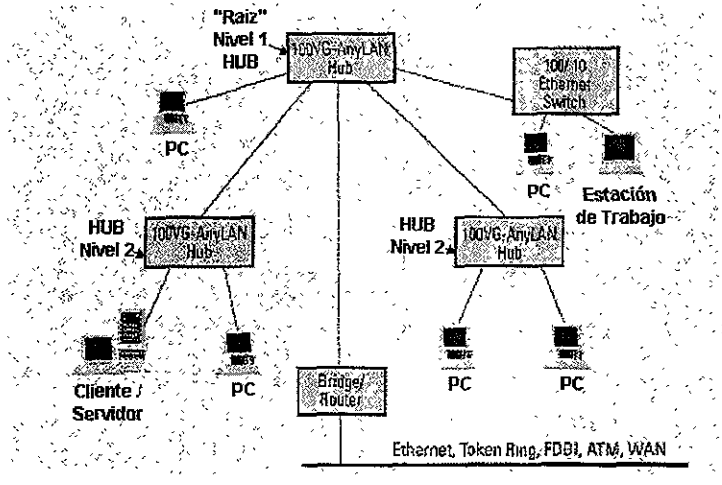


Ilustración 5-1Estructura de Una Red 100VG-Anylan

Esta red inicialmente propuesta por **HP** y **AT&T**, y apoyada además por **IBM**, **Proteon**, **MicroElectronics** y **Ungermann-Bass**, está en proceso de estandarización ante el subcomité 802.12 de la IEEE. Fue diseñada con dos objetivos fundamentales:

[15] Mejía, M., "FDDI: una Red Local de Alta Velocidad", Soluciones avanzadas, Año 1, No. 4, Julio-Agosto 1993, pp. 27-30.
[16] Biery, R., "Isochronous Ethernet and its Potential to Support Multimedia Networking", Telecommunications, April 1994, pp. 63-68.

1) Aprovechar la infraestructura de cableado que muchas empresas tienen instalado

2) Favorecer aquellas aplicaciones con requerimientos críticos de respuesta en tiempo.

El primer objetivo queda cubierto ya que *100Base-VG* tiene una topología en estrella basada en concentradores, como se observa en la Ilustración 5-1, y utiliza cuatro pares de hilos que pueden ser UTP de categoría 3 (categoría de voz, de ahí el término VG) o categoría 5 (categoría de datos), STP (par trenzado blindado) o bien fibra óptica. La información primero se codifica transformando 5 bits en 6 símbolos (5B/6B) y después éstos se transmiten con señalización NRZ distribuidos en los cuatro canales pues la comunicación es half duplex.

Para satisfacer el segundo objetivo, esta red sustituye el protocolo de acceso al medio *CSMA/CD* por un protocolo de demanda con prioridad:

Un nodo puede enviar paquetes con prioridad normal o alta. El concentrador sensa de manera cíclica sus puertos para determinar qué estaciones desean transmitir y cuál es su prioridad. Las solicitudes con mayor prioridad son atendidas primero. Cuando se tengan varias solicitudes con la misma prioridad, éstas serán satisfechas en estricto orden secuencial (round-robin).

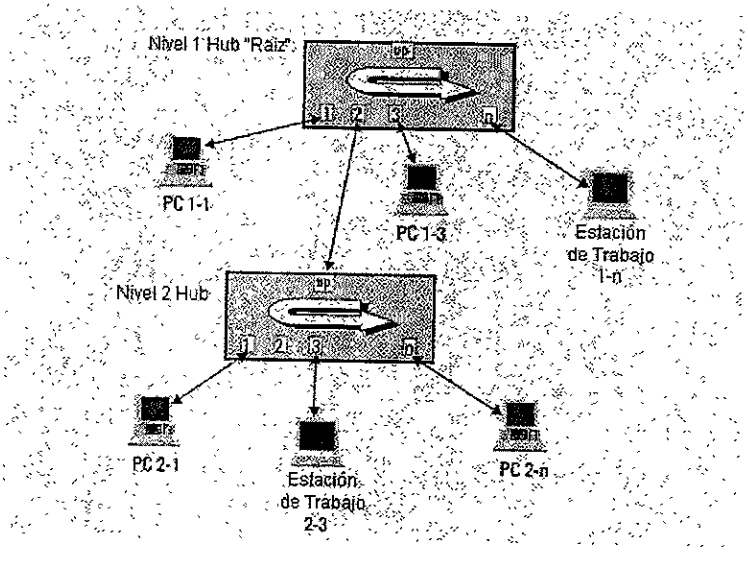


Ilustración 5-2 Funcionamiento de un HUB Round Robin

Para garantizar un comportamiento justo, el protocolo prohibe que una estación transmita más de una trama si existen otras estaciones esperando transmitir con la misma prioridad. Además, si un puerto que trata de enviar un mensaje de baja prioridad ha esperado por más de 250 ms, su prioridad es automáticamente ascendida, evitando así que se tengan mensajes esperando indefinidamente. Los puertos del concentrador que no transmiten información generan una señal especial (idle signal). Cuando el concentrador determina cuál es la siguiente estación a transmitir, retira esta señal del puerto correspondiente, lo que es interpretado por la estación conectada a ese puerto como una invitación para iniciar la transmisión.

Se permiten hasta 3 niveles de concentradores en la configuración. El concentrador base es el que establece el dominio de prioridad. En una configuración multi-concentrador, los puertos son censados en el orden que se muestra en la ilustración 5-2.

La distancia permitida entre una estación y el concentrador, o bien entre concentradores, es de 100 metros. Esta red permite que las estaciones envíen tramas tipo *Ethernet* o tipo *Token Ring* aunque únicamente se permiten tramas de un mismo tipo en un dominio de prioridad. Por lo anterior, a esta red también se le llama *100VG- AnyLAN*.

5.3. 100Base-T (Fast Ethernet)

El subcomité 802.3 coordina la estandarización de 100Base-T[17], que es la evolución de 10BaseT a altas velocidades. 100Base-T utiliza *CSMA/CD* como protocolo de acceso al medio, transmite tramas con el formato *Ethernet* a 100 Mbps y emplea una topología de estrella basada en un concentrador. En la capa física existen tres propuestas diferentes: 100Base-TX, 100Base-T4 y 100Base-FX, que permiten utilizar diferentes medios de transmisión. El subcomité 802.3 ha dicho que los esquemas de señalización serán interoperables en una misma red[18].

Muchas empresas interesadas en desarrollar estas tecnologías formaron una agrupación, **The Fast Ethernet Alliance**, que entre otras cosas ha logrado presionar al subcomité 802.3 para acelerar los procesos de estandarización.

El trabajo original de la propuesta 100Base-TX fue desarrollado por **Grand Junction Networks**, y a ella se han sumado muchas otras empresas como **David Systems, Chipcom, SynOptics, 3Com, Intel, National Semiconductor, DEC** y **Sun**.

[17] Flynn, D., "Fast Ethernet", The 3Com Technical Journal, Vol. 5, No. 4, october 1994, pp 3-10.
[18] Schnaidt, P., "Plug in at 100", LAN The Network Solutions Magazine, Vol 9, No. 3, March 1994, pp.71-79.

El 100Base-TX consolida dos estándares: el protocolo de acceso al medio *CSMA/CD* de 802.3 (cambiando únicamente la duración del intervalo entre tramas de 9.6 a 0.96 µs), y la subcapa física dependiente del medio TP-PMD de *FDDI*. Así, 100Base-TX requiere dos líneas UTP de categoría 5, a través de los cuales transmite con señalización MLT-3, para conectar cada estación al concentrador. Se define una capa de convergencia para mapear la señalización continua full duplex de *FDDI* con el esquema asíncrono half duplex usado en *Ethernet*. También puede utilizarse STP como medio físico.

Por otra parte, la tecnología 100Base-T4 es propuesta con el objetivo fundamental de transmitir información a 100 Mbps a través del cableado que se utilizaba hasta 1992 y que se sigue utilizando para redes de voz y de datos (IVD LANs) a velocidades hasta de 10 Mbps. Este cable es UTP de categoría 3. La especificación sometida a consideración del subcomité 802.3 ha sido desarrollada por **SMC**, **3Com** e **Intel**.

Utiliza cuatro pares **UTP** (de ahí el término T4), tres pares se utilizan para transmitir o recibir la trama (la comunicación es half duplex) mientras que el último par se utiliza exclusivamente como entrada para detección de colisiones. Antes de ser transmitidos, los datos se codifican transformando 8 bits en 6 símbolos ternarios (8B/6T). La información ternaria es entonces transmitida por los canales de datos.

Este modelo es técnicamente similar a la señalización MLT-3, ofreciendo un nivel adecuado de emisiones electromagnéticas.

Por último, la propuesta 100Base-FX emplea dos fibras ópticas múltimodales.

Al igual que en 10BaseT, la distancia máxima entre una estación y el concentrador 100Base-T es de 100 metros. Sin embargo, las reglas de topología permitidas son diferentes en 100Base-T: sólo se permiten dos repetidores, y la distancia máxima de una red es de 205 metros si se utiliza par trenzado y 325 si se emplea fibra óptica[19].

[19] Flynn, D., "Fast Ethernet", The 3Com Technical Journal, Vol. 5, No. 4, October 1994, pp. 3-10.

5.4. Migración de arquitecturas.

La incesante evolución de la tecnología en la globalización de comunicaciones da como resultado que aún las redes de computo más pequeñas al integrarse al Internet tengan que emigrar a topologías más definidas. Un ejemplo es como convertir una determinada Topología Ethernet en una Topología con Ethernet Conmutado. Obteniendo beneficios en el costo de administración y mantenimiento, además de comunicaciones más eficientes y transparentes.

Retomando el ejemplo de las instalaciones en Leganes, se cuenta inicialmente con nueve puestos de trabajo conectados con un *hub Ethernet* estándar, y tres servidores Pentium a 100 Mhz. Además de ocupar 12 puertos del *hub* adicionalmente.

Los primeros tres puestos de trabajo se conectan al servidor **1**, los tres siguientes al servidor **2** y los tres últimos al servidor **3**. No se ha cometido ningún tipo de segmentación.

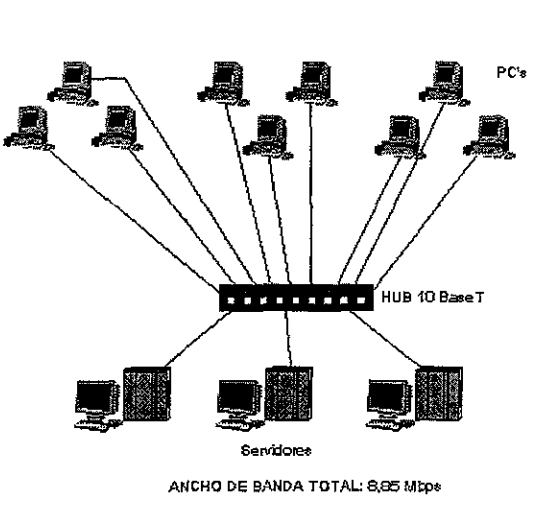


Ilustración 5-3 Red Ethernet 10 Mbits.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

Al margen del número de puestos de trabajo en la red y al margen total de servidores, todos ellos se comunican compartiendo los 10 Mbps que están disponibles para todos, si se añaden más puestos de trabajo peor será el rendimiento de *Ethernet* debido al cuello de botella del ancho de banda propio de la topología. Precisamente al tener todos los dispositivos de la red en el mismo dominio de colisión se supone que el ancho de banda efectivo es de 8,5 Mbps.

Supongamos ahora que añadimos a la topología dos *hubs* más y un *EtherSwitch*. Configuramos los puertos de este último a funcionamiento *half-duplex*. Lo que el EtherSwitch hace es segmentar dinámicamente la red en tres sub-redes separadas.

Cada puerto del servidor crea un segmento de *LAN* propio y separado. Todo el tráfico está dirigido por la matriz de conmutadores internos en el EtherSwitch al nivel del Media Access Control (MCA).

Cada vez que llega un paquete al conmutador, éste toma nota de su dirección de destino y establece una conexión con el destinatario. Al contrario que los *bridges* donde los paquetes tienen que ser almacenados y reenviados, aquí los paquetes siempre se transmiten inmediatamente.

Ahora conseguimos un 300 por ciento de incremento del ancho de banda efectivo, pasando de los 8,5 Mbps hasta los 24,5 Mbps.

Cuando varios segmentos se conectan a la red utilizando *bridges*, un mensaje mandado desde el nodo **A** en el segmento **1** al nodo **B** del segmento **2**, incurre en dos retrasos de entre 100 a 3200 microsegundos. Si se reemplazan los *bridges* por un conmutador Ethernet (etherswitch) y hay un puerto adicional conectado a la red, el mensaje mandado por el nodo **A** en el segmento **1** al nodo **B** en el segmento **2**, verá reducida su latencia en una cifra situada entorno a los 40 microsegundos (ver Ilustración 5-4)

TOPOLOGIA B - ETHERNET CONMUTADO

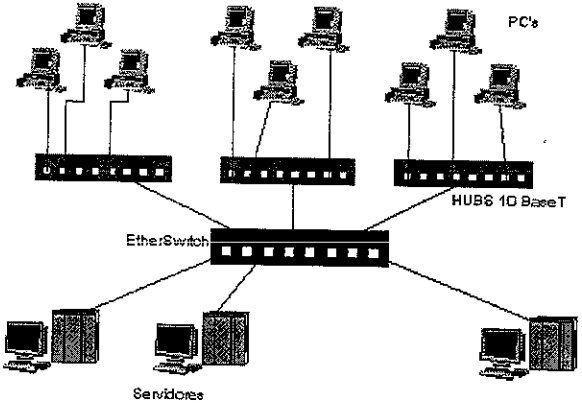


Ilustración 5-4 Ethernet conmutado.

(Fuente: Centro de calculo, edificio Betancurt, Universidad Carlos III Campus Leganes, Madrid España)

5.5. Ampliación de la red y mejora en la gestión

La ampliación de la red se hace adaptándola a las necesidades del momento, para mejorar su gestión e incrementar su robustez y seguridad; estos son algunos puntos gestionables:

- Ampliación de los ruteadores existentes(más interfaces) e instalación de nuevos para disponer de más sub-redes de computadoras y así redistribuir el tráfico, al aumentar los niveles de seguridad existentes.
- Actualización de los módulos de gestión de los *hubs* a versiones avanzadas para permitir un mayor control sobre los cambios de ubicación de los equipos conectados a la red, y dificultar la conexión de equipos no autorizados, para permitir reconfiguraciones más cómodas desde la estación de gestión de red.
- Creación de nuevas sub-redes de computadoras para descargar el tráfico etc.

5.5.1. Ampliación de los ruteadores existentes e instalación de nuevos

Es muy común que al instalar una red sólo existan medios de transmisión (cables. par trenzado y fibra óptica), equipos de canalización (regletas, rosetas, bandejas de fibra, etc.), y lugares físicos (repartidores) para ubicar los equipos de interconexión que se decidieran utilizar.

Al decidir instalar un ruteador de altas prestaciones, da como resultado que en lugar de tener un único segmento, contaremos con un conjunto de segmentos de red (sub-redes de computadoras).

Los equipos de interconexión tienen mucho que ver con la topología de la red. A continuación se presenta las posibles conexiones que se podrían efectuar en un edificio con estas mismas características.

Router con 1 interfaz
Repartidor secundario con 1 concentrador stand-alone (10BaseT)
Ejemplo de 1 red en la zona D

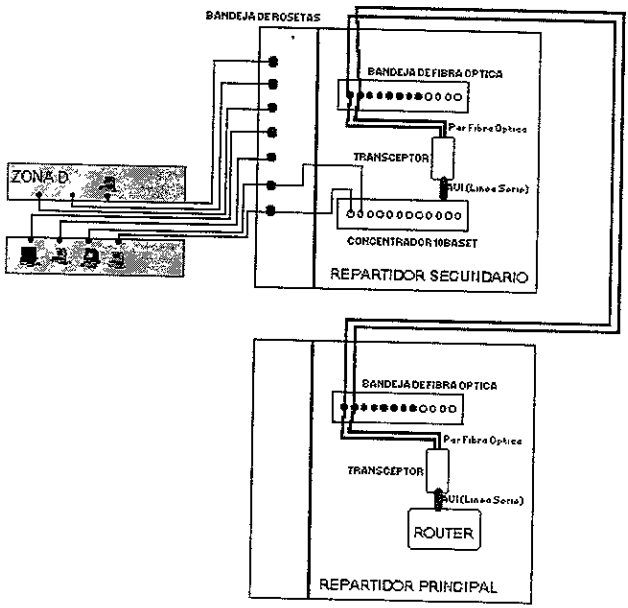


Ilustración 5-5 Conexión de una red en la zona D.

Router con 3 interfaces
.Repartidores secundarios con 1 concentrador stand-alone (10BaseT)
Ejemplo de 1 Subred en la zona D
1 Subred en la zona C
1 Subred en la zona B

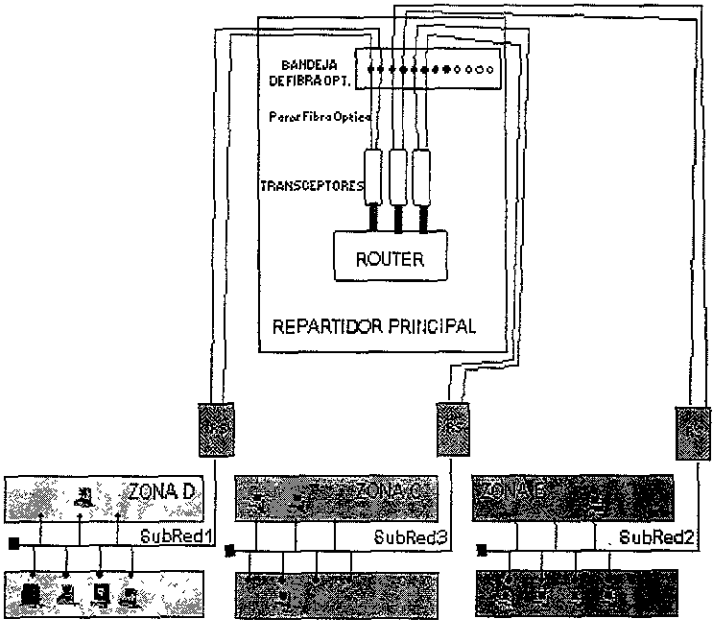


Ilustración 5-6 Conexión de sub-redes, en la zona D,C y B.

Router con 2 interfaces
Repartidor secundario con 2 concentradores stand-alone (10BaseT)
Ejemplo de 2 Subredes en la zona D

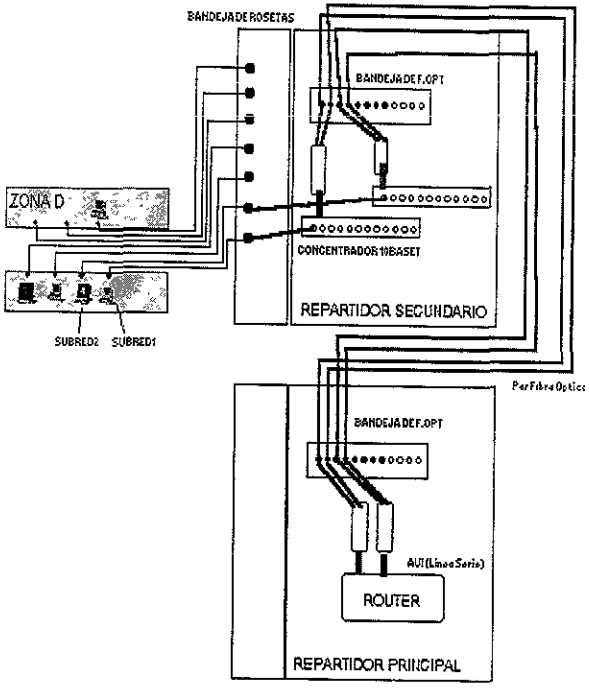


Ilustración 5-7 Interconexión de 2 sub-redes en la zona D.

5.5.2. Posibles migraciones de la topología

A continuación se presentan algunas de las posibles topologías que se pueden adoptar en un futuro, derivadas de redes locales Ethernet (10 Mbps.).

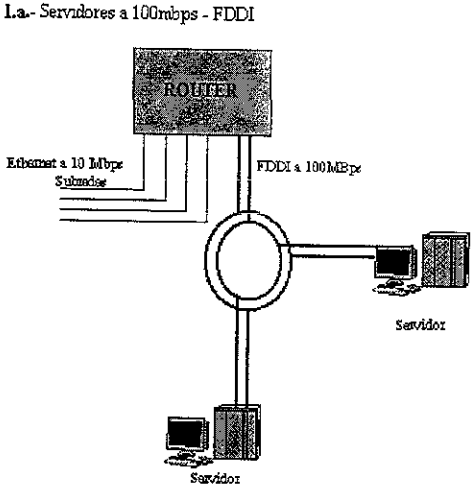


Ilustración 5-8 Migración Ethernet 10 Mbps. A FDDI 100 Mbps.

Requerimientos:

- Un *ruteador* de altas prestaciones. En este caso no necesita cambiar el ruteador **CISCO** AGS con 10 interfaces.
- Interfaz *FDDI* en el *ruteador* (tarjeta). Tiene un costo aproximado de 60,000 pesos.
- Cada servidor debe contar con una tarjeta *FDDI*.
- Estructurar la fibra (Anillo FDDI) e introducir una serie de dispositivos.

Ventajas:

- Mayor ancho de banda para acceder a los servidores (100 Mbps).
- Mayor flexibilidad en el filtrado de paquetes.
- Costo menor que el resto de opciones.

Inconvenientes:

- Es una estructura menos robusta y centralizada (en el ruteador).

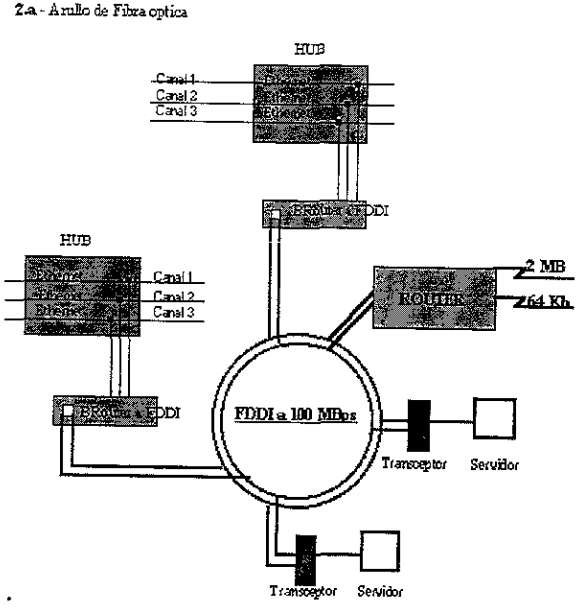


Ilustración 5-9 Interconexión por anillo FDDI.

Requerimientos:

- Un *ruteador* de mínimas prestaciones.
- Un *Brouter*[20] a *FDDI* por cada *hub*. Con un costo aproximado de 45,200 pesos.
- Interfaz *FDDI* en el *ruteador.*
- Cada servidor debe contar con una tarjeta *FDDI.*
- Estructurar la fibra (Anillo FDDI) e introducir una serie de dispositivos.

Ventajas.

- Es una estructura más robusta y menos centralizada (en este caso el anillo es el centro del esquema, no como en el caso anterior que lo es el

[20] Bridge-Router (Ruteador Puente), ejecuta la función de exportar datos entre las capas físicas de una o más redes; además de rutear esta misma información en el ámbito de datos.

ruteador). De forma que si se estropea un *Brouter*, por ejemplo, deja de funcionar sólo un segmento de la red.

- Mayor ancho de banda en la red troncal (100 Mbps).

Inconvenientes:

- Cuando se utilizan *Brouters* lo normal es encapsular las tramas *Ethernet* en tramas *FDDI* (Máquinas propietarias). Lo cual supone que los *Brouters* deben ser iguales o a los menos compatibles, ya que no hay un estándar fijado. La mejor solución sería utilizar máquinas que tradujeran las tramas *Ethernet* en tramas *FDDI*, con lo que se evitaría una sobrecarga en la red, al ser más cortas las tramas.

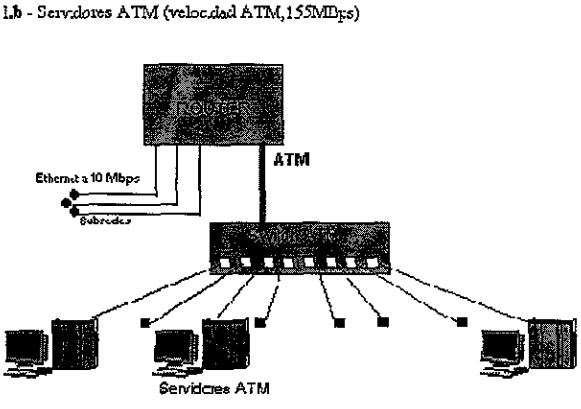


Ilustración 5-10 Migración de redes y sub-redes Ethernet 10Mbps. a ATM 155Mbps.

Requerimientos:

- Un *ruteador* de altas prestaciones que permita *ATM*. En este caso si necesitamos cambiar el *ruteador*.
- Interfaz *ATM* en el *ruteador* (tarjeta).
- Cada servidor debe contar con una tarjeta *ATM*.
- Un *Switch ATM*.

Ventajas:

- Mayor ancho de banda que con *FDDI* para acceder a los servidores (155 Mbps mínimo).

Inconvenientes:

- El estándar *ATM* es adecuado para Voz e Imagen, pero no para Datos. Muchos fabricantes han propuesto cambiar el estándar de *ATM*, añadiendo una nueva funcionalidad conocida como 'Rate Based Flow Control' (Control de Flujo en función de la velocidad), que resuelve el problema de mal rendimiento con IP, siempre que se saturan los enlaces. Por ello se debe adoptar una tecnología que cuente con esta funcionalidad.
- Su alto costo, el Switch cuesta alrededor de 285 o 340 mil pesos.

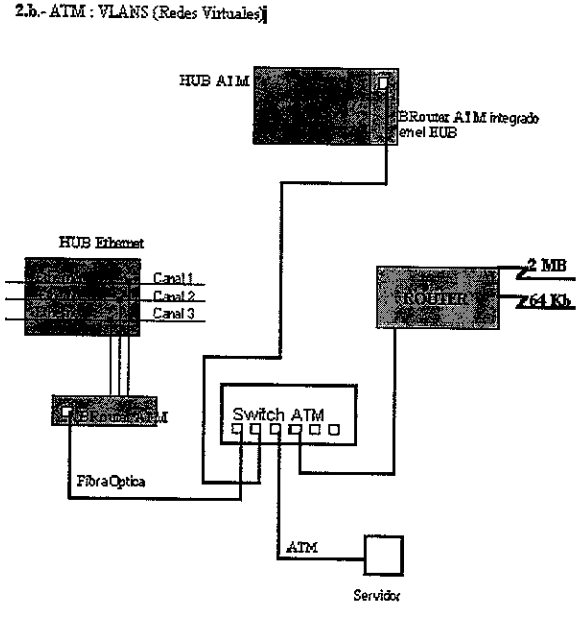


Ilustración 5-11 Red virtual básica ATM 155Mbps.

Requerimientos:

- Un *ruteador* de pocas prestaciones que permita *ATM*.
- Un *BRouter ATM* por cada *hub* o bien cambiar los *hubs* existentes por *HUBs ATM*. Esto último es mejor porque facilita la gestión y es más tolerante a fallos.
- Interfaz *ATM* en el *ruteador*.
- Cada servidor debe contar con una tarjeta *ATM*.

- *Switch ATM.*

Ventajas:

- Mayor ancho de banda en la red troncal (155 Mbps como mínimo).

Inconvenientes:

- Los mismos que en el caso anterior.

La Migración completa a *ATM*, es decir, introduciendo *HUBs ATM* y demás, supone un proceso más largo y costoso que todos los anteriores. El costo aproximado es de unos 6 millones de pesos.

En principio, esta última opción, resulta recomendable para todas aquellas topologías que pretendan dar altas prestaciones a sus comunicaciones de Intranets Corporativas metropolitanas y regionales, así como en edificios inteligentes y campus Universitarios con enlace directo al Internet.

6. Redes de banda ancha (WAN)

Está claro que el ancho de banda es siempre escaso, independientemente de cuánto haya disponible. Por lo tanto, se ha desarrollado un enorme esfuerzo de investigación en redes de Banda Ancha, con el objetivo de llegar a redes de Gigabits/s, que tecnológicamente hoy ya han sido concebidas como la próxima generación en redes conmutadas.

La forma más evidente y la base de las redes conmutadas es la reducción del número de nodos por red, con lo que se logra el objetivo de incrementar el ancho de banda disponible para cada usuario en dicho tramo, llegando incluso a un sólo nodo en cada red. Esto es a lo que se denomina segmentación, y a cada tramo de red creado así se le llama segmento.

Pero, como es lógico, los usuarios de esos segmentos necesitan una comunicación con el resto de la red, e incluso con otros segmentos, o se perdería el objetivo de las redes. Además, dicha comunicación entre segmentos debe poder realizarse gran velocidad.

Por ahora existen dos líneas de redes en desarrollo que son las más prometedoras: La multiplexión en frecuencia de la fibra óptica (FDDI) y *ATM.*

A pesar que la primera es mucho más atractiva, puesto que el ancho de banda total disponible en ese caso en una fibra es enorme, aún es demasiado caro construir un filtro que cambie dinámicamente las frecuencias del láser. Sin embargo, es probablemente la tecnología que desplazará a *ATM* en unos cuantos años.

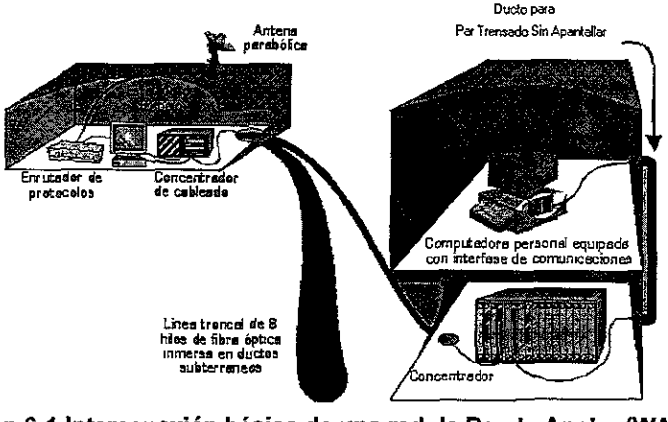


Ilustración 6-1 Interconexión básica de una red de Banda Ancha (WAN)

(Fuente: Centro de cómputo, unidad occidente, Cinvestav IPN, Mérida, México.)

6.1. Nivel de datos

En este nivel, suponemos que dos computadoras están comunicadas directamente por un "cable" bidireccional. Esto puede ser un circuito virtual, un cable serial, una conexión telefónica con módems, una Ethernet, una *FDDI*, etc.

Suponemos que podemos hacer un 'write' (escritura) de algunos bytes en ese cable y al otro lado pueden hacer un 'read' (lectura).

En el esquema OSI de layers, el nivel de datos se encarga de simular un canal de comunicaciones punto a punto libre de errores. Veremos después que, en la práctica, éste no es el mejor lugar para hacer ese rol. Sin embargo, es el mejor lugar donde estudiarlo, y los protocolos y algoritmos que veremos se usan en la práctica, pero en otro nivel.

La idea es que el **'write'** y el **'read'** son llamadas al nivel físico para enviar los datos pero lo podemos ver como un **'pipe'** (línea) bidireccional que conecta ambas máquinas. El problema es que este 'pipe' puede tener errores: puede perder *bytes* y puede alterar *bytes*.

6.1.1. Codificación de datos

ATM es la tecnología más usada en el ambiente de redes rápidas. Es un protocolo híbrido, que toma muchos elementos aprendidos de los diversos sistemas existentes, y su objetivo es soportar muchos servicios distintos sobre el mismo medio: desde *POTS*[21], vídeo, hasta correo electrónico y datos.

Los conceptos básicos de *ATM* son muy simples: todo el recorrido de la conexión va por fibra óptica (aunque un buen cableado de par trenzado puede usarse también) la que sé multiplexa usando paquetes de datos. Los paquetes son minimales, y por ello se llaman celdas. Una celda es de tamaño fijo y muy rápida para ser ruteada (ver Ilustración 6-2).

Para que esto sea posible, se requiere que haya un protocolo de conexión que asigne los números de *Path Virtual* y *Circuito Virtual* en todos los *switches*[22] involucrados. Esta última característica hace que *ATM* sea muy parecido a un sistema de conmutación de circuitos, pero con reserva mínima de recursos. El problema de *ATM* es: establecer la conexión. La idea es que se quieren soportar servicios muy diferentes: Rango Constante de Bits (CBR)[23] como vídeo, Rango Disponible de Bits (ABR)[24] como datos, etc. Todos ellos van a costar diferente (porque son distintas calidades de servicio) y debe entonces garantizarse que, si la conexión se establece, se obtendrá la calidad deseada.

---

[21] Plain Old Telephone Service, de sus siglas en inglés.
[22] Conmutadores dedicados.
[23] Constant Bit Rate, de sus siglas en inglés.
[24] Available Bit Rate, ídem.

Sin embargo, los *switches* no quieren realmente reservar la capacidad requerida, y quieren aprovechar los momentos sin transmitir (ejemplo: silencio en las conversaciones telefónicas) para ocupar los recursos en las conexiones que sí tienen tráfico.

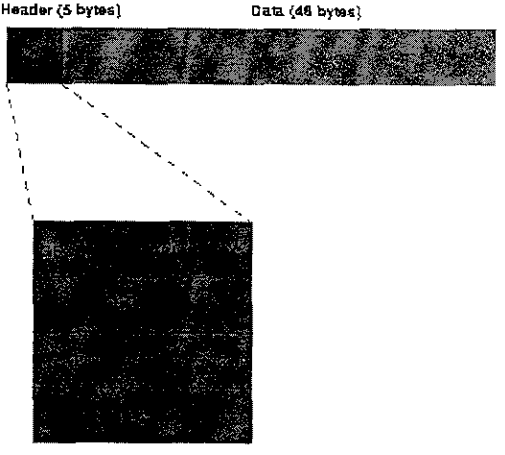


Ilustración 6-2 Celda de Datos ATM.

Existía gran controversia en si *ATM* realmente llegase a convertirse en una solución para dar servicios públicos a gran escala, Pero los hechos han demostrado hoy en día que es no sólo un buen protocolo de red local de banda ancha es una solución integral a la transmisión de una amplia gama de datos por el *Backbone* de Internet.

6.1.2. Conmutación de paquetes

Los 2 Mbps de las redes *Arcnet*[25] han sido superados ampliamente por los 4 y 16 Mbps de *Token-Ring* y los 10 Mbps de *Ethernet*, y todo ello en un corto espacio de tiempo; y más aún, en los últimos años oímos hablar de *Fast Ethernet* (100 Mbps), y como no, también *ATM* (desde 155 hasta 622 Mbps) .

Sin embargo, cabe preguntarse si realmente se necesitan estas velocidades entre todos los puntos de la red, o si las redes actuales pueden seguir cumpliendo sus cometidos y permitir, incluso, las nuevas aplicaciones de videoconferencia, excepto en puntos concretos (estaciones, servidores, etc.), hacia donde el tráfico ésta centralizado.

Hay que tener en cuenta además que por ejemplo en una red *Ethernet* de 10 Mbps en la que existan 10 nodos que generen una cantidad de tráfico similar, el ancho de banda, o por decirlo de un modo más comprensible, la velocidad media a la que dichos puestos de trabajo acceden en la actualidad a la red, es de 1 Mbps. Esto es lo que se puede denominar conmutación de paquetes, que es la oferta de las redes actuales.

Pero, ¿qué ocurriría si, por ejemplo, se lograse que todo el ancho de banda que permite *Ethernet*, 10 Mbps, pudiera estar disponible en todo momento a cada uno de los puestos de la red? La respuesta es, sin duda, que en la mayoría de los casos y en gran parte de las redes de pequeño y medio tamaño, sería suficiente y no requeriría cambiar toda la estructura de la red hacia las nuevas tecnologías, como las que proponen *Fast Ethernet* y *ATM*.

Esta es la propuesta que ofrecen las nuevas técnicas de conmutación de paquetes y además, funcionando a través de las redes actuales, sin cambios en el cableado ni en las tarjetas y software; de los puestos de trabajo.

6.2. *Transporte de Datos*

6.2.1. Tramado (framing)

Para poder detectar errores en los datos, la técnica más usual es encapsular los datos en una trama (frame) que permita sincronizarse y descartar los errores. La técnica tradicional es agregar *bytes* a los datos, en particular una verificación de suma (checksum). Un *checksum* es un número calculado en base a los datos (como un dígito verificador) que se envía junto con ellos. Al recibir los datos, el *checksum* sé re-cálcula, y si no calza se sabe que hubo un error, y el *frame* debe ser descartado.

[25] *Arquitectura de la red digital de transmisión de datos evolucionada del post, que permite intercomunicar* redes metropolitanas de computadoras.

Dividir los datos en *frames* no es tan fácil porque todos los *bytes* (también los del frame) pueden perderse. Por ejemplo, poner primero el largo (Lenght) y luego los bytes (Data), puede ser peligroso, porque el largo se puede perder (uso como largo un byte de datos y luego no puedo volver a sincronizarme). Por ello, el *checksum* debe incorporar también los datos del *frame*. Sin embargo, aún así, si debo descartar un *frame* (cuyo largo no es confiable) ¿cómo sé dónde empieza el siguiente? (Ver. Ilustración 6-3)

Una técnica clásica es usar *bytes* delimitadores de comienzo (SOH) y fin (EOP) de *frame*. Estos son *bytes* especiales que sirven para sincronizarme. Sin embargo, estos *bytes* (tengan el valor que tengan) pueden aparecer también en los datos, y no deben confundirse con los delimitadores. Para ello, utilizo otro *byte* especial (ESC) que **"escapa"**. Entonces, si aparece un *SOH* en los datos, envío *ESC, SOH*. Un nuevo problema, claro, es qué hago si aparece *ESC* en los datos, y en ese caso envío *ESC, ESC* (un escape escapado). Obviamente, todo se puede perder, desde los delimitadores, los *ESC*, etc. Pero el receptor siempre podrá detectarlo. El tener un delimitador permite no tener que enviar el largo, pero por razones de eficiencia (administración de memoria) muchas veces se envía el largo también.

Ilustración 6-3 Esquema de Un Frame de Datos.

El determinar cuántos *bytes* enviar en un *frame* puede ser delicado. El rango va entre 0 y MAX_PACK (incluyendo los delimitadores y los ESC necesarios). Una línea con muchos errores puede preferir *frames* pequeños (la probabilidad de perderlos es menor), pero es más eficiente enviar *frames* grandes (sino se pierden).

En general se considera al *framing* como una sub-capa de la capa Datos.

Al usar *framing*, los errores del medio físico (pérdida de bytes y alteración de bytes) aumentan: ahora podemos perder *frames* completos. Parte de la misión será ahora retransmitir los *frames* perdidos, lo que también puede traernos la recepción de *frames* duplicados o en desorden. Esto implica protocolos bastante complejos si se quiere ser eficiente (ver Transporte de Datos).

6.2.2. Control de errores

Existen varios algoritmos de redundancia para detección y corrección de errores en una secuencia de *bits*. Por ejemplo, al enviar un *byte* por líneas seriales, típicamente se usaban 7 *bits* de datos y el octavo se usaba como *bit* de paridad (1 si el número de bits en 1 es par, 0 si es impar, o viceversa).

Esto permite detectar todos los errores de un *bit*. Además, si yo supiera cual *bit* se alteró o perdió, podría corregirlo, deduciéndolo a partir del *bit* de paridad (esto se usa en los arreglos de discos redundantes (RAID), porque se sabe cuál disco falló).

El problema es que tampoco queremos aumentar demasiado la información que se transmite, por lo que se usan esquemas aceptados con una buena probabilidad de detectar los errores habituales. En general, es mucho más eficiente retransmitir los *frames* con errores que anexar información de corrección a todos.

Por ejemplo, Código de Redundancia Cíclica (CRC)[26], éste calcula 16 bits de *checksum*, detecta todos los errores de uno y dos *bits*, todos los errores de 16 o menos *bits* contiguos, y el 99% de los errores de *bits* contiguos más largos. La idea es que los errores no son realmente aleatorios en las redes, sino que vienen acumulados en *bits* contiguos.

6.3. Protocolos de retransmisión

Si quiere simular un enlace punto a punto fiable y sin errores, debemos retransmitir los *frames* perdidos. Adelante veremos una serie de modelos en protocolos de transmisión.

6.3.1. Stop and wait

Un protocolo *stop and wait* es lo más simple que existe. La idea es transmitir un grupo de *bytes* y esperar que el otro lado me indique que los recibió. Sólo una vez que recibí su respuesta decido que puedo seguir enviando. Suponemos que el flujo de datos es en una sola dirección, aunque la comunicación es bidireccional (para permitir que me indiquen que los datos llegaron). Por lo tanto hay flujo de datos y flujo de control. Los paquetes de control que usamos en este caso son muy simples: sólo indican que recibieron los datos bien. Este paquete se conoce como un Ack[27] (de acknowledgement).

El nivel datos requiere un formato de empaquetamiento de los bytes (además del que ya provee el frame) para poder entenderse y detectar los errores. Usaremos la Ilustración 6-4.

Ilustración 6-4 Paquete de Datos.

[26] Cyclic Redundancy Code, de sus siglas en inglés.
[27] Señal de reconocimiento o acuse de recibo, es una respuesta enviada por un receptor para indicar que recibió con éxito la información que le fue enviada.

El campo tipo es para distinguir los paquetes de datos de los paquetes de control (aunque en este primer caso no se requiere). El campo largo es un short int con el tamaño del paquete y luego los datos. Al final se anexa el *checksum* de verificación (CC). Cuando es un *Ack*, no se envía el largo, sino directamente el *checksum* (para evitar que un error me haga llegar un Ack inexistente).

La función de lectura de datos es más compleja por el manejo de los *buffers* de datos. El número de *bytes* que me piden al nivel datos no tiene porqué ser el mismo que recibo desde el nivel físico, por lo que debo tener un *buffer* intermedio para manejar los bytes que sobran de una lectura a otra.

Este protocolo considera un emisor y un receptor. No funciona en un esquema en que se alternen los roles (por ejemplo pedir un servicio y recibir una respuesta). Al tener datos en ambas direcciones, puedo recibir un paquete de datos al esperar: un *Ack* y tengo que considerarlo para evitar quedar bloqueados ambos lados a la vez.

Hay varias optimizaciones interesantes: por ejemplo en vez de esperar un tiempo fuera (*timeout)* para retransmitir, el receptor podría ayudar enviando un Nack (Negative Acknowledgement)[28] cuando recibe un paquete con errores, apurando la retransmisión. Pero lo más importante es eliminar los largos tiempos de bloqueo que presenta este protocolo.

En general, los canales de comunicación tienen un retardo que no es despreciable (el ejemplo más típico es el satélite, donde la ida y vuelta es más de medio segundo). Por lo tanto, puedo transmitir muchos paquetes en el cable durante el tiempo que me toma llegar al otro lado y esperar el *Ack* de vuelta. Por supuesto, en el caso de transmitir varios paquetes antes de recibir los *Acks*, debo cuidar de no saturar la capacidad del receptor, lo que se denomina Control de Flujo. En *stop and wait*, esto es automático, puesto que sólo requiero almacenar un paquete cada vez.

En general, *stop and wait* sólo se usa si la simplicidad del algoritmo es lo principal y la eficiencia no interesa.

6.4. Protocolos de ventana deslizante (sliding window)

Los protocolos de comunicación avanzados intentan sacar el mayor provecho posible del enlace, en particular en casos de retardos no despreciables, que son bastante frecuentes. La idea entonces es no esperar el *Ack* para transmitir el próximo paquete, sino seguir transmitiendo un tiempo. Para ello, cada paquete lleva un número de secuencia, y los *Acks* también de este modo se sabe qué paquetes corresponden.

El número de paquetes que tengo derecho a transmitir sin haber recibido un *Ack* se conoce como el tamaño de mi ventana.

[28] Reconocimiento Negativo.

Obviamente, si no hay errores, este protocolo es mucho más eficiente que *stop-and-wait*, puesto que utilizo lo más que puedo el ancho de banda disponible (si logro que el tamaño de la ventana llene el cable), no teniendo que detenerme nunca.

Si hay errores, depende cómo manejemos la retransmisión, y la eficiencia que podamos lograr.

El receptor también maneja una ventana. En el caso que los errores no sean demasiado frecuentes, se estila un protocolo simple que usa una ventana de recepción de tamaño 1 (Go-Back-N). Cuando se esperan tasas de errores importantes, se usa una ventana de tamaño mayor (Selective Repeat), lo que permite recibir paquetes adelantados y guardarlos dentro de la ventana hasta completar el trozo faltante.

Si la ventana del enviador y del receptor es de tamaño 1, nos encontramos con *stop and wait*.

Al tener una ventana más grande en el enviador, el hecho de transmitir paquetes en secuencia, sin esperar los *Acks* secuenciales, introduce un nuevo error: paquetes en desorden. Como siempre, debemos garantizar que los paquetes que entregamos a la aplicación mantienen el orden original.

Estos protocolos manejan tiempo fuera (*timeouts*) por paquetes y almacenan múltiples paquetes que fueron transmitidos pero de los que su Ack aún no llega (por sí hay que retransmitirlos). Esto produce una actividad del nivel de datos que se produce en paralelo con la aplicación. Por ejemplo, la aplicación sigue generando datos mientras el nivel de datos puede estar recibiendo *timeouts* o *Acks*.

Esto lleva a que el nivel de datos ya no puede sea una sub-rutina simple de la aplicación (como en el caso previo). Por ejemplo, si la aplicación no llama más al nivel de datos (porque ya le pasó todos los datos), igual debo terminar de procesar los *Acks* y retransmitir los paquetes perdidos.

6.4.1. Go-back-n

La idea es ir transmitiendo los paquetes de la ventana, hasta el tamaño máximo acordado. Al ir recibiendo los *Ack's*, la ventana se va corriendo y puedo enviar el resto de los paquetes, sin pasar el tamaño máximo.

Cada paquete tiene un *timeout* asociado. Cuando se cumple un *timeout*, decido que la transmisión de la ventana falló, y retransmito la secuencia completa.

Esto me permite tener un receptor simple, con una ventana de tamaño 1. Basta con que recuerde el número de secuencia del próximo paquete que debe recibir.

Si el número de errores es bajo, este protocolo es muy eficiente con ventanas grandes. Al aumentar la tasa de errores, las ventanas deben ser más pequeñas.

6.4.2. Selective repeat

En este caso, la idea es no retransmitir más que los paquetes perdidos. Para ello, el receptor también posee una ventana donde almacena los paquetes llegados por adelantado. Esta ventana es del tamaño máximo de la ventana del enviador para asegurarse de nunca perder paquetes demás. Al recibir un paquete, el receptor revisa su número de secuencia para colocarlo en el *buffer* correspondiente en su ventana. Al ir llenando los primeros *buffers*, pueden ir pasándose a la aplicación.

Al recibir un *timeout*, se retransmite el paquete al que le corresponde, pero no el resto. En este caso, no podemos asumir los *Acks* adelantados como validando los paquetes anteriores, puesto que el receptor envía los *Acks* en cuanto recibe bien un paquete.

Por otro lado, se debe tener más cuidado con los números de secuencia. Al tener varios *buffers* en el receptor. Al avanzar la ventana tendremos un overlap con los números anteriores. Supongan que recibo toda la ventana correcta y mis *Acks* se pierden. El emisor me retransmite la ventana y yo ya la avancé. Como los números de secuencia sé rehusan, voy a aceptar los duplicados como correctos. Debo entonces definir que el tamaño máximo de la ventana es la mitad del largo de la secuencia, para asegurar que no haya *overlap* entre una ventana y la siguiente.

6.4.3. Optimizaciones

Algunas optimizaciones son interesantes, por ejemplo usar *nacks* en caso de paquetes erróneos. También, cuando hay flujo en dos direcciones, puedo poner los *Acks* en un campo de los paquetes de datos (piggybacking) en vez de usar paquetes distintos.

Estos esquemas también se aplican en caso de varias aplicaciones compartiendo el nivel Datos. Basta multiplexar, anotando a cual conexión pertenece cada paquete.

7. Redes virtuales

Los grupos de trabajo en una red han sido creados hasta ahora. por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o *hub*.

Como consecuencia directa de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de transmisión (*broadcast*), así como la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un grupo determinado deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN, o red Virtual) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de una forma lógica , en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios comparten sus dominios de transmisión. La diferencia principal con la agrupación física es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red *LAN*, incluso situándose en distintos concentradores de la misma. Los usuarios pueden así trabajar a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además al poder distribuir a los usuarios en diferentes segmentos de red, se pueden situar puentes (*bridges)* y/o ruteadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, se pueden mantener diferentes usuarios del mismo grupo, unos con *FDDI* y otros con *Ethernet*, en función tanto de las instalaciones existentes como el ancho de banda que precise cada uno por su función específica dentro del grupo. Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red. Se pueden permitir o no que el tráfico de una *VLAN* entre y salga desde/hacia otras redes. Pero se puede llegar aún más lejos. Las redes virtuales permiten que la ubicuidad geográfica no-se límite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes *WAN* o *MAN*, a lo largo de países y continentes sin ninguna limitación, más que la que impone el administrador de dichas redes.

7.1. Tecnología

Existen tres aproximaciones diferentes que pueden emplearse como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de *bridging*, y conmutación de segmentos con funciones de *bridging/routing*.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones validas, sólo la ultima, con funciones de puente/ruteador (bridge/router), ofrece todas las ventajas a las VLAN.

7.1.1. Conmutadores de puertos

Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden asociarse dinámicamente a cualquiera de los segmentos, mediante comandos *software*. Cada segmento se asocia a un *backplane*, que equivale a su vez a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignarse y reasignarse a diferentes grupos de trabajo o redes virtuales.

Se puede definir los conmutadores de puertos como "**software patch panels**[29]", y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo. Sin embargo, existen graves limitaciones, dado que están diseñados como dispositivos que comparten un *backplane* físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos adolecen de conectividad con el resto de la red. Al segmentar sus propios *backplanes* no proporcionan conectividad integrada entre los mismos, y por tanto están separados de la comunicación con el resto de la red. Requieren para ello un *bridge/router* externo. Ello implica mayores costos, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red.

Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o *backplane*, por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

[29] Paneles de Parches para Software, de su traducción al español.

7.1.2. Conmutadores de segmentos con puenteo (Bridging)

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Se emplean para ello los algoritmos tradicionales de los *bridges*, o subconjuntos de los mismos para proporcionar conectividad entre varios segmentos a la banda o velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las *VLAN* no son grupos de trabajo conectados a un sólo segmento o *backplane*. Si no grupos lógicos de nodos que pueden conectarse a cualquier número de segmentos de red físicos. Estas *VLAN* son dominios de transmisión lógicos (domain logic broadcast): conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la *VLAN* como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, se puede reconfigurar y modificar la estructura de la *VLAN* mediante comandos *software*, con la ventaja añadida de ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red necesitan routers, con las consecuencias que ya se han mencionado en el caso anterior, relativas al costo y la reconfiguración de la red.

7.1.3. Conmutadores de segmentos con puenteo/ruteo (Bridging/Routing)

Son la solución evidente tras la lectura atenta de la dos soluciones anteriores. Ambos dispositivos comparten todas las ventajas de los conmutadores de segmentos con funciones de puenteo (*bridging*), pero además con funciones añadidas de ruteo (*routing*), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de la red. Además, sus funciones de encaminamiento facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales se puede crear un nuevo grupo de trabajo, con tan sólo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de sub-redes de computadoras, permitiendo así asignar el ancho de banda requerido por el nuevo grupo de trabajo, sin afectar a las aplicaciones de red existentes.

En las *VLAN* con funciones de encaminamiento, la comunicación con el resto de la red se puede realizar de dos modos distintos: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de encaminamiento multiprotocolo, que facilitan el tráfico incluso entre varias *VLAN*.

Los dispositivos con funciones *VLAN* ofrecen prestaciones de valor añadido suplementarias a las funciones específicas de las redes virtuales

7.2. *Prestaciones de las redes virtuales (VLAN)*

Los dispositivos con funciones *VLAN* ofrecen unas prestaciones de valor añadido, suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las *VLAN*.

Al igual que en el caso de los grupos de trabajo de *LAN*, las *VLAN* permiten que un grupo de trabajo lógico comparta un dominio de transmisión. Ello significa que los sistemas dentro de una *VLAN* determinada reciben mensajes de *broadcast* desde el resto, independientemente de que residan o no en la misma red física. Las aplicaciones que requieren por ello de tráfico en la transmisión siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos *broadcast* no son recibidos por otras estaciones situadas en otras *VLAN*.

Las *VLAN* no se limitan únicamente a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica.

Las redes virtuales pueden además solaparse, permitiendo que varias de ellas compartan determinados recursos, como troncales (*Backbones*) de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales es la administración de las redes y sub-redes de computadoras. Las *VLAN* tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.

Las soluciones tradicionales de *internetworking*, empleando *hubs* y *ruteadores*, requieren que cada segmento sea una única sub-red; por el contrario, en un dispositivo con facilidades *VLAN*, una sub-red puede expandirse a través de múltiples segmentos físicos, y un sólo segmento físico puede soportar varias sub-redes de computadoras.

Hay que tener en cuenta asimismo que los modelos más avanzados de conmutadores con funciones *VLAN* soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que permiten determinar con gran precisión las características del tráfico y de la seguridad que se desea en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de *bridging* y multiprotocolo de *routing*.

7.2.1. Aplicaciones y productos

Se pueden intentar esquematizar los puntos en que las redes virtuales pueden beneficiar a las redes actuales:

1. Movilidad.

Como se ha visto, el punto fundamental de las redes virtuales es permitir la movilidad física de los usuarios dentro de los grupos de trabajo.

2. Dominios lógicos

Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos; o en otras palabras los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.

3. Control y conservación del ancho de banda

Las redes virtuales pueden restringir las transmisiones (*broadcast*) a los dominios lógicos donde han sido generados. Además añadir usuarios a un dominio determinado o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.

4. Conectividad

Los modelos con funciones de encaminamiento permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

5. Seguridad.

Los accesos desde y hacia los dominios lógicos pueden ser restringidos en función de las necesidades específicas de cada red, proporcionando un alto nivel de seguridad.

6. Protección de la inversión

Las capacidades *VLAN* están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales.

El primer suministrador de conmutadores con soporte *VLAN* fue **Alantec** (familia de concentradores/conmutadores (hub/swich) multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones *VLAN*:

Bytex (concentrador inteligente 7700)

Cabletron (ESX-MIM)

Chipcom (OnLine)

Lannet (MultiNet Hub)

SynOptics (Lattis System 5000)

UB (Hub Acess/One)

3Com (LinkBuilder).

Con los procesos de reingeniería de empresas, *downsizing*, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes. Las redes virtuales combinan mayores anchos de banda, facilidades de configuración y potencial de crecimiento, lo que ayudará a que se conviertan en un estándar en los entornos corporativos.

En la actualidad, las implementaciones de tecnologías de redes virtuales no son interoperativas entre diferentes productos de diversos fabricantes.

Muchos de estos fabricantes intentan buscar soluciones adecuadas para lograr dicha interoperabilidad, y por ello una gran ventaja de las soluciones basadas en *software* es que podrán adaptarse a las normalizaciones que tendrán lugar en un futuro cercano. Algunas soluciones basadas en *hardware* habrán de quedarse atrás en este sentido.

Otro punto a destacar es que la tecnología *ATM* prevé, como parte importante de sus protocolos, grandes facilidades para las redes virtuales, lo que equivaldrá sin duda a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas *VLAN*.

El futuro es claro respecto de este punto. Las características *VLAN* formarán parte, en breve, de todos los equipos que se precien de querer ser competitivos.

8. Protocolos ruteables y no ruteables

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, asimismo las conexiones entre redes metropolitanas (*MAN*) y redes de banda ancha (*WAN*). Estos protocolos operan en diferentes capas del modelo OSI.

Así encontramos que en las primeras dos capas del modelo se definen los protocolos que se encargan de accesar al medio físico de comunicaciones; así de como generar los frames correspondientes a una determinada topología y arquitectura, como *Ethernet*, *Token* Ring o *FDDI* entre otras.

Cada *frame* de información lleva datos provenientes de las capas superiores en las que intervienen protocolos, cuya función es la de "mover" datos de un nodo a otro, una vez que se trama la información en un *frame*. También se encarga de entregarla o recibirla sin la trama del *frame* al medio, según sea el caso de transmitir o recibir respectivamente.

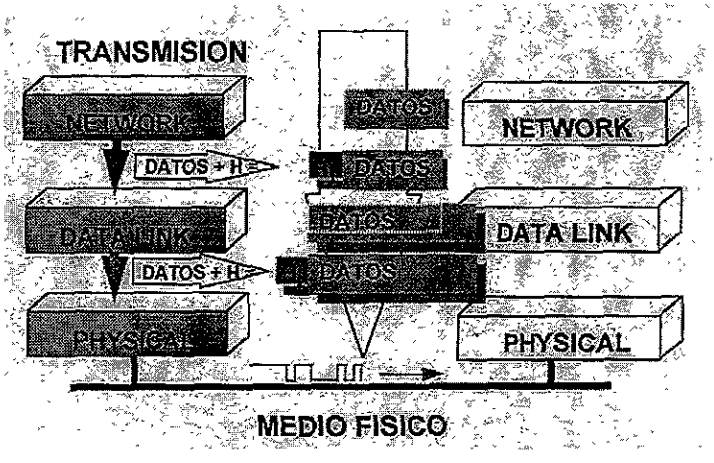


Ilustración 8-1Transmisión de Datos Por el Medio Físico.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

Podemos encontrar una gran variedad de los protocolos que están funcionando sobre la capa 2 del modelo OSI, ya que las diferentes arquitecturas de cómputo y teleinformática hacen uso de aquellos propietarios de la arquitectura, estos son protocolos estándares o tal vez una combinación de ellos.

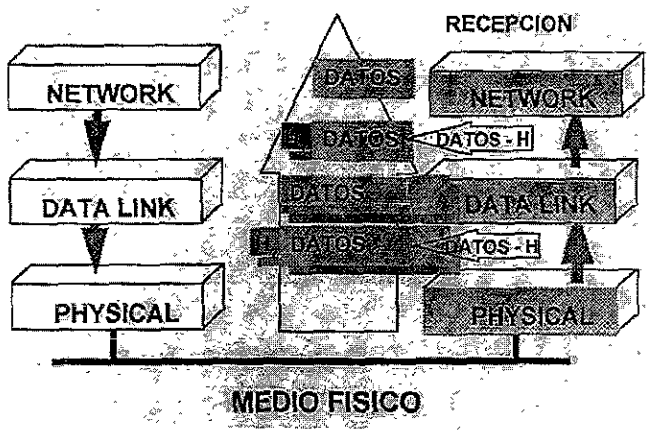


Ilustración 8-2 Recepción de Datos Por el Medio Físico.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

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

8.1. Protocolos ruteables

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

En la Ilustración 8-3 puede observarse que el **nodo A** de la ***red a*** envía datos al **nodo B** que se encuentra en la ***red b***. El protocolo es capaz de interpretar la dirección lógica de la ***red a*** como el origen en donde se genera la información del **nodo A**, la dirección lógica b como el destino.

Cuando el protocolo percibe esto, prepara dentro del paquete de información un formato con el remitente y destinatario de esta unidad de información. A continuación el software de red, corriendo en el nodo A, en este caso trama este paquete en un *frame* de *Ethernet* y lo transmite por el medio de comunicación. El ruteador conectado a ese segmento de red, recibe el *frame* y lo "**lee**".

Si el ruteador posee la habilidad de interpretar cuál es el protocolo ruteable que generó el paquete encapsulado en el *frame*, esto es, si cuenta con el software que habilitó el proceso de ruteo para este protocolo, entonces el *ruteador* lo retransmitirá por la interface que lo conecta con la ***red b***. Esto lo consigue porque el ruteador también es capaz de comprender el origen y el destino de esta información. A este proceso se le conoce como "**ruteo de información**".

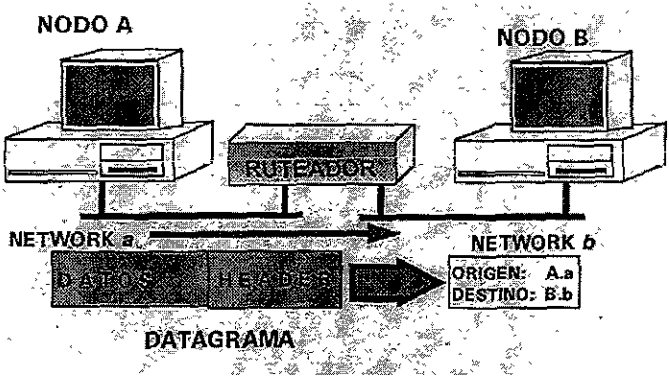


Ilustración 8-3 Operación del Datagrama Origen - Destino.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

Los protocolos ruteables guardan una analogía 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 del remitente)* y de la red destino (*calle del destinatario)*, y que puede llevar también el número de nodo origen (*Núm. de casa del remitente)* y el número de nodo destino (*Núm.* de casa del destinatario). En la analogía el número de red es el *nombre de la calle* y el número de nodo físico (*MAC Address)*, es el *número de la calle* 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 red debe definirse con una red lógica. Esto se aplica tanto a segmentos *LAN* como a segmentos *WAN*.

8.1.1. Protocolos orientados y no orientados a la 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 hasta 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 este 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 encontrasen conectadas entre sí mediante una **"conexión"** virtual. De ahí el nombre de que el protocolo se **"orienta"** a mantener esa conexión virtual. A estos protocolos se les conoce como protocolos orientados a la conexión *(connection oriented protocolos).*

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

La mayoría de los protocolos ruteables que operan en la capa 3 del modelo **OSI** no son orientados a la 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 la conexión, pero que lo consigue transfiriendo su información al protocolo de capa superior inmediata que sí está orientado a la conexión, en este 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 tienen que esperar los reconocimientos *(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 le dejan estas tareas a protocolos de capas superiores.

En el siguiente cuadro se pueden observar algunos de los protocolos ruteables más importantes y sus principales características:

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
IPX/SPX	ESTANDAR	NOVELL INC.	SERVIDORES NETWARE Y CLIENTES DIVERSOS	8 BYTES PARA RED 12 BYTES PARA NODO

Características.

El Internetwork Packet eXchange/Sequenced Packet eXchange, es el protocolo que usa la arquitectura de Novell. Introducido al mercado en 1983 opera virtualmente sobre cualquier plataforma de hardware. IPX no es orientado a la conexión, SPX sí lo es. Otros protocolos auxiliares son RIP (Routing Information Protocol) para el intercambio de información de ruteo, SAP(Service Advertising Protocol) para notificar la presencia de los servidores y servicios, así también cuenta con el NCP (Netware Core Protocol) que regula las sesiones de trabajo entre el servidor y el cliente. Existen varios clientes que se comunican con él file server usando IPX entre los que se pueden citar Macintosh, UNIX, OS/2, DOS, Windows NT, Windows For Workgroup, etcétera. IPX es adecuado para redes de área local, pero no se recomienda para enlaces de red de área amplia con velocidades superiores a 64 Kbits/seg; aunque existen técnicas para mejorar su rendimiento.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
TCP/IP	ESTANDAR	DOD USA	UNIX, NETWARE,SNA, WINDOWS NT, OS/2 Y CLIENTES DIVERSOS	4 BYTES PARA RED Y NODO

Características:

El Transmition Control Protocol/Internet Protocol, busca facilitar la comunicación entre computadoras múltiples de diversas arquitecturas. Se le encuentra prácticamente en todas las arquitecturas de cómputo actuales. IP no está orientado a la conexión, TCP sí lo es. Desarrollado a principios de los 70's, hoy en día es uno de los protocolos más 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 el ARP (Address Resolution Protocol) para mapear direcciones lógicas en físicas; RIP (Routing Information Protocol), para intercambio de información de ruteo; ICPM (Internet Menssage Control Protocol), que reporta condiciones de error en la red; UDP (User Datagram Protocol), protocolo de transporte similar a TCP pero no es orientado a la conexión; FTP (File Transfer Protocol), usado para transferencia de archivos; TELNET (Terminal Emulation Link Network), 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 llamar procesos remotos, SNMP (Simple Network Magnamet 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 LAN y WAN.

Una de las grandes ventajas de este 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.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
APPLE TALK	ESTANDAR	APPLE COMPUTER INC	MACINTOSH, NETWARE, WINDOWS NT, ETC.	2 BYTES PARA RED 1 BYTES PARA NODO

Características

Apple talk no sólo es una familia de protocolos, sino también una arquitectura. Originalmente diseñada para servir a las redes de computadoras Macintosh, pero se ha convertido en uno de los protocolos mas socorridos. Para cuestiones de interoperabilidad, muchas otras arquitecturas se comunican con Apple Talk para integrarse al mundo de la Macintosh. Todos los protocolos de esta familia están diseñados para facilitar las tareas que el usuario tiene que hacer para crear una red de cómputo debido a la filosofía de la compañía A.T. que requiere para su operación crear no sólo redes lógicas por segmento físico, también grupos lógicos de redes llamados "zonas". Entre los principales protocolos que conforman la familia se tienen. DDP (Deliver Datagram Protocol), no esta 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 Transition Protocol), similar al DDP pero sí es orientado a la conexión, RTMP (Routing Table Maintenance Protocol), su propósito es mantener actualizadas las tablas ruteo en los ruteadores que operan con los protocolos 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 y que consiste en simplificar las tareas que debe hacer el usuario para accesar no sólo la computadora si no la red y todos sus servicios.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
DECNET	ESTANDAR	DIGITAL EQUIPMENT CORP.	EQIPOS DEC, GATEWAYS Y CLIENTES.	2 BYTES (6 BITS PARA RED, 6 BITS PARA RED EN FASE IV) 48 BITS PARA NODO 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 ser una arquitectura abierta, lo que le da versatilidad para integrarse con otras plataformas tanto con protocolos propietarios como estándares, sobre todo en DecNet fase V, donde DEC 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 de DecNet de 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.

En 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 su serie de protocolos, los especificados en cada capa del modelo OSI.

Los protocolos que llevan información en DecNet fase IV no son orientados 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 service Protocol) que equivale a un protocolo de la capa de transporte que está orientado a la conexión.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
OSI	ESTANDAR INTL.	INTERNATIONAL ORGANIZATION FOR STANDARIZATION.	DEC FASE V, Y OTRAS ARQ. ABIERTAS	48 BITS

Características.

El modelo OSI también define sus propios protocolos. Para las capas de red y transporte. A nivel de red OSI propone dos protocolos· CLNS (Connection Less Network Service) y CONS (Connection Oriented Network service). Como sus nombres lo indican, el primero es un protocolo de red "no" orientado a la conexión y el segundo sí lo es OSI también propone un protocolo de red derivado de X.25. 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. Estos protocolos se identifican como TPO, TP1, TP2 y hasta TP4 TP es por Transport Protocol y mientras que TPO es un protocolo 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 cómputo las han adoptado.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
X.25	ESTANDAR INTL.	C.C.I.T.T.	TODAS LAS ARQ. DE COMPUTO Y TELE-INFORMATICA.	15 BYTES PARA RED

Características:

Se desarrolló en la mitad de los 70's y fue ideado para crear redes de comunicaciones para múltiples plataformas de cómputo que operan sobre una red pública de paquetes conmutados. TelePAC TeleNEt son ejemplos de este tipo de redes. Hoy en día los costos de instalación de este 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 WAN es un segmento de una inter-red X 25 se pueden instalar sobre cualquier medio físico de comunicaciones remotas como líneas telefónicas, enlaces satelitales, microondas, enlaces digitales de RDI, etc. Su instalación se recomienda para enlaces de baja velocidad hasta no más de 256 Kilobits/seg. 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" deben su desarrollo a las experiencias con el protocolo X.25.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
FRAME RELAY	ESTANDAR INTL.	A.N.S.I. Y LA C.C.I.T.T.	TELE-INFORMATICA.	10 BITS (ACTUAL) 17 BITS (AVANZADO) 24 BITS (FUTURO)

Características.

Muchas de las características de X.25 se pueden encontrar en F. Relay. También es un protocolo orientado a la conexión y opera bajo el concepto de conmutación de paquetes. Puede instalarse en redes públicas o privadas y al igual que X.25 el tamaño de sus paquetes es variable. Frame Relay puede funcionar sobre cualquier plataforma de comunicaciones remotas. Es adecuado principalmente para operar a velocidades mayores a 64 Kbits/seg; y una de las ventajas que tiene sobre X.25 es su relativa simplicidad de operación y control, lo que mejora el uso del ancho de banda Se debe recordar que X.25 es un protocolo desarrollado hace casi 20 años y fue diseñado para proteger la información que viajaría por líneas telefónicas poco confiables, tareas que consumen muchos recursos en los equipos de comunicaciones. Frame Relay aprovecha la confiabilidad de los enlaces digitales modernos y sus recursos se enfocan al manejo eficiente de la información que transporta

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
ATM	ESTANDAR INTL	ATM FORUM	EQUIPO DE INTER-NETWORKING	2 BYTES

Características:

ATM es un protocolo ruteable orientado a la conexión, 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 transmisión, llegando incluso hasta los 622.08 Mbits/seg. Y sus unidades de información son fijas, puede transportar lo mismo voz, datos e imágenes en tiempo real. Otra característica fundamental de ATM, es la de ser un protocolo que define desde las primeras capas del modelo OSI y permite extender sus servicios desde redes LAN a toda clase de redes con enlaces WAN. Esta versatilidad pronostica una amplia aceptación para el diseño e implantación de futuras inter-redes.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

8.2. 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 las direcciones físicas de los nodos. Esa dirección física es conocida como el número de nodo o la dirección de MAC *(Media Access Control)*.

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

Al conectar varios segmentos físicos de red entre sí. Es decir, al crear una inter-red, ya sea con segmentos de *LAN* o segmentos de *WAN*, debemos utilizar un dispositivo de 'internetworking" conocido como *Bridge*. Un *Bridge* es un elemento de comunicaciones que sólo propaga las direcciones físicas de los nodos; es decir, es una red formada por todos los segmentos interconectados. Por esta razón, los *bridges* permiten extender los segmentos físicos de red y hacen parecer a los protocolos no ruteables una sola.

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 sólo les interesa saber las direcciones físicas de cada nodo.

Para este propósito los *bridges* crean en sus memorias una tabla de direcciones físicas para saber si propagan los *frames* generados en un segmento de red hacia otros segmentos.

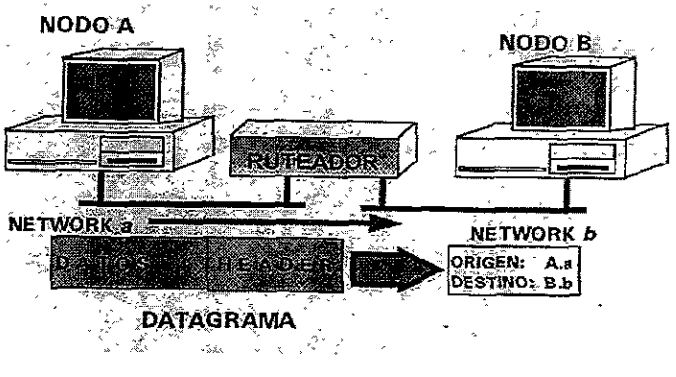


Ilustración 8-4 Proceso de Ruteo de la Información.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

Los protocolos **no ruteables** generalmente no son "**comprendidos**" por los *bridges*, por lo tanto la información de control contenida en los paquetes de información no es interpretada por éstos. 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 *bridge* es un dispositivo de "**internetworking**" más rápido que un "**ruteador**". Pero para inter-redes muy grandes la eficiencia decae con el uso de este tipo de protocolos. Por otro lado, muchos protocolos no ruteables no están diseñados para operar en ambientes *WAN*, porque al asumir que se encuentran en un 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 la conexión y no orientados. 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.

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

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
APPC NETBIOS NETBEUI	ESTANDAR	IBM. CORP.	EQUIPOS IBM, GATEWAYS Y CLIENTES.	12 BYTES

Características

El 60% de las redes de cómputo hoy en día utilizan algún equipo de arquitectura propietaria de IBM SNA (Standard Network Arquitecture). IBM originalmente desarrolló esta arquitectura basada en grandes procesadores centrales que atendían un gran número de terminales "**tontas**"[30]. Pero al integrarse en 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 LAN y que utiliza la dirección física de cada nodo para mover información; NetBEUI (NetBIOS Extended User Interface), similar a NetBIOS que 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 extender su uso a lo largo de una WAN.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
SNA	ESTANDAR	IBM CORP.	EQUIPOS IBM , GATEWAYS Y CLIENTES.	2 BYTES (WAN) 12 BYTES (LAN)

Características.

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 mas de una década SNA se mantuvo como plataforma monolítica y cerrada, de tal forma que para interconectar equipos entre sí debían de ser de la misma naturaleza, ya que SNA utilizó protocolos y esquemas de comunicación propietarios. Con el éxito que tuvieron las LAN's en la década de los 80's, IBM rompió su viejo esquema de cómputo centralizado para incursionar en el distribuido. 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 implementación 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 (Service Access Point), es usado para entregar y recibir información que sólo 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 este tipo de tecnologías, se consigue una mejor interconexión de equipos de arquitectura SNA. Con plataformas de otras arquitecturas diferentes.

Es importante para una buena conectividad el 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.

[30] En el argot del cómputo suele definirse terminal "tonta" a las unidades carentes de unidad de respaldo de información (floppy, disco duro, etc.) debido a que sé inicializan por conexiones RS232 en plataformas UNIX, o por tarjetas de red en PC's.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
LLC2	ESTANDAR	IEEE 802	EQUIPOS IBM, GATEWAYS, Y CLIENTES WINDOWS NT, NOVELL, OS/2, ETC.	12 BYTES (MAC)

Características:

El proyecto 802 de la IEEE define dos tipos de tramado de un frame para diferentes tipos de LAN. 802.3 para Ethernet y 802.5 para Token-Ring. Pero define sobre éstos un formato más el 802.2 que le da ciertas ventajas de comunicación cuando se pasa la información de cada frame a las capas superiores. En esas capas pueden estar operando muchos y diferentes protocolos de muy diversas arquitecturas. Un método eficiente de entregar esa información es utilizar un puerto lógico (SAP) a cada uno de esos protocolos, así se consigue que con un sólo formato de frame pueda intercambiarse fácilmente la información de una plataforma a otra. LLC2 asigna un número 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.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
DEC LAT DEC LAN BRIDGE	ESTANDAR	DIGITAL EQUIPMENT CORP.	EQUIPOS DEC, TERMINAL SERVERS	12 BYTES (MAC)

Características:

En ciertos equipos DEC se utiliza el protocolo de LAT (Local Area Transport) principalmente para conectar terminales "**tontas**" de minicomputadores DEC, usando una red Ethernet como medio de comunicación. Este protocolo asume que el servidor que atiende a las terminales y siempre está conectado al mismo segmento de LAN. Esto lo constituye como un protocolo no-ruteable. DEC LAN BRIDGE es un protocolo de DEC que permite extender las redes 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 BRIDGE. Esto implica el uso de un dispositivo que haga esta función.

NOMBRE	TIPO	DESAROLLADOR	USOS	DIRECCIONAMIENTO
PPP	ESTANDAR INDUSTRIAL	IAB. SOC.	EQUIPOS DE TELE-INFORMATICA TCP/IP	8 BITS EN CAPA 2 4 BITS EN CAPA 3

Características:

El Point to Point Protocol es un protocolo sincrono de comunicaciones para enlaces WAN (punto a punto). Forma parte del set de protocolos de 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 éste es una red por sí sola.

(Fuente: Seminario de Interconectividad, Intersys de México, 1994, Ciudad de México.)

9. Protocolos TCP/IP

Antecedentes

A mediados de los años 70's, la Agencia de Investigaciones Avanzadas de Proyectos de Defensa (DARPA)[31]se interesó en proveer comunicaciones de red por paquetes conmutados (packet-switched) entre las instituciones de investigación en los Estados Unidos de Norteamérica.

DARPA y otras organizaciones del gobierno en ese entonces comprendieron las posibilidades de la tecnología en conmutación de paquetes y comenzaron a descubrir que virtualmente todas las compañías con red necesitarían tener un soporte de comunicaciones disímil a sus sistemas computacionales.

Con la idea en mente de lograr la conexión heterogénea de sistemas, DARPA suministró fondos de investigación para las universidades de Stanford y Bolt, Beranek, y Newman para crear una serie de protocolos de comunicación. Los resultados de este desarrollo fueron completados a finales de la década de 1970 como Internet Protocol Suite, del cual, los dos miembros más conocidos son el Protocolo para Control de Transmisión (TCP)[32] y el Protocolo de Internet (IP)[33] son los dos miembros más conocidos.

Utilizar el término de "**Internet**" para referirse a estos protocolos es el apropiado, porque los protocolos de Internet fueron creados para proveer conectividad y operar a través de redes de comunicaciones ya existentes (por ejemplo, la red telefónica, líneas dedicadas, y circuitos satelitales).

El diseño de los protocolos de Internet ejecuta explícitamente la vinculación de las redes comenzando a juntar sus medios heterogéneos de manera natural, debido a que cada uno de ellos soporta diferentes velocidades, características de error, tamaño de datos, e información de formatos. .

A dos décadas desde su invención, la heterogeneidad de las redes se ha expandido más con el desplegado de redes Ethernet, Token Ring, *Fiber Distribuited Data Interface* (FDDI), X.25, Frame Relay, *Switched Multimegabit Data Service* (SMDS), *Integrated Services Digital Network* (ISND), y más recientemente, *Asinchronous Transfer Mode* (ATM)[34] Los protocolos de Internet han sido aprobados como los mejores medios de Internetworking acercando diversos rangos de tecnologías LAN y WAN.

La suite del protocolo de Internet no incluye únicamente las especificaciones de bajo-nivel (tal como TCP e IP), pero sí las especificaciones para las aplicaciones comunes como el correo electrónico {e-mail}, emulación de

[31] Defense advanced Research Projet Agency, por sus siglas en inglés.
[32] Transmission Control Protocol, ídem.
[33] Internet Protocol, ídem.
[34] Ver. Arquitecturas, Cap. 2.1 , Pag.20 y Redes virtuales, Cap. 7 ; Pag.98

terminal {Telnet}, y file transfer {FTP}.la Ilustración 9-1 presenta algunos de los más importantes protocolos de Internet y su relación con el modelo OSI.

El protocolo de Internet es la suite más amplia de protocolos multidistribuidos utilizados hoy en día, manteniendo la disponibilidad virtual para cada computadora vendida como protocolo básico de comunicaciones.

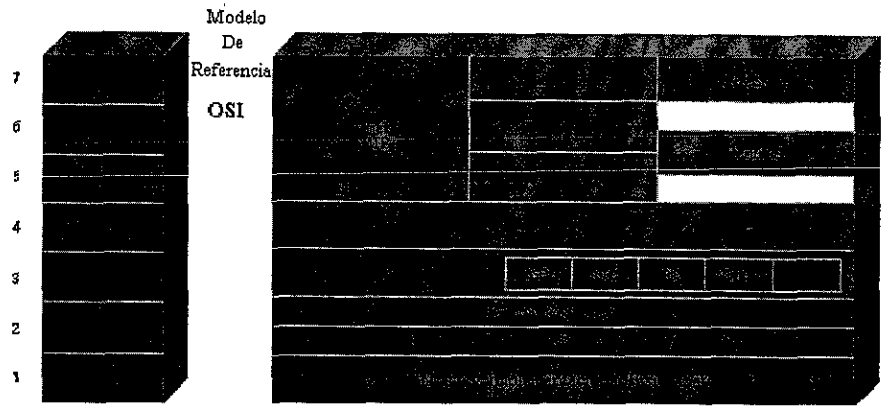


Ilustración 9-1 Relación De La Suite Del Protocolo De Internet Con El Modelo OSI.

9.1. Tecnología TCP/IP

En esta sección se describen los aspectos técnicos del TCP/IP, protocolos relacionados, y de ambiente con los cuales se puede operar la comunicación entre redes (Internetworking). Donde nos enfocaremos en la función de ruteo (función de la capa 3), y discutiremos el TCP (protocolo de la capa 4) resumiendo relativamente sus aplicaciones.

9.1.1. TCP

El TCP es un protocolo de transporte orientado a la conexión que envía los datos como un stream[35] de bytes. Utilizando una secuencia de números y mensajes de reconocimiento, el TCP puede proveer un nodo de envío con la información de entrega que contiene la cantidad de paquetes transmitidos a un nodo de destino. Cuando los datos transmitidos se pierden en el tránsito del origen-destino, el TCP puede retransmitir los datos hasta que cualquiera de los dos condicione un tiempo-fuera de llegada o hasta que la entrega haya sido archivada exitosamente.

[35] Torrente, flujo; de su traducción al español.

El TCP también puede reconocer los mensajes duplicados y podrá descartar los que no sean apropiados. Si existe un envío transmitido demasiado rápido y no se pudiese recibir por la computadora de destino, el TCP podrá emplear un mecanismo de control de flujo para disminuir la velocidad de transferencia de datos. El TCP puede también comunicar la información de entrega a las capas superiores del protocolo y dar soporte a las aplicaciones.

9.1.2. IP

El protocolo IP es la 3ra. Capa primaria en la suite de Internet. Adicional a la operación de ruteo entre-redes, el IP proporciona los reportes de error, la fragmentación y el reensamblado de las unidades de información llamadas "**datagramas**" para la transmisión sobre redes con diferente tamaño máximo de datos[36] . Así tenemos que el IP representa el corazón de la suite del protocolo de Internet.

Las direcciones IP son internacionalmente únicas, un número de 32-bits es asignado por el Centro de Información de Redes (NIC)[37] del Internet local en cada país del mundo. Las direcciones mundialmente únicas son permitidas a las redes IP de cualquier parte del globo para comunicarse con cualquier otra.

La dirección IP está dividida en tres partes. La primera parte designa la dirección de la red, la segunda parte designa la dirección de sub-red de computadoras, y la tercera parte designa la dirección del servidor.

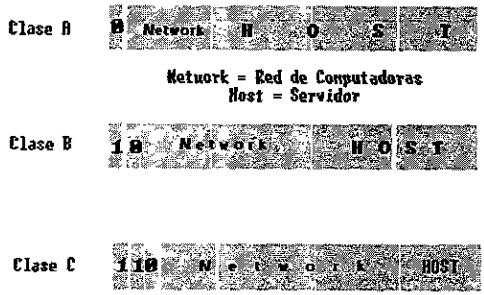


Ilustración 9-2 formato de direcciones clase A, B, y C.

El direccionamiento IP soporta tres diferentes clases de redes. Red clase A proyectada principalmente para usarse en redes muy largas, debido a esto se proveen 8 bits al campo de dirección de red.

[36] Ver. Codificación de datos, Cap. 6.1.1, Pag 90.
[37] Network Information Center, por sus siglas en inglés

La red clase B asigna 16 bits, y la red clase C asigna 24 bits al campo de red. La red clase C únicamente proporciona 8 bits a la dirección del servidor, de cualquier manera, el número de servidores por red podrá ser limitado por un factor. En los tres casos, el bit (s) más significativo (s) a la izquierda indica la clase de red. Las direcciones de IP son escritas en puntos decimales; por ejemplo, 34.0.0.1 de la Ilustración 9-2 presenta los formatos de las direcciones IP de redes clase A, B, y C.

Las redes IP además pueden ser divididas en pequeñas unidades llamadas sub-redes o "subnets" quienes proveen flexibilidad extra para el administrador de la red. Por ejemplo, se asume que una red de clase A tiene direcciones clase A en todos los nodos de la red. Más se debe asumir que la representación en puntos decimales de la dirección de esta red es 34.0.0.0. (todos los ceros en el campo del servidor de una dirección especifican la red entera). El administrador puede subdividir la red usando sub-redes. Esto se hace "aprovechando" los bits del servidor proporcionado en la dirección y usando al mismo como un campo de sub-red de computadoras, como se describe en la Ilustración 9-3.

Si el administrador de red ha escogido utilizar 8 bits de sub-red, el segundo octeto de dirección IP clase A provee el número de sub-red. En nuestro ejemplo, la dirección 34.1.0.0 se refiere a la red - 34, sub-red -1; la dirección 34.2.0.0 se refiere a la red 34, sub-red 2, y así subsecuentemente.

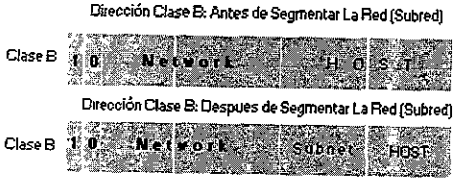


Ilustración 9-3 Direccionamiento de sub-redes.

El número de bits que se pueden apropiar para la dirección de sub-red varía. Para especificar cuantos bits se usan y donde se localiza en el campo del servidor, el IP provee máscaras de sub-red (subred mask). Las máscaras de sub-red utilizan el mismo formato y técnica de representación como las direcciones IP. La máscara de sub-red posee la mayoría de espacios de bits que la dirección IP excepto porque especifica el campo del servidor. Por ejemplo, la máscara que especifica 8 bits de sub-red con dirección clase A 34.0.0.0 es 255.255.0.0.; la máscara de sub-red que especifica 16 bits de sub-red con dirección clase A 34.0.0.0 es 255.255.255.0. ambas máscaras de sub-red son presentadas en la Ilustración 9-4.

Las máscaras de sub-red pueden relacionarse a través de una red en demanda de tal manera que se puede aprender como algunos bits de sub-red son usados en su red.

Ilustración 9-4 Ejemplo de máscara de sub-red.

Tradicionalmente, todas las sub-redes del mismo número de red usan la misma máscara de sub-red. En otras palabras, el administrador de red podrá escoger una máscara de ocho-bits para todas las sub-redes. Esta estrategia es fácil de manejar tanto para la administración de la red como para los protocolos de ruteo. Como siempre, esta práctica desperdicia el espacio de direccionamiento en algunas redes. Varias sub-redes tienen muchos servidores y otras sólo algunos, pero cada uno consume un número completo de sub-red. Las líneas seriales son un ejemplo extremoso porque cada una posee dos servidores que únicamente pueden ser conectados en línea serial de la sub-red.

Conforme las sub-redes tienden a crecer, el administrador tiene que observar la forma en que se ocupará el espacio de direccionamiento más eficientemente. Una de las técnicas que ha tenido mayores resultados es la llamada Máscara De sub-red de computadoras Con Variable Amplia (VLSM)[38].

Con esta técnica, un administrador de red puede utilizar una máscara grande en redes con menos servidores y una máscara pequeña en sub-redes de computadoras con más servidores. De cualquier modo, esta técnica es más compleja que hacer todo de un mismo tamaño y el direccionamiento tendrá que ser asignado cuidadosamente.

Claro que en el orden en que se utilice el VLSM, el administrador de red podrá utilizar componentes que soporten este protocolo de ruteo.

[38] Variable Length Subred Masks, de sus siglas en inglés.

Los ruteadores Cisco soportan el VLSM con el modo de Primer Sendero Corto Abierto (OSPF)[39], modo de Integración De Sistema Intermedio A Sistema Intermedio (Integrated IS-IS)[40], modo avanzado para Protocolo De Ruteo Interno En Gateway (Enhanced-IGRP)[41], y ruteo estático.

Varios medios, como las redes locales IEEE 802, poseen direcciones IP dinámicas obtenidas por medio del uso de otros dos miembros de la suite del protocolo de Internet : El Protocolo para la Resolución De Direcciones (ARP) y su inverso (RARP). ARP utiliza la emisión de mensajes para determinar la dirección correspondiente del hardware (capa MAC) a una capa de dirección de red en particular. ARP es lo suficientemente genérico para permitir el uso virtual del IP con cualquier tipo de mecanismo de acceso al medio por debajo de la línea. RARP utiliza la emisión de mensajes para determinar la dirección de la capa de red asociada con una dirección en particular del hardware. RARP es especialmente importante para los nodos con "**terminales tontas**", para las cuales la dirección de la capa de red usualmente es desconocida para inicializar a tiempo.

9.2. Ruteo En Ambientes IP

El "Internet" es un grupo de redes interconectadas. El Internet desde otro punto de vista es la colección de redes que permite la comunicación entre más instituciones de investigación, universidades, y muchas otras organizaciones alrededor del mundo. Debido a esto los ruteadores dentro del Internet son organizados jerárquicamente, ya que algunos ruteadores son usados para mover la información a través de un grupo particular de redes bajo el mismo control y autoridad administrativa (tal entidad es llamada un sistema autónomo).

Los ruteadores usados para el intercambio de la información dentro del sistema autónomo son llamados ruteadores internos, y utilizan una variedad de protocolos de gateway internos (IGPs)[42] para complementar dicho sistema.

Así los ruteadores que mueven la información *entre* los sistemas autónomos son llamados ruteadores externos; y utilizan el Protocolo Exterior de Gateway (EGP)[43] o Protocolo Fronterizo de Gateway (BGP)[44]. La arquitectura que hoy en día compone el Internet se presenta en la Ilustración 9-5

[39] Open Shortest Path First, ídem.
[40] Intermediate System to Intermediate System, ídem.
[41] Interior Gateway Routing Protocol, ídem.
[42] Interior Gateway Protocols, de sus siglas en inglés.
[43] Exterior Gateway Protocol, de sus siglas en inglés.
[44] Border Gateway Protocol, ídem.

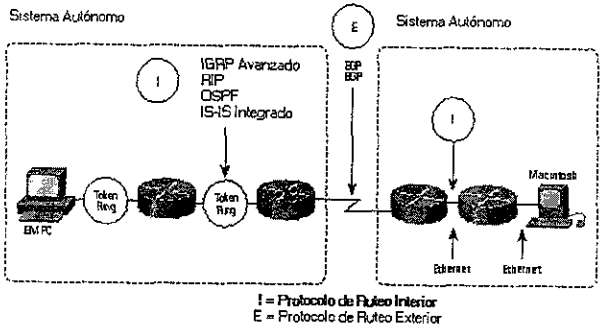


Ilustración 9-5 Representación de la arquitectura del Internet.

Los protocolos de ruteo usados con el IP son dinámicos por naturaleza. Debido a esto, el ruteo dinámico requiere de software especializado en los componentes para poder calcular las rutas más confiables y rápidas. Los algoritmos de ruteo dinámico adaptan la red a los cambios posibles y automáticamente seleccionan las mejores rutas.

En contraste con el ruteo dinámico, el ruteo estático busca los ruteadores para establecer su enlace por medio del ruteador que administra la red. El ruteador estático no puede cambiar la ruta si no es cambiada en el administrador de la red.

Las tablas de ruteo IP constan de pares con dirección destino/próximo punto. En el ejemplo presentado de una tabla de ruteo en la Tabla 9-1, la primera entrada está interpretada tal como significa "para ir a la red 34.1.0.0 (sub-red 1 en la red 34), la próxima parada es el nodo con la dirección 54.34.23.12."

Dirección Destino	Próximo Salto
34.1.0.0	54.34.23.12
78.2.0.0	54.34.23.12
147.9.5.0	.
17.12.0.0	.
.	54.32.12.10
.	54.32.12.10
.	.
	..

Tabla 9-1Una entrada de ruteo IP.

Tal como vemos, el ruteo IP especifica que el datagrama IP viaje a través de una red interna a un punto del ruteador al mismo tiempo. La ruta completa es desconocida desde el principio del desplazamiento.

En cambio, a cada parada, el próximo salto de ruteador está determinado por la marca de la dirección de destino dentro del datagrama con una entrada en el nodo actual de la tabla de ruteo. Cada nodo involucra un proceso que consiste únicamente en el desplazamiento de paquetes basándose en la información interna. El IP no puede proveer un retorno por reporte de errores hacia la fuente cuando una anomalía ocurre. Esta tarea es ejecutada por otro protocolo de Internet: El Protocolo De Internet Para Control De Mensajes (ICMP)[45].

El ICMP provee varias tareas para el desempeño del trabajo interno de redes IP. En adición a la principal razón para cual fue creado (regreso de reporte de fallas a la fuente de emisión), ICMP provee un método para pruebas de alcance a través del Internet (el ICMP Echo y mensajes de respuesta)[46], un método para incrementar la eficiencia de ruteo (el re-direccionamiento de mensaje ICMP)[47], un método para fuentes de información donde el datagrama tiene excedente por tiempo permitido para subsistir dentro del Internet (el tiempo excedido de mensaje ICMP)[48], y otras ayudas para mensajes.

De todo a todo el ICMP es parte integral para cualquier implementación IP, particularmente aquellas que corren en los ruteadores.

9.3. Protocolos De Ruteo Interno

Los protocolos de ruteo interno o IGPs operan dentro de los sistemas autónomos. En las siguientes secciones se describirá brevemente varios IGPs que son actualmente muy populares en redes TCP/IP.

9.3.1. RIP

Un protocolo de ruteo muy discutido dentro del ambiente IP es el protocolo para ruteo de información (RIP)[49]. El RIP fue desarrollado por Xerox Corporation a principios de los 1980's para su uso en redes con el sistema de red Xerox (XNS)[50]. Hoy en día muchas redes de PC usan protocolos de ruteo basados en RIP.

El RIP trabaja en ambientes pequeños debido a que presenta serias limitaciones cuando se utiliza para redes amplias. Por ejemplo, el RIP limita el número de saltos en el ruteador por cada dos servidores en una red de Internet a 16. El RIP es también lento cuando converge, le toma un tiempo relativamente largo para cambiar de red una vez que conoce todos los ruteadores.

---

[45] Internet Control Menssage Protocol, de sus siglas en inglés.
[46] ICMP Echo and Reply Menssage, ídem.
[47] ICMP Redirect Menssaje, ídem.
[48] ICMP Time Exeeded Menssage, ídem.
[49] Routing Información Protocol, de sus siglas en inglés.
[50] Xerox Network System, ídem.

Finalmente, el RIP determina el mejor camino a través del Internet para tomar únicamente el número de saltos entre los últimos dos nodos restantes hacia el destino. Esta técnica ignora las diferencias de velocidad en la línea, la utilización de esta, y todas las demás magnitudes, muchas de las cuales pueden ser factores importantes al escoger el mejor camino entre dos nodos. por esta razón, muchas compañías con amplias redes internas emigran a través de RIP para mas sofisticados protocolos de ruteo.

9.3.2. IGRP

Con la creación del protocolo interno para ruteo de gateway (IGRP) a mediados de 1980's, Cisco Systems fue la primer compañía en resolver los problemas asociados con el uso del RIP para el ruteo de datagramas entre los ruteadores internos.

El IGRP determina el mejor camino a través del Internet examinando el ancho de banda y el retraso para la conexión de redes entre los ruteadores. El IGRP converge más rápidamente que el RIP, evitando los ciclos (loops) causados por incompatibilidad sobre los próximos saltos de ruteo a seguir. Más, el IGRP no comparte las limitaciones de conteo para saltos del RIP.

Como resultado de esto y otras mejoras sobre el RIP, el IGRP es más amplio, complejo, y diverso topológicamente para desplazarse en los sistemas de redes internas.

Cisco posee hoy en día un IGRP avanzado para manejar el amplio crecimiento y los estados de misiones-críticas en las redes diseñados actualmente. Esta nueva versión de IGRP se le llama "Enhanced IGRP". Este combina el uso tradicional del protocolo de ruteo a distancia por vectores con la rapidez de las capacidades de re-ruteo presentada por los protocolos de ruteo para estados de enlace.

El IGRP avanzado consume significativamente menos ancho de banda que el IGRP por que éste es capaz de limitar el intercambio de información de ruteo para incluir únicamente los cambios en ésta. Adicionalmente, el IGRP avanzado es capaz de manejar la información de ruteo IPX del AppleTalk y Novell, tal como la información de ruteo IP.

9.3.3. OSPF

El OSPF fue desarrollado por la fuerza operante del área de ingeniería del Internet (IETF)[51] como remplazo del RIP. El OSPF se basa en el trabajo iniciado por Jonh McQuillan a finales de los 1970's y fue continuado por Radi Perlman y Digital Equipment Corporation (DEC) a mediados de los 1980's. Los principales vendedores de ruteadores soportan OSPF.

[51] Internet Engineering Task Force, de sus siglas en inglés.

El OSPF es un intradominio, un estado de enlace, y un protocolo de ruteo jerárquico. El OSPF soporta el ruteo jerárquico dentro de un sistema autónomo. El sistema autónomo puede ser dividido en áreas de ruteo. Un área de ruteo es típicamente una colección de una o más sub-redes que están cerradas relativamente. Todas las áreas podrán conectarse en si al área del backbone.

El OSPF provee rápido re-ruteo y soporta las máscaras de sub-red de variable amplia (VLSM)

9.3.4. Integración IS-IS.

El ISO 10589 (IS-IS) al igual que el OSPF es un intradominio, un estado de enlace, y un protocolo de ruteo jerárquico usado como el algoritmo de ruteo DECnet Phase V. En si es muy similar al OSPF. El IS-IS puede operar sobre una variedad de sub-redes de computadoras, incluyendo las transmisiones de enlaces LANs, WANs, y Point-to-Point.

La Integración IS-IS es la implementación del IS-IS que sólo acepta la función de los protocolos OSI. Ahora, la Integración IS-IS soporta ambos protocolos OSI e IP.

Al igual que todos los protocolos ruteables, la Integración IS-IS convoca a todos los ruteadores a correr un algoritmo simple de ruteo. El aviso del estado de conexión se envía por los ruteadores que ejecutan dicho protocolo incluyendo todos los destinos que llevan a cabo la tarea de transmisión ya sean los protocolos de red para la capa IP o los de la Capa OSI.

Los protocolos tales como ARP e ICMP para IP y el Sistema Final-al-Sistema Intermedio (ES-IS)[52] para el OSI podrá ser soportado por los ruteadores que ejecuten la Integración IS-IS.

9.4. Protocolos De Ruteo Exterior

9.4.1. EGP

Los EGPs se caracterizan por proveer el ruteo entre los sistemas autónomos del TCP/IP.

El primer protocolo de ruteo exterior general que existió dentro de la suite de los protocolos de Internet fue el EGP. Este provee una conectividad dinámica pero asume que todos los sistemas autónomos están conectados por una topología de árbol (Estrella Modificada), que fue el principio original del Internet pero no tan larga realmente.

[52] End System-to-Intermediate System, de sus siglas en inglés.

Aunque si bien, el EGP es un protocolo de ruteo dinámico, éste utiliza un diseño muy simple. No utiliza las magnitudes de la línea ni tampoco puede hacer decisiones inteligentes de ruteo. El ruteo IGP actualiza el contenido de la información con las redes que puede alcanzar. En otras palabras, éste especifica que redes pueden ser seguramente alcanzadas a través de los ruteadores asegurados del sistema. Todas estas pequeñas limitaciones deben ser consideradas hoy en día para los sistemas complejos de inter-redes, dada esta situación el EGP está siendo gradualmente eliminada a favor de un protocolo de ruteo conocido como BGP.

9.4.2. BGP

El protocolo de gateway fronterizo representa un atentado al problema de direccionamiento más serio de los EGPs. Tal como EGP, BGP es un protocolo de ruteo de intradominio creado para el uso de los ruteadores en el núcleo del Internet.

Nada parecido al EGP, el BGP fue diseñado para prevenir los "loops" en topologías arbitrarias y permitir la selección de ruteadores basadas en la política del sistema correspondiente.

El BGP fue co-autorado por la fundación Cisco, misma que aún continúa involucrada en su desarrollo. La última revisión del BGP, el BGP4, está diseñado para manejar los problemas escalables del crecimiento del Internet.

9.5. Mecanismos de operación TCP/IP

Como lo indica el modelo de referencia OSI, los protocolos (los cuales se componen de varias capas) son un altero de piezas colocadas unas sobre otras. Debido a esta estructura, los grupos de protocolos relacionados son llamados pilas o protocolos apilados.

Los datos pasan por debajo del la pila de una capa a la siguiente, mientras se trasmite a través de la red por la capa de protocolos con acceso a red. Las cuatro capas del modelo de referencia son habilitadas para distinguir entre las diferentes maneras en que los datos son manejados conforme pasan por debajo de la estructura del protocolo, desde la capa de aplicación hacia la línea física subyacente de la red.

En el punto remoto final, los datos pasan arriba de la pila para que los reciba la aplicación. Las capas individuales no necesitan conocer como las capas superiores o inferiores a ellas funcionan, lo único que necesitan conocer es cómo pasan los datos a ellas.

Cada capa en la pila adiciona la información de control (tal como la dirección de destino, los controles de ruteo, y la suma de control) para asegurar la entrega apropiada. Está información de control es llamada encabezado y/o trailer según se encuentre al frente o detrás de los datos a ser transmitidos.

Cada capa trata toda la información que recibe de la capa anterior como datos, y coloca su propio encabezado y/o trailer alrededor de esta información.

Estos mensajes resguardados son los que pasan a la capa inmediata inferior con información de control adicional, alguna de la cual puede ser regresada o derivada de una capa superior. Al tiempo que un mensaje sale del sistema. Debido al tiempo de transmisión en un enlace físico (tal como un cable), el mensaje original se envuelve en múltiples cobertores anidados para su resguardo - uno para cada capa de protocolo a través del cual los datos pasaron.

Cuando un protocolo utiliza los encabezados o trailers para empaquetar los datos de otro tipo de protocolo, se crea el proceso llamado encapsulado. Este proceso se representa en la ilustración 9-6.

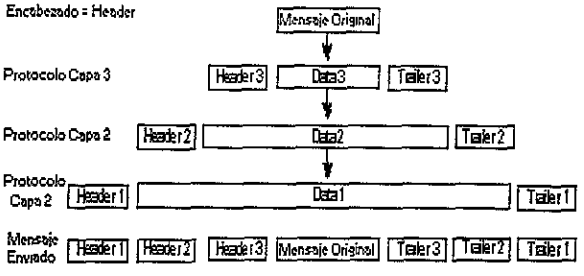


Ilustración 9-6 Encapsulado de Datos Enviados por Red.

Cuando se reciben los datos, sucede lo contrario. Cada capa se desmantela de su encabezado y/o trailer para después pasar los datos a la capa superior. Como la información fluye de inversamente a la pila, la información recibida de una capa baja es interpretada como un encabezado/trailer y datos. El proceso de remoción de encabezados y trailers de datos es llamado decapsulación. Este mecanismo habilita a cada capa para la transmisión de las computadoras-origen para comunicarse con su capa correspondiente en la computadora-destino. Capa en la computadora emisora se comunica con su homóloga en la computadora receptora a través de un proceso llamado comunicación punto-a-punto.[53]

Cada capa tiene responsabilidades y reglas específicas para llevar a cabo esas responsabilidades, y desconoce los procedimientos que siguen las otras capas. Una capa de transmisión es la que ejecuta las tareas y entrega el mensaje a la siguiente capa del protocolo apilado. Un mecanismo de direccionamiento es el elemento común que permite a los datos para ser ruteados a través de varias capas hasta que alcanza su destino.

[53] Point Per Point, de sus siglas en inglés.

Cada capa también posee una estructura independiente de datos. Conceptualmente, una capa ignora las estructuras de datos utilizada por las capas inferiores y superiores. En realidad, las estructuras de datos de una capa es diseñada para ser compatible con las estructuras usadas por las capas que la rodean para una más eficiente transmisión de datos. Aún cada capa posee su propia estructura de datos y su propia terminología para describir esas estructuras.

La siguiente sección describe el modelo de referencia para Internet más detalladamente.

9.6. El modelo de referencia de Internet.

Como se había mencionado anteriormente, el modelo de referencia para Internet contiene cuatro capas: la capa de acceso de red, la capa de Red de redes, la capa de transporte de servidor-a-servidor, y la capa de aplicación.

A continuación, se describe la función de cada capa detalladamente, comenzando por la capa de acceso a la red y trabajando de manera ordenada hasta la capa de aplicación.

9.6.1. Capa de acceso a la red

La capa de acceso a la red es la capa más baja en el modelo de referencia. Esta capa contiene los protocolos que la computadora usa para enviar datos a las demás computadoras y componentes que están conectados a la red. Los protocolos de esta capa realizan tres funciones distintas:

- ⊗ Definen como utilizar la red para transmitir un marco que es la unidad de datos que cruza la conexión física.
- ⊗ Intercambian datos entre la computadora y la red física.
- ⊗ Envían datos entre dos dispositivos en la misma red. Para enviar datos en la red local, los protocolos de la capa de acceso a la red usan: las direcciones físicas de los nodos de la red. Una dirección física es almacenada en la tarjeta del adaptador de red propiedad de la computadora u otro dispositivo y éste es un valor que es codificado en la tarjeta adaptador por el fabricante.

A diferencia de los protocolos de alto nivel, los protocolos de la capa de acceso a la red deben entender los detalles de la red física subyacente, tal como la estructura de paquetes, el tamaño máximo de marco, y los esquemas de la dirección física de red que se usan. Comprender los detalles y las restricciones de la red física asegura que estos protocolos puedan darle el formato correcto a los datos para ser trasmitidos a través de la red.

9.6.2. Capa de Red de redes (Internetwork)

En el modelo de referencia de Internet, la capa sobre el ídem de acceso a la red es llamada "**capa de red de redes**". Esta capa es la responsable de rutear mensajes a través de las redes. Dos tipos de componentes son responsables de esto. El primer componentes es llamado gateway (Puerta), que es una computadora que posee dos tarjetas adaptadoras de red.

Esta computadora acepta los paquetes de una red por una tarjeta adaptadora de red y rutea estos paquetes a una red diferente vía una segunda tarjeta adaptadora de red.

El segundo componente es un ruteador, el cual es un componente de hardware dedicado a pasar los paquetes de una red a otra diferente. Este par de términos es intercambiado frecuentemente, pero existen diferentes distinciones en su habilidad para rutear paquetes y en sus roles, como podremos apreciar en los firewalls[54].

Los protocolos de la capa de Red de redes proveen un servicio de datagramas de red. Los datagramas son paquetes de información que comprenden un encabezado (Header), datos (data) y un remolque (Trailer). El encabezado contiene la información, como la dirección de destino que la red necesita para rutear el datagrama. Un encabezado puede contener también otra información, tal como la dirección fuente y las etiquetas de seguridad. Los remolques típicamente contienen un valor de suma de verificación, el cual se utiliza para asegurar que los datos no han sido modificados durante su tránsito.

Las entidades de comunicación - como pueden ser las computadoras, sistemas operativos, programas, procesos, o gente - que usan los servicios de datagrama deben especificar la dirección de destino (utilizando la información de control) y los datos para cada uno de los mensajes a transmitirse. Los protocolos de la capa de Red de redes empaquetan el mensaje en un datagrama y lo envían.

Un servicio de datagrama no soporta ningún concepto de sesión o conexión. Una vez que un mensaje es enviado o recibido, el servicio no conserva la memoria de la entidad con la cual se estaba comunicando. Si ésta es necesaria, los protocolos en la capa de transporte servidor-a-servidor la mantienen. La habilidad para retransmitir datos y verificar si existen errores es mínima o inexistente en los servicios de datagrama. Si durante la transmisión mediante el uso del valor la suma de verificación, simplemente ignora (o se suprime) el datagrama sin notificar a la capa superior receptora.

[54] Ver. Firewalls y seguridad en Internet, Cap. 11 , Pag. 156.

9.6.3. Capa de transporte servidor-a-servidor

La capa de protocolo justamente encima de la capa de Red de redes es la capa de transporte servidor-a-servidor. Este es el responsable de proveer íntegramente los datos nodo-a-nodo y provee un servicio de comunicación de alta confiabilidad para las entidades que quieren transmitir una conversación extendida de dos-vías.

Adicionalmente a las funciones de transmisión y recepción, la capa de transporte servidor-a-servidor usa comandos abiertos y cerrados para iniciar y terminar una conexión Esta capa acepta la información para ser transmitida como un stream de caracteres, y regresa la información al receptor como tal.

El servicio emplea el concepto de una conexión (o circuito virtual). Una conexión es el estado de la capa de transporte servidor-a-servidor que existe entre el tiempo en que la computadora de recepción acepta un comando de apertura y el tiempo en que el comando de cierre emitido por otra computadora.

9.6.4. Capa de aplicación

La capa superior en el modelo de referencia de Internet es la capa de aplicación. Esta capa provee funciones para el usuario o sus programas, y es altamente específica para la aplicación que se está ejecutando. Provee los servicios que las aplicaciones usuarias utilizan para comunicarse sobre la red, y es la capa donde reside el proceso de acceso-a-usuarios de la red. Estos procesos incluyen todos aquellos que están directamente relacionados a la interacción de los usuarios, así como otros procesos de los cuales los usuarios no están enterados.

Así también, esta capa incluye todos los protocolos de aplicación que son usados por los mismos de la capa de transporte de servidor-a-servidor al transmitir datos. Otras funciones que realiza es el proceso de datos para el usuario, tal como la encriptación y descriptación de datos y la compresión y descompresión, que reside en la capa de aplicación.

La capa de aplicación también administra las sesiones (conexiones) entre las aplicaciones de cooperación. En la jerarquía del protocolo TCP/IP, las sesiones no se identifican como una capa separada, ya que estas funciones son ejecutadas por la capa de transporte servidor-a-servidor. En lugar de usar el termino "**sesión**", el TCP/IP usa el término "**socket**" y "**port**" para describir su camino (o el circuito virtual) sobre el cual las aplicaciones cooperativas se comunican. Sin embargo, en la descripción de un sistema firewall, hacemos la distinción entre sesiones y puertos. Una sesión es una conexión sobre un puerto TCP o UDP que se ejecuta entre dos computadoras, y una de las cuales está protegida por este sistema.

La mayoría de protocolos de aplicación en esta capa proveen los servicios al usuario, y los nuevos servicios son adicionados frecuentemente. Para el intercambio de datos se habilitan las aplicaciones de cooperación, que deben acordar sobre como están representados los datos. La capa de aplicación es la responsable de estandarizar la presentación de datos.

En la siguiente sección se trata de resumir la historia del TCP/IP así como definir la suite del protocolo de Internet usando el modelo de referencia.

9.7. Como trabaja el TCP/IP

El diseño del TCP/IP oculta la función de sus capas a los usuarios - esto se relaciona con la obtención de datos a través de un tipo específico de red física (tal como Ethernet, Token Ring, etc.). Este diseño reduce la necesidad de re-escribir los niveles altos de una pila TCP/IP cuando una nueva tecnología física de red es introducida (tal como ATM and Frame Relay).

Las funciones realizadas a este nivel incluyen la encapsulación de datagramas IP en marcos que son transmitidos por la red. También además se mapea las direcciones IP a direcciones físicas utilizadas en la red. Uno de los puntos fuertes del TCP/IP es su esquema de direccionamiento, el cual únicamente identifica cada computadora en la red. Esta dirección IP debe convertirse en cualquier dirección que sea apropiada para la red física sobre la cual el datagrama es transmitido.

Los datos para ser transmitidos se reciben de la capa de Red de redes. La capa de acceso de red se responsabiliza del ruteo y debe adicionar su información a los datos. La información es añadida en el formato de un encabezado, que se adjunta al principio de los datos.

En Windows NT, los protocolos de esta capa aparecen como driver NDIS y sus programas relacionados. Los módulos que son identificados por los dispositivos de red son encapsulados y enviados con los datos a la misma, mientras que los programas relacionados realizan las funciones relacionadas con el mapeo de dirección.

9.7.1. Capa de Red de redes

El más brillante de los protocolos conocidos del TCP/IP en la capa de Red de redes es el protocolo de Internet (IP), el cual provee el servicio de transmisión básico de paquetes por todas las redes TCP/IP. Adicionalmente al direccionamiento físico de nodos usada en la capa de acceso de red, el protocolo IP implementa un sistema de direccionamiento lógico de servidores llamado direcciones IP. Las direcciones IP son usadas por las capas altas y la de Red de redes para identificar los dispositivos y ejecutar el ruteo de Red de redes. El protocolo de resolución de direcciones (ARP) permite al IP identificar la dirección física que corresponde a una dirección IP dada.

El IP es usado por todos los protocolos en las capas inferiores y superiores al enviar datos, lo cual significa que todos los datos TCP/IP fluyen a través del IP cuando se envía y recibe, a pesar de su destino final.

9.7.2. Protocolo de Internet: ruteo de datagramas (IP)

El IP es un protocolo sin conexión, lo cual significa que el IP no ejecuta el intercambio de la información de control (llamado handshake) para establecer una conexión punto-a-punto antes de transmitir los datos. En contraste, un protocolo orientado a la conexión intercambia la información de control con la computadora remota para verificar que esta lista para recibir datos y antes enviarlos. Cuando el handshake es aplicado exitosamente, la computadora indica que la conexión es establecida. El IP actualiza los protocolos en otras capas para establecer la conexión si se requiere de un servicio orientado a la conexión.

El IP además actualiza los protocolos en otras capas para proveer detección de errores y recuperación de errores. Debido a que no contiene el código para la detección y recuperación. Se dice que el IP es un protocolo poco fiable.

Las siguientes funciones realizadas en esta capa:

- Define el datagrama, que es la unidad básica de transmisión en el Internet. El protocolo TCP/IP fue construido para transmitir datos sobre el ARPANET[55], que fue una red formada por intercambio de paquetes. Un paquete es un bloque de datos que se transportan con la información necesaria para entregarlo, en manera similar al servicio postal donde una carta es enviada a la dirección que le fue escrita en un sobre. Una red de intercambio de paquetes utiliza la información de direccionamiento en los paquetes para conmutarlos de una red física a otra, moviéndolos hacia su destino final. Cada paquete viaja en la red independientemente de cualquier otro paquete. El datagrama es el formato de paquete definido por el IP.
- Definir el esquema de direccionamiento de Internet. El IP entrega el datagrama verificando la dirección de destino en el encabezado. Si la dirección corresponde a un servidor directamente conectado a la red, el paquete es enviado directamente a su destino. Si la dirección destino no pertenece a la red local, el paquete pasa a un gateway para ser entregado. Los gateways y ruteadores son dispositivos que intercambian paquetes entre diferentes redes físicas.

[55] Advanced Research Projects Agency Network, de sus siglas en inglés.

Decidir que gateway usar, se denomina rutear. El IP ejecuta la decisión de ruteo para cada paquete en forma individual.

- Ø Mueve los datos entre la capa de acceso a la red y la capa de transporte servidor-a-servidor. Cuando el IP recibe un datagrama que esta direccionado al servidor local, deberá pasar la porción de datos del datagrama al protocolo correcto del la capa de transporte servidor a servidor. Esta selección se hace mediante el uso del número asignado al protocolo en el encabezado del datagrama. Cada protocolo de la capa de transporte servidor-a-servidor posee un número único de protocolo que identifica su IP.

- Ø Ruteo de datagramas a servidores remotos. Los gateways de Internet (y periféricos mas precisamente) son comúnmente referidos como ruteadores IP porque utilizan el IP para el ruteo de paquetes entre redes. En el ámbito tradicional de TCP/IP, sólo existen dos tipos de componentes en la red:

gateways y servidores. Los gateways envían los paquetes entre las redes, los servidores no. De cualquier modo, si un servidor esta conectado a más de una red (llamado servidor multi-homed[56]), éste puede desplazar los paquetes entre las redes. Cuando un servidor multi-homed desplaza los paquetes, está actuando como un gateway y será considerado como gateway.

- Ø Fragmenta y reconstruye datagramas. Como un datagrama es ruteado a través de diferentes redes, pudiera ser necesario modular el IP en un gateway para dividir un datagrama en partes más pequeñas. Un datagrama recibido de una red puede ser demasiado grande como para transmitirlo en un paquete simple a una red diferente. Esta condición únicamente ocurre cuando un gateway conecta redes físicamente diferentes.

Cada tipo de red posee una unidad de transmisión máxima (MTU), la cual es el paquete más grande que se puede transmitir. Si el datagrama recibido de una red es más grande que el MTU de la otra red, es necesario dividir el datagrama en fragmentos más pequeños para la transmisión. Este proceso de división es llamado fragmentación.

[56] multi-sesion, de su traducción al español.

9.7.3. Protocolo Internet: mensajes de error y control (ICMP)

El Protocolo Internet: mensajes de error y control es parte de la capa de red de redes (Internetwork) y utiliza la destreza del datagrama de entrega al IP para enviar los mensajes. El ICMP envía mensajes que realizan el seguimiento del control, reporte de errores, y funciones informativas para la suite del protocolo TCP/IP:

- ⊕ Control de flujo. Cuando un datagrama arriva demasiado rápido para ser procesado, el servidor destinatario o un gateway intermediario envía de regreso un mensaje fuente ICMP de apagado al remitente. Este mensaje da instrucciones a la fuente de detener temporalmente el envío del datagrama.
- ⊕ Detecta destinos inalcanzables. Cuando un destino es inalcanzable, la computadora que detecta un problema, envía un mensaje de destino inalcanzable a la fuente del datagrama. Si este destino es una red o un servidor, el mensaje es enviado por un gateway intermedio. Pero si el destino es un puerto inalcanzable, lo enviará el servidor destino.

9.7.4. Capa de transporte servidor-a-servidor

La capa de protocolo justamente arriba de la capa de red de redes (Internetwork) es la capa servidor a servidor. Es responsable de la integridad de datos punto-a-punto. Los dos protocolos más importantes en esta capa son el protocolo de control de transmisión (TCP) y el protocolo de datagrama de usuario (UDP).

El TCP provee confiabilidad en conexiones full-duplex[57]y servicio, al asegurarse que los datos sean representados cuando resulta un error en la transmisión (detección y corrección punto a punto). Además, el TCP autoriza a los servidores mantener conexiones simultáneas múltiples. Cuando no se requiere una conexión de error, el UDP provee un servicio desconfiable de datagrama (sin conexión) que se incrementa a través de toda la red en la capa de transporte servidor-a-servidor.

Ambos los protocolos entregan los datos entre la capa de aplicación y la capa de red de redes. Los programadores de aplicaciones pueden escoger qué servicio es el apropiado para sus aplicaciones específicas.

[57] Conexiones proporcionadas por el servicio de streamer, propio de la suite TCP/IP, que permiten la transferencia concurrente en ambas direcciones.

9.7.5. Protocolo de datagrama de usuario (UDP)

El protocolo de datagrama de usuario da programas de aplicación con acceso directo a un servicio de entrega por datagramas, como el servicio de entrega que provee el IP. Este acceso directo permite a las aplicaciones intercambiar mensajes sobre la red con un mínimo de protocolos generales.

El UDP es un protocolo de datagrama sin conexión desconfiable. "**desconfiable**" meramente significa que el protocolo no posee técnicas para la verificación de aquellos datos que se hallan alcanzado correctamente al final de la otra red. Dentro de tu computadora, el UDP puede entregar datos correctamente.

¿Por qué los programadores de aplicaciones eligen el UDP como un servicio de transporte de datos? Existe un buen número de buenas razones. Si la cantidad de datos a transmitir es pequeña, la generación de conexiones creadas y aseguradas fiablemente pueden ser mejores para entregar datos que trabajar para volver a retransmitir el conjunto entero de datos. En este caso, el UDP es el protocolo más eficiente de escoger en la capa de transporte servidor-a-servidor.

Las aplicaciones que corresponden al modelo "**pregunta-respuesta**" son excelentes candidatas para usar UDP. La respuesta puede ser utilizada como un reconocimiento positivo a la pregunta. Si no se recibe respuesta dentro de un cierto periodo de tiempo, la aplicación todavía vuelve a gestionar la respuesta posible. Aún otras aplicaciones proveen sus propias técnicas para la entrega fiable de datos y no requieren del servicio de los protocolos de la capa de transporte. El imponer otra capa de reconocimiento en cada tipo de estas aplicaciones es redundante.

9.7.6. Protocolo de control de transporte (TCP)

Las aplicaciones que requieren del protocolo de transporte servidor-a-servidor para proveer una entrega fiable de datos utilizan el TCP porque éste verifica precisamente que los datos son entregados a través de la red correctamente y en que secuencia. El TCP es confiable, orientado a la conexión, y es un protocolo común de bytes.

9.7.7. Capa de aplicación

Las capas de protocolos de aplicación TCP/IP más ampliamente conocidas e implementadas son:

* Protocolo de transferencia de archivos[58](FTP). Función básica interactiva de transferencia de archivos entre servidores.
* Protocolo de servicio en terminal remota[59](Telnet). Permite al usuario ejecutar sesiones terminales con servidores remotos.
* Protocolo de manejo de red simple[60](SMTP). Soporte básico para el servicio de entrega de mensajes.
* Protocolo de transferencia de hipertexto[61](HTTP). Soporta el transporte inferior-superior de archivos formados de la mezcla de textos y gráficos. Utiliza una conexión estática y un protocolo orientado a objetos con comandos simples que soportan la selección y transporte de objetos entre el cliente y el servidor.

Adicionalmente a los protocolos ampliamente conocidos, la capa de aplicación incluye los siguientes protocolos:

* Servicio de Nombre de Dominio[62](DNS), además llamado servidor de nombres, es un sistema de base de datos distribuida en línea que se utiliza para transformar nombres de componentes en red, en direcciones IP que puedan leer los usuarios, ejemplo nombre del servidor: www.unam.mx, dirección IP: 132.248.10.4.
* Protocolo de información de ruteo[63](RIP). El ruteo es centralizado a la manera que el TCP/IP trabaja. El RIP es utilizado por los dispositivos de red para intercambiar información de ruteo.
* Protocolo de administración simple de red[64](SNMP). Un protocolo que es utilizado para recopilar la información de administración de los dispositivos de red.
* Sistema de archivos en red[65](NFS). Un sistema desarrollado por Sun Microsystems.

El cual permite a las computadoras montar unidades de información (drive´s) en servidores remotos y operar como si fueran unidades locales.

---

[58] File Transfer Protocolo, de sus siglas en inglés.
[59] Terminal Emulation Network, ídem
[60] Simple Mail Transfer Protocol, ídem
[61] HyperText Transfer Protocol, ídem
[62] Domain Name Service, ídem.
[63] Routing Information Protocol, ídem
[64] Simple Network Management Protocol, ídem
[65] Network File System, ídem

Algunos protocolos, tales como Telnet y FTP, pueden ser usados únicamente si el usuario posee conocimientos de la red. Otros protocolos, como el RIP, corren sin que el usuario tenga conocimiento de que existe. Encapsulado de Paquetes y Unidad Máxima de Transmisión (MTU)

Antes un datagrama podía transmitirse a través de un salto de red, siendo encapsulado dentro del encabezado(s) (Header) requerido por la tecnología de red, como se muestra en la Ilustración 9-7. Por ejemplo, entrecruzamos un frame 802.3 o 802.5 y un datagrama que incorpora la información de enlace en los encabezados y el remolque de MAC.

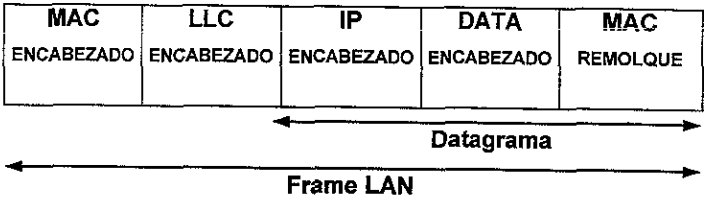


Ilustración 9-7 Datagrama incorporado a un frame de LAN.

Como hemos podido apreciar en capítulos anteriores, cada LAN y WAN tecnológicamente imponen un diferente límite de tamaño en sus Frames. El IP transmite un datagrama completo en un frame único, de modo que el tamaño del marco máximo restringe el tamaño de los datagramas que el IP puede enviar a través de un medio particular.

El tamaño de un datagrama es igual a:

[El Tamaño del Frame] - [El T. Del Encabezado MAC] - [El T. Del Encabezado LLC[66]] - [El T. Del Remolque MAC]

Al máximo tamaño de un datagrama para un tipo de red en común se le denomina Unidad Máxima de Transmisión o MTU. El Ethernet tiene un MTU de 1500 octetos. El 802.3, tiene un MTU de 1492 octetos, El FDDI, tiene un MTU de 4352 octetos, el 802.4, tiene un MTU de 8166 octetos, y el SMDS, tiene un MTU de 9180 octetos.

[66] LLC Link Layer Control, de sus siglas en inglés.

9.8. Funciones IP

En esta sección se describen las funciones que realiza la capa IP. En la Ilustración 9-8 se presenta el sumario de las funciones que desempeña el IP, ilustrando con nubes y rectángulos, se comienza con la implementación de diálogos interactivos con una estación de trabajo SunMicrosystems o similar que utilice un sistema operativo UNIX; debido a que la Internet inició sus servicios en este tipo de servidores.

Estas líneas de operación son idénticamente similares a los comandos que entablan diálogo en otros muchos tipos de sistemas computacionales.

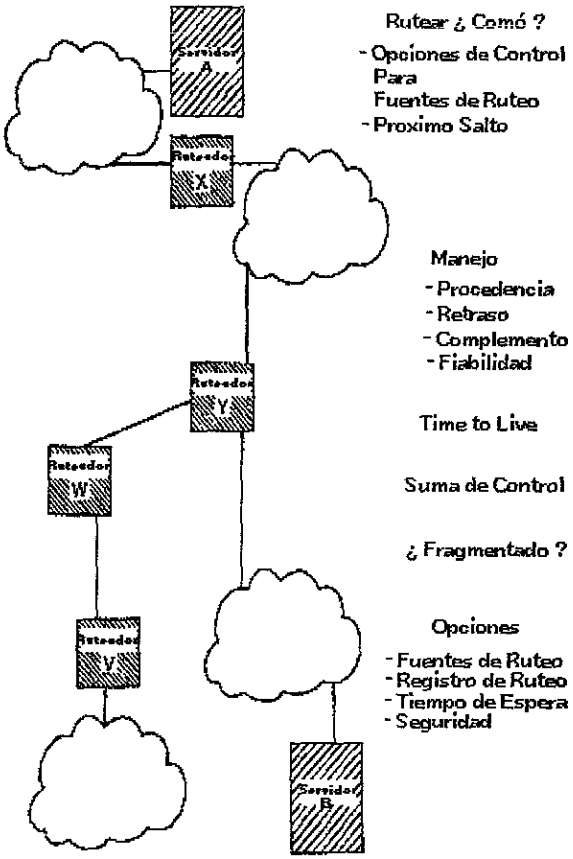


Ilustración 9-8 Funciones de Ruteo IP.

9.8.1. Función Primaria IP

La función primaria del IP es la de aceptar los datos de una fuente TCP o UDP de un servidor (host) , crear un datagrama y rutearlo a través de la red.

El IP en el servidor destino entrega los datos al recipiente TCP o UDP. Y el software IP rutea los datos a su destino usando dos mecanismo:

Máscaras de red (Netmasks).

Búsqueda de direcciones (Lookup).

9.8.2. Máscaras de Red (Netmasks)

Recordemos que las máscaras de una red o sub-red, en estos casos son una secuencia de 32 bits, que se encuentran dentro de la dirección de red.

Así, si tenemos que una mascara de sub-red es:

11111111 11111111 11111111 00000000

Puede estar escrito en base hexadecimal como:

ff ff ff 00

Alternativamente, puede escribirse notación de punto decimales como:

255.255. 255.0

Para ver cómo la máscara de sub-red es utilizada, supongamos que tenemos nuestro servidor dentro de una LAN y tiene la dirección IP 123.36.12.27 con sub-red enmascarada ff ff ff 00.

Si quisiéramos enviar información al servidor con dirección IP 128.36.12.14, entonces la máscara nos dice que tanto la dirección-destino como la dirección fuente pertenecen a la misma sub-red 128.36.12. Entonces, pueden intercambiar tráfico directamente a través de la sub-red. Antes de que nuestro servidor pueda enviar información, la dirección IP tiene que estar transmitiendo con su dirección física de LAN. El IP coincide y enlaza las direcciones físicas que están almacenadas en la Tabla de Traducción del ARP. Si la Dirección física de destino no está actualmente asignada, nuestro sistema utiliza las funciones básicas del protocolo ARP para emitir una solicitud de información.

9.8.3. Búsqueda de Direcciones IP (Looking up)

¿Cómo podemos averiguar cuál es nuestra dirección IP y máscara de subred?. Estos parámetros son parte de la configuración básica de las interfaces tendidas en la sub-red. Por ejemplo, "suponga" que nuestro servidor es atendido vía Ethernet a través de una interface de red nombrada le0.

Examinando la información de la configuración para esa interface. En un Sistema Unix de muestra, el comando ifconfig se utiliza para situar o ver información de configuración para la interface le0[67].

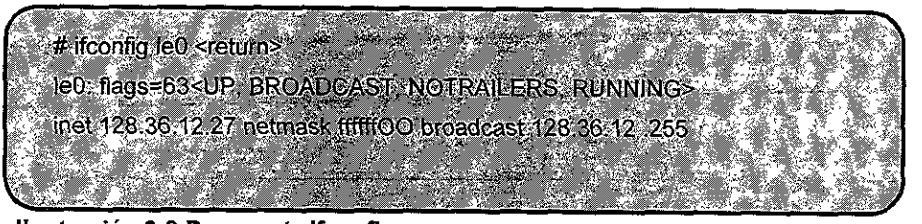


Ilustración 9-9 Respuesta Ifconfig

La respuesta presenta que la dirección IP asociada con esta interface es 128.36.12.27. La máscara de sub-red está expresada como hexadecimal ffffff00, que es 255.255.255.0 cuando se escribe en notación de punto decimal, aquí hay que recordar que la Dirección 128.36.12.255 debe de ser usada para transmitir emisiones dentro de esta sub-red.

Es fácil de encontrar el comando ieconfig en cualquier sistema de UNIX, y también es posible encontrarlo cargado en otros sistemas operativos para red. Por ejemplo, el Software TCP de ftp para D.O.S. incluye un comando ieconfig que define y muestra las características de la red local y sus enlaces seriales, e interfaces X.25. Esta última ya discontinuada hoy en día por ATM.

Por otra parte, las interfaces en un sistema IBM AS/400 son configuradas por medio de menús, mientras que un Sistema IBM VMS combina la información de interface con otros parámetros de TCP e IP en un archivo único.

9.8.4. Operación de Tablas

Generalmente, un datagrama se adapta a su ruteo. Este tipo de funciones se manejan en los ruteadores adaptables donde lo primero que hacen antes de ejecutar el siguiente salto, buscan la mejor opción revisando la tabla de ruteo en el servidor-origen y en cada ruteador a lo largo del recorrido. Independientemente de la topología de red el datagrama podrá ser re-orientado automáticamente en cualquier momento incorporando flexibilidad y robustez a nuestro sistema.

[67] En sistemas UNIX, los nombres de las interfaces de red cambian debido al genero de su topología y a las variables de ambiente del propio sistema. Ejemplo: et0 para en la red Ethernet en el sistema A.I.X. 3.2. de IBM.

¿Cómo se construyen y se mantienen las tablas de ruteo?

Inicialmente, cada tabla es configurada manualmente con algunas direcciones de gateways conocidas y una dirección de valor por omisión para ejecutar un alto a cualquier destino que no esté listado. Para redes pequeñas, solamente se necesitan las direcciones de los gateways estáticos. En redes medias y de banda ancha se necesitan tablas de ruteo que cambien dinámicamente durante la operación. El cambio es automatizado por medio de un ruteador RIP que permite a los ruteadores intercambiar información unos con otros y compilar automáticamente las direcciones de los gateways disponibles en las tablas de ruteo.

Hoy en día el hecho de no singularizar el protocolo de ruteo en las redes permite seguir la filosofía de Internet donde cualquier organización tiene la libertad de escoger cualquier protocolo de ruteo interno que requiera, alentando así a muchas compañías vendedoras de ruteadores a la experimentación y la invención de muchas mejoras en sus productos.

9.8.5. Tablas de Ruteo (Routing Tables)

Ahora supongamos que queremos comunicarnos con un servidor cuya dirección IP es 192.35.89.5. Claramente no está en nuestra LAN. En este caso el IP tiene que consultar las tablas de ruteo. ¿Qué comando va utilizar? Para averiguar, podemos utilizar el comando - netstat - para obtener una impresión de la Tabla de ruteo en nuestro servidor local:

¿De quien es la dirección IP 128.36.12.27?

```
#netstat -nr <return>
Destination      Gateway           Flags    Refcnt   Use      Interface
default          128.36.12.1       UG       0        21325    le0
127.0.0.1        127.0.0.1         UH       1        130      lo0
128.36.12.0      128.36.12.27      U        20       22199    le0
192.35.89.0      128.36.12.1       UG       0        29       le0
130.132.0.0      128.36.12.2       UG       3        26621    le0
128.36.17.0      128.36.12.1       UG       0        0        le0
```

Ilustración 9-10 Respuesta del Comando netstat.

Cada gateway provee información acerca del ruteo a un destino individual. Un destino puede ser una red, una subred, o un servidor individual. Un gateway de valor por omisión (default) o "**comodín**" también puede ser incluido y así puede ejecutar un itinerario a cualquier destino que no sea explícitamente listado en la tabla. Los gateways individuales permiten tomar una la dirección más cercana a la tabla de ruteo. Recordemos que todas las direcciones que inician con 127 serán utilizadas para pruebas de retorno (loopback).

Aquí podemos ver que el primer destino en la tabla es una dirección loopback.

El destino 128.36.12.0 es la LAN dentro de la cual se encuentra incluido nuestro servidor. El ruteador contiene la dirección de este servidor. Observe que si el servidor posee varias interfaces de red, habrá un gateway por cada una de éstas.

El siguiente destino, 192.35.89.0, identifica una red remota Clase C. Esta red es alcanzada a través de un gateway en la dirección 128.36.12.1. El servidor que originalmente queremos alcanzar tiene una dirección IP de 192.35.89.5 y éste se encuentra enlazado por la dirección-destino, así que el tráfico dirigido a ese servidor deberá enviarse a través de este gateway.

El destino 130.132.0.0 es una red remota Clase B y se alcanza a través de un gateway con dirección IP 128.36.12.2. El destino 128.36.17.0 pertenece a una sub-red de la misma Clase que la sub-red local, y es alcanzada a través del gateway con la dirección IP 128.36.12.1.

El gateway marcado con el valor por omisión es el más importante de todos. Ya que cualquier tráfico que no sea específicamente enviado por otro gateway de la tabla de ruteo será enviado a la dirección default.

Las banderas dicen si un itinerario está arriba o mejor dicho es utilizable (U), y si el destino es un servidor (H) o un gateway (G)

El Refcnt contabiliza el número de sesiones activas actuales de dicho itinerario. La columna de Use marca la cantidad de paquetes enviados dentro del itinerario. La interface le0 es una interface lógica utilizada para las pruebas de loopback.

Como práctica verifique los servidores de su red local tengan un ruteador único, es frecuente encontrar que éstos continúan con exactamente tres gateways: Un loopback de destino, un gateway para la red local, y un gateway con valor por omisión para todo el tráfico no-local.

Cuando el IP busca la dirección-destino, las primeras búsquedas son a través de la tabla de ruteo. Para ver si hay un gateway para enlazar a dicha dirección. Si lo hay, entonces este gateway permitirá el paso del tráfico. Si no, entonces el IP buscará un gateway correspondiente a la red de destino, y si no fuese encontrada, se utilizará el gateway por default.

9.8.6. Tablas de Servidores (Host Tables)

Los servidores generalmente trabajan con algunas direcciones de gateways estáticos. ¿Pueden éstos ejecutar cambios dinámicos? En el capítulo de Protocolos de Ruteo Interno, veremos como un ruteador automáticamente notifica al servidor la existencia de otro ruteador que provee trayectorias más eficientes a un destino en específico.

Además, un servidor debe de ser lo suficientemente ingenioso para notar cuando un ruteador local se encuentra saturado y así verificar una nueva ruta de encause para salir del dominio de la red lo más rápido posible.

Un servidor puede ser copartícipe del ruteo dinámico ejecutando una serie de procesos que verifican la situación actual del ruteador local por medio de la emisión de mensajes ICMP. El servidor puede utilizar esta información para actualizar su propia tabla de ruteo. Sin embargo, hay que recordar que este tipo de servicios ocupa recursos del sistema; un servidor así puede terminar por almacenar una gran cantidad de información extraña que no resulta de mejores decisiones de ruteo y aminora la velocidad de búsqueda en la tabla del sistema.

9.9. Desempeño del Internet

El desempeño del Internet depende de la cantidad de recursos disponibles eficientemente entre los servidores y los ruteadores. Estos recursos son:

- La transmisión por ancho de banda.
- La memoria Buffer.
- El procesamiento del CPU.

Los mecanismos perfectos del protocolo son desconocidos. Ya que el diseño de los protocolos involucra "**trueques**" ganando y perdiendo eficiencia al inter-operar las redes de computadoras.

9.9.1. Ancho De Banda

El IP hace un uso eficiente del ancho de banda, debido a que los datagramas que utiliza para el transporte de datos, después de un salto al ruteador más próximo, pueden transmitirse rápidamente gracias a su disponibilidad de banda. No hay desperdicio ya que se reserva un ancho de banda específicamente para el tráfico o espera las llamadas de reconocimiento origen-destino, serían embalados para una capa orientada a la conexión a nivel 3 del protocolo OSI.

Aún más, hay nuevos protocolos de ruteo para el IP capaces de dividir el tráfico sobre trayectorias múltiples y poder escoger de manera mas dinámica las vías de comunicación despejadas evitando las aglomeraciones de un ruteador o sobrecargar un enlace de datos.

El uso de estos protocolos ayudará a mantener el mejor uso posible de los recursos de transmisión disponibles. Debido a que existirán pocos mensajes de control por encima de los datos presentados por los mensajes de error del ICMP, debido a que éste es la única fuente de control para el tráfico en la red. Existen también algunos caracteres distintivos potencialmente negativos. Bajo la carga pesada, un datagrama puede amontonarse sobre las colas de espera de un ruteador y entregar a tiempo el mensaje fuente a su destino, siendo posible que si se exceden los datagramas en el tiempo de espera éstos serán desechados, obligando al TCP a que se retransmitan los datagramas, incrementando así la carga y disminuyendo la productividad efectiva.

Obsérvese que una vez aglomerada la red, el datagrama se retarda y su entrega será menos confiable. Las retransmisiones del TCP pueden tener el efecto de mantener una red aglomerada. Afortunadamente, algunos algoritmos efectivamente desarrollados por P. Karn y V. Jacobson en la Universidad de Stanford, hacen que el TCP responda al congestiónamiento inmediatamente suprimiendo la cantidad de información que es enviada, retrocediéndola y reduciendo la velocidad de la tasa de retransmisión. Estos algoritmos tienen una significativa repercusión en el desempeño de la red y se han puesto como una parte requerida del estándar del TCP.

El protocolo ICMP también provee auxilio para la sobrecarga de red durante la congestión, los mensajes ICMP avisan al origen que trasmita a un ritmo más lento las unidades de datos UDP y TCP.

Hoy en día es muy importante, ya que los proveedores de ruteadores compiten ofreciendo productos capaces de procesar miles de datagramas por segundo. Para asegurar su desempeño, se debe de configurar una red de TCP/IP de modo que la carga máxima esperada en un ruteador sea de 50170 d/seg, de capacidad aproximada.

9.9.2. Buffer De Memoria

Una vez que el IP ha transmitido un datagrama, es responsabilidad del buffer desocupar el área de memoria asignada para los datos siendo ésta disponible para reutilizarse de inmediato. Sin embargo, el IP de un servidor-destino tendrá que detener un proceso logrando así asignar un espacio de buffer mientras se reúne un datagrama fragmentado. Los problemas de congestión pueden surgir cuando un ruteador interconecta una red rápida a una red lenta. Los datagramas de la red rápida puede inundar los buffers del ruteador en cuestión de la red lenta.

Esto comúnmente ha ocurrido cuando se conecta una LAN a un circuito WAN. Hoy en día las tecnologías de redes WAN: ISND, T1, FRAME RELAY y SMDS ofrecen la flexibilidad para interoperar redes LAN y WAN manteniendo el suficiente ancho de banda para manipular el tráfico.

9.9.3. Procesos del CPU

Existe un área pequeña del CPU para el proceso de los datagramas. El análisis del encabezado se realiza directamente. El direccionamiento de 32-bit se utiliza para asignar la velocidad de alcance en la tabla de ruteo. No hay necesidad de obtener software muy elaborado para lograr interrupciones (timeouts) y retransmisiones cuando se utiliza una capa de red orientada a la conexión. Sin embargo, debido a que se poseen circuitos virtuales y una gama de servicios IP, se requiere de un ruteo dinámico para ejecutar un salto próximo en la tabla de ruteo. El tiempo consumido durante el proceso de enrutamiento depende de la complejidad del algoritmo de ruteo.

El encauzado que se tiene en cuenta condiciona la productividad y la demora de los datos, intentando balancear la carga de tráfico, debido a esto y de acuerdo a las preferencias de servicio al usuario se requiere mucho más poder de procesamiento. Afortunadamente, hoy en día el poder de procesamiento en los servidores es muy barato, y poseen altas prestaciones en robustez y desempeño del sistema. Con esto las prestaciones del software de ruteo pueden ser substanciales.

10. Administración de redes

La administración de redes es el proceso que se lleva a cabo para controlar una red de datos compleja de forma que se aumente su eficiencia y productividad.

El objetivo de fondo de la acción de redes, más allá de detectar y corregir fallas, es convertir a la red en una herramienta de trabajo confiable para las organizaciones. Al tener un sistema confiable, la eficiencia y productividad del usuario aumentan en forma considerable.

Surge la necesidad de administrar redes.

Conforme las redes departamentales de pocos usuarios se interconectan con otras redes departamentales dentro de la organización, ya sea en el mismo edificio o en edificios diferentes, mantener el control y la correcta operación de cada una de esas redes individuales, se convierte en una actividad compleja.

La red se vuelve compleja al tener un número grande de usuarios en localizaciones geográficas diferentes y con topologías de redes diversas operando entre sí. Existe todo tipo de problemas para mantener funcionando un sistema con esas características, desde fallas en el cableado hasta en las aplicaciones especializadas.

La **ISO** (International Standars Organization) define cinco áreas funcionales de administración de redes y podemos añadir una sexta que se denomina mesa de ayuda o *Help Desk.*

En este capitulo nos enfocaremos a la administración global de la red como lo es la administración de fallas, administración de rendimiento, administración de la configuración, administración de la seguridad. Y administración de costos.

Además de estudiar las técnicas y herramientas que se requieren para administrar efectivamente una red.

Primero, se examinará el Protocolo Simple de Administración de Red *(SNMP)*, Monitoreo Remoto *(RMON)*, y el Administrador de Información Básica *(MIB)*.

10.1. Protocolos de administración

10.1.1. SNMP.

Simple Network Management Protocol **(SNMP)**[68] fue originalmente desarrollado como un mecanismo para administración de redes *Ethernet* y *TCP/IP*. Desde que el primer estándar fue publicado en 1988, la aplicación de *SNMP* considerablemente se ha ido expandiendo, actualizando los procesos de autentificacion, control de acceso y otras características fundamentales de la administración de la red, introducida en 1993.

[68] Protocolo Simple de Administración de Red; de su traducción al español.

A través del uso de *SNMP*, se pueden direccionar los componentes básicos de la red entre nodos en el ámbito de comandos, obteniendo de esta manera información concerniente al funcionamiento y estado de la red. El *SNMP* provee el mecanismo para resolver problemas, analizando la actividad de la red, observando todas aquellas actividades tratando de resolver los problemas de la red.

10.1.1.1.Componentes básicos.

El *SMNP* es integrado por tres partes - Administración de Software, Agentes, Administrador de Información Básica *(MIB)* -, que más tarde representaría la base de datos para la administración de los componentes de la red. La administración de software en red *(NMS)* en la Workstation (estación de trabajo) y la anterior son responsables de la búsqueda de agentes para el uso de comandos *SNMP*. El agente de software representa uno o más programas modulares que operan en manera conjunta con la administración de los componentes de red, tales como *estaciones, bridges, ruteadores,* o *gateways.* Cada agente clasifica y administra los datos de información provistos por las últimas revisiones a la red. El *MIB,* representada como una base de datos, está estructurada en forma de árbol incluyendo grupos de objetos que pueden ser administrados en funciones específicas, el primer *MIB*, referente a *MIB-I* incluye 114 objetos organizados dentro de 8 grupos.

Grupo	*Descripción*
Sistema	Provee la identidad del vendedor, e incluye la configuración y el tiempo de administración desde la ultima vez que el sistema fue inicializado.
Interfaces	Provee las interfaces simples o múltiples de la red, obteniéndola en forma local o remota, y designa el rango de operaciones de cada interface.
Tabla de transdirección	Provee la traslación entre las direcciones de red y su equivalente físico.
Protocolo de Internet para el Control de Mensajes (ICMP)	Provee la cuenta de mensajes y errores ICMP.
Protocolo de Control de Transmisión (TCP)	Provee la información concerniente a transmisiones, y retransmisiones en las conexiones TCP, manteniendo una lista activa de conexiones.
Protocolo de Uso de Datagrama. (UDP)	Provee un contador de los datagramas trasmitidos, recibidos, o sin despachar.
Protocolo Exterior de Gateway (EGP)	Provee la cuenta de comunicaciones vía inter-router, tal que EGP genera mensajes locales, EGP recibe los mensajes con o sin error, y mantiene vigilada su información.

Tabla 10-1 MIB-I

La anterior lista marca los grupos soportados por el primer *MIB*; definida por la Organización de Estándares de Internet

Examinado la Tabla 10-1 es importante notar que el *SNMP* representa un protocolo en el ámbito de aplicación. Este protocolo corre a través del *UDP*, cual reside al frente del Protocolo de Internet *(IP)*, en el stack del *TCP/IP*.

La siguiente Tabla 10-2 ilustra la relación de los elementos *SNMP* en referencia al *Ethernet* con respeto al Modelo **OSI**.

Aplicación		SNMP
Presentación		
Sesión		
Transporte		UDP
Red		ICMP
Enlace de Datos		ETHERNET
Física		FISICA

Tabla 10-2 Relación de los elementos del protocolo SNMP al ETHERNET.

Examinado la tabla anterior, el *SNMP* representa el mecanismo de funcionamiento remoto para administrar la red. Estas operaciones son transportadas vía *UDP*, reduciendo el servicio de tiempo de conexión, el cual puede ser visto como un servicio paralelo provisto por el *TCP*, el cual opera al nivel 4 del **OSI**. A nivel 3, se provee el protocolo de Internet para el desarrollo del *SNMP*, controlando la fragmentación y reensamblando los datagramas, este último término se refiere a las porciones de mensajes. Localizado entre el *IP* y el nivel 4 se encuentra el *ICMP*. El *ICMP* es el responsable para la comunicación entre *TCP* y *UDP* e *IP* reportando el control de mensajes y errores.

Adicionalmente para ser transportado vía *UDP*, el *SNMP* puede ser transportado vía *IPX* de *Novell*, entre los *frames* de *Ethernet* a través del uso del *AppleTalk* y transportes **OSI**. En 1992, un nuevo *MIB*, referido *MIB-II*, comenzó con el estándar de Internet. *MIB-II* incluye los ocho grupos del *MIB-I* previo a la tabla anterior, y dos nuevos grupos - El de Administración Común de Información y Servicios Totales de TCP *(CMONT)*[69] y el *SNMP*. Cuando el esfuerzo en correr la administración **ISO** encima del *TCP/IP* se abandono, *CMON* fue esencialmente suministrado como grupo activo. La adición de un grupo *SNMP* permite a éste incluir una pista donde se incluya el control de tráfico y errores propios.

10.1.1.2.Operación.

El *SNMP* posee cinco comandos compuestos tales como el Protocolo de Unidades de Datos *(PDUs)*[70], que incluye **GetRequest**, **GetNetxRequest**, **SetRequest**, **GetResponse**, y **Trap**.

[69] Common Management Information and Services Over TCP, de sus siglas en inglés.
[70] Protocol Data Units, ídem

El *NMS* emite un **GetRequest** para recuperar el valor simple de un agente del *MIB*, mientras un **GetNetxRequest** se utiliza para pasar a través de los agentes de la tabla de *MIB*. Cuando un agente responde a cada llamada, se ejecuta un **GetResponse**.

El **SetRequest** suministra un administrador con el que se habilitan los agentes del *MIB*. Bajo la versión 1 del *SNMP*, ya no existen métodos de restricciones al uso de este comando, si éste es usado impropiamente pueden corromper los parámetros de configuración y dar los servicios de la red. Reconociendo este problema, muchos de los vendedores a elegir, no soportan el comando **SentRequest** en su *software* de agente *SNMP*. La introducción de la versión 2 del *SNMP* adiciona la autenticación tal como el encriptado, cuidando que los mensajes recibidos en el administrador de la red puedan ser reconocidos si fueron alterados, y a su vez verificados por el administrador apropiado Esto permite que el **SentRequest** sea soportado sin miedo por una persona no-autorizada, tomando el control de una sola porción de la red, o cuando un agente retorne información falsa.

Desde que el *SNMP* es un protocolo boteable, ha sido usado como mecanismo de alerta por los administradores, al presentar situaciones que requieran de su total atención. De otro modo, un intervalo largo de tiempo durante el boot del equipo en red se daría como resultado al verificar si ocurrió un serio problema que no halla sido detectado en un periodo relativamente largo en la red. El mecanismo usado par alertar al administrador es el comando **TRAP**, invocando a un agente del administrador de red.

Bajo la versión 2 del *SNMP*, se le adiciono dos *PDUs* - **GetBulkRequest** e **InformRequest**. El comando **GetBulkRequest** soporta la recuperación múltiple de filas con datos de los agentes *MIB* con una sola solicitud. El **InformRequest** habilita un administrador *PDU* para transmitir información "**no-solicitada**" por el administrador de otro sistema, permitiendo el soporte de administración distribuida en red, mientras que el *SNMP v2* era perfeccionado en una manera más propia.

Uno de los problemas asociados con el desarrollo de los *MIBs* fue la estandarización que tuvieron que realizar los vendedores al *software* para el manejo de las bases de datos con la información del equipo en red de varios vendedores. Aunque la estructura de árbol que tiene el *MIB* habilita el *software* para desarrollar un equipo en red de un vendedor, éste puede lecturar los demás equipos como genéricos del propio sistema, hacer esto requiere un poco de esfuerzo y en ocasiones aparecen problemas de interoperabilidad. Para reducir en cierto grado estas situaciones el Monitoreo Remoto *(RMON)* del *MIB* fue desarrollado como un estándar para *LANs*-Remotas. Así el protocolo provee la infraestructura que habilita los productos de diferentes vendedores para comunicarse con un administrador en común, permitiendo a una simple consola el soporte de una mezcla de equipos en red.

10.1.2. Monitoreo remoto

El Monitoreo Remoto *(RMON)* representa la evolución lógica en el uso del Protocolo Simple de Administración de Red *(SNMP)*. *RMON* provee la información que se requiere para la administración de los segmentos de red localizados en un edificio inteligente o en otra parte del mundo.

10.1.2.1. Operación.

El *RMON* basa su operación sobre el *software* o *firmware*, menos en el administrador de componentes o en las pruebas *Standalone* del *hardware*. Administrando los componentes de red que pueden incluir productos programables de *hardware* como *bridges*, *ruteadores*, *gateways*, *hubs*, *workstations*, *minicomputadoras*, y *mainframes* que están conectados a la red.

Por medio del *software* apropiado, cada componente administrado responde a la Estación de Administración de Red *(NMS)* solicitando la vía de transporte del protocolo *SNMP*. A través de una prueba *Standalone* se puede considerar una representación de la administración de los componentes, lo cual difiere singularmente de lo mencionado anteriormente acerca de los componentes basados en *firmware* y están restringidos por el funcionamiento de un montón de variables predefinidas por las operaciones del *RMON*.

El Tabla 10-3 ilustra la relación existente entre una estación de administración de red *(NMS)* y una serie de componentes para administración o sondeo consistentes en agentes *RMON*.

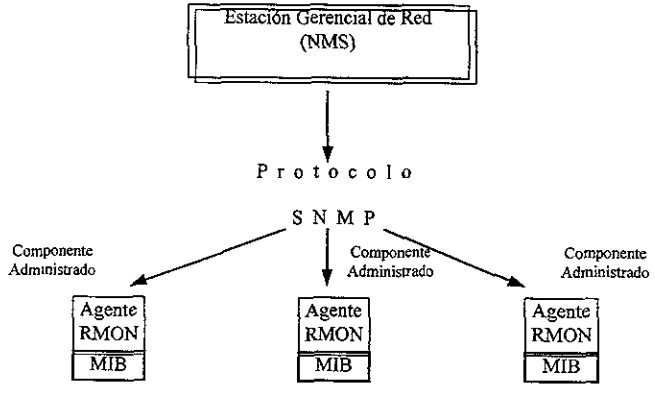


Tabla 10-3 Operación RMON.

El Administrador de Información Básica *(MIB)* provee la representación standard de los datos colectados, tal como definir grupos de objetos que puedan ser administrados. En el *NMS*, uno o más programas controlan las aplicaciones de interacción entre los componentes de la red, mientras se presenta su información y se generan los reportes de estado. Otras funciones perfeccionadas por aplicaciones *NMS* pueden incluir protección por password para abrir una sesión y tomar el control propio de la estación, dando soporte para múltiples operadores en diferentes lugares, adelantando la información de un evento critico vía E-mail o anunciándolo para facilitar las operaciones, y asimilando las funciones.

10.1.3. RMON MIB.

El sondeo o el monitoreo remoto de red es representado por *hardware* y *software* diseñado para proveer a los agentes y administradores la información de los diferentes segmentos de red a la que están conectados. El Monitoreo Remoto *MIB* esta definido en el RFC 1271, el cual consiste de un arreglo de objetos dentro de nueve grupos.

Grupo	*Descripción*
Statistics	Contiene la estimación de las estadísticas de sondeo de RMON para cada interfaz monitoreada.
History	Graba las muestras estadísticas de una red para un intervalo de tiempo seleccionado y las almacena para recuperlas más tarde
Alarm	Recupera las muestras estadísticas en una base periódica de variables almacenada en sus recursos administrables, y compara sus valores para predefinirlos en el umbral de la red. Si el monitoreo de variables excede el umbral, se genera el aviso de alarma.
Host	Contiene las estadísticas asociadas a cada host descubierto en la red.
HostTopN	Es un grupo utilizado para prepara reportes que describen los hosts que tienen demasiado tráfico o lleva el conteo de errores en un intervalo de tiempo.
Matrix	Almacena las estadísticas del tráfico y los errores conjugados entre dos direcciones.
Filter	Permite que los paquetes sean marcados bajo una ecuación de filtrado.
Packet Capture	Permite capturar los paquetes después que fluyen a través de las conexiones.
Event	Controla la generación y notificación de sucesos en los recursos administrados.

Tabla 10-4 Grupos MIB del monitoreo remoto de red.

La Tabla 10-4 lista cada uno de los grupos del *MIB* y da una breve descripción de sus funciones. Todos los grupos listados en ésta son opcionales y pueden ser o no soportados por el sistema de administración.

Ambos grupos, el de *statics* e *history* pueden dar información de valor concerniente al estado de los segmentos de la red *Ethernet* al ser monitoreada. El grupo de *statistics* contiene 17 entradas para lo cual se mantiene un contador., Mientras que el grupo de *history* contiene 11 entradas de la misma característica. Adicionalmente, el grupo de *history* incluye el cuidado en tiempo-real de un integrador que demuestra el nivel físico de red utilizado centésimas de veces.

La Tabla 10-5 a continuación presenta la comparación de los sistemas funcionales por los grupos *RMON* de *statics* e *history*. A través de ambos grupos se obtiene esencialmente la misma información, aunque para ambos tenga un significado diferente.

La primer diferencia más sería son los datos de las estadísticas por el grupo statics dada la libertad del contador, que comienza de cero cuando el valor de entrada es recibido, y da la información concerniente al estado de segmento en operación. En comparación, las estadísticas en el grupo *history* dan la información más general analizando los segmentos largos. Reconociendo las diferencias, el grupo de *statics* manda paquetes de diferentes tamaños, mientras que el grupo *history* ignora el largo de los paquetes y las pistas de red utilizadas.

	Statistics	*History*
Buzón de Resultados	Sí	Si
Octetos	Si-	No
Paquetes	Si	Si
Transmisión de Paquetes	Si	Si
Multitransmisión de Paquetes	Si	Si
Alineación de errores CRC	Si	Si
Mínimo de Paquetes	Si	Si
Máximo de Paquetes	Si	Si
Fragmentos	Si	Si
Parloteo	Si	Si
Colisiones	Si	Si
Paquetes 64-octectos de largo	Si	No
Paquetes 65-127 octetos de largo	Si	No
Paquetes 128-255 octetos de largo	Si	No
Paquetes 256-511 octetos de largo	Si	No
Paquetes 512-1025 octetos de largo	Si	No
Paquetes 1024-1518 octetos de largo	Si	No
Utilización	No	Si

Tabla 10-5 Comparación de sistemas de medida del grupo *Statistics* e *History*.

El componente gerencial del sistema o el sondeo son esencialmente ineficaces si un segmento de red llegase a incomunicarse debido a la falla del *ruteador* o del *bridge* o un problema de cableado, muchos vendedores proporcionan el *RMON* para sondear redes *Ethernet* con capacidad de acceso redundante. Esta característica es normalmente proporcionada a través del uso del soporte integrados por *módem* o *ISND.* Otra característica en común es la de pruebas *Standalone* con soporte de capacidad en multisegmentos. Esta se habilita en sondas simples para ser usadas por el soporte de redes mayores de cuatro segmentos, asumiendo que la distancia entre el cableado lo permite.

10.2. Administración de costos

Las organizaciones están divididas en áreas funcionales y es importante para muchas tener identificado los costos reales por departamento o división.

La administración de costos permite prorratear los costos totales de la función informática de la organización por centro de costos, obteniendo así información real del uso de los recursos de red de cada uno de los usuarios, departamentos o divisiones.

10.2.1. Administración de la configuración

Esta consiste en obtener datos en línea de la red para mantener el control de todos sus dispositivos.

Para llevar al cabo la administración de la configuración es necesario contar con herramientas capaces de detectar y obtener información sobre los dispositivos de la red y guardarlos en una base de datos para su uso posterior.

En una red compleja los constantes cambios y modificaciones hacen que se pierda fácilmente el control de la configuración de la red y sus dispositivos. Normalmente el inventario que se tiene por escrito difiere de lo que realmente está instalado en la red.

La administración de la configuración puede llevarse a niveles tan avanzados que permiten accesar y controlar tanto las versiones de *software* y licencias a lo largo de la red, como la distribución automática de *software* o actualizaciones.

10.3. Administración de la seguridad

La administración de la seguridad consiste en proteger la información sensible que se encuentra en los dispositivos de la red al controlar los puntos de acceso a esa información.

La administración de la seguridad involucra 3 pasos

1) Identificar la información que debe ser protegida de acuerdo a las políticas y mecanismos de confidencialidad de la organización. Debe determinarse cuál información es pública y cual debe tener restricciones de acceso.
2) Encontrar y asegurar los puntos de acceso. No solamente las computadoras que están conectadas a la red, sino los servidores y comunicaciones remotas, deben tener mecanismos de seguridad establecidos. Existe seguridad en el ámbito de sistema operativo y seguridad en el ámbito físico.
3) Mantener el sistema de seguridad. El sistema de seguridad debe ser a la vez dinámico y estricto; así como también debe poder detectarse los intentos de violación a la seguridad.

10.3.1. Administración del rendimiento

Consiste en garantizar que la red se mantendrá siempre accesible con tiempos de respuesta aceptable de manera que los usuarios puedan la en forma eficiente.

Permite también planear el crecimiento de la red y su impacto en el rendimiento futuro. Esto se lleva al cabo mediante el monitoreo constante y la corrección de los problemas de rendimiento que presente la red.

Para llevar al cabo el monitoreo del rendimiento se deben seguir cuatro pasos:

I. Obtener datos de la utilización de dispositivos de la red o sus enlaces.
II. Analizar datos relevantes para detectar puntos de alta utilización.
III. Establecer umbrales de utilización tolerados.
IV. Hacer un modelo manual o automático para proponer modificaciones que aumenten el rendimiento.

Este mismo esquema puede ser utilizado no solamente para detectar los puntos en donde el rendimiento actual es *bajo;* si no que permite planear el crecimiento futuro de la red sobre la base de las tendencias en la utilización.

10.4. Administración de fallas

Es el proceso mediante el cual se localizan problemas o fallas en la red de datos. Se compone de tres elementos:

~ Detectar el problema, en algunos casos antes de que se presente.

~ Aislar el problema.

~ Corregir el problema, si es posible.

Con el uso de herramientas de administración de redes se pueden localizar y corregir problemas de manera más rápida.

Para detectar el problema deben estar definidos los elementos de los que se va a obtener información de la red y establecer niveles y prioridades para cada uno de ellos

No hacer esto puede provocar:

- Recibir una avalancha de mensajes de fallas no importantes.
- Recibir las alarmas verdaderamente críticas con una prioridad mal definida.

Una vez detectado el problema, debe ser aislado. Este proceso puede en ocasiones ser muy complejo. Aquí es donde el poder de las herramientas de administración debe ser cuidadosamente seleccionado.

La herramienta debe ser capaz de detectar la existencia de un problema y dar los mecanismos necesarios para aislar el mismo.

Una vez terminado el problema la herramienta debe preferentemente ser capaz de corregirlo.

Normalmente se utilizan códigos de colores para detectar, aislar y corregir el problema dentro de su interfaz gráfica de objetos.

10.4.1. Mesa de ayuda (Helpdesk)

El servicio, soporte, reporte de problemas, seguimiento de problemas y estadísticas de fallas en una red compleja se vuelven actividades en las que se puede perder fácilmente el control. Un sistema de mesa de ayuda permite automatizar los procesos mencionados, aumentando el nivel de atención que se le da a los usuarios de la red.

11. Firewalls y seguridad en Internet

La seguridad se ha convertido en una de las preocupaciones principales cuando una organización conecta su red privada al Internet. Sin considerar el tipo de negocio, un número creciente de usuarios de redes privadas están demandando el acceso a los servicios de Internet, tales como la World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Además, las empresas (corporaciones) quieren ofrecer las múltiples ventajas de las paginas electrónicas (home pages) y los servidores FTP de acceso publico en Internet.

Los administradores de red tienen preocupaciones en lo que se refiere a la seguridad de los sistemas, primordialmente cuando se exponen datos confidenciales o privados de la organización así como la infraestructura de su red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación de información privada. Todavía, aún si una organización no esta conectada al Internet, pudiera desear el establecimiento de una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

11.1. Firewalls

Un Firewall en Internet se define como un sistema o grupo de sistemas que hace cumplir una política de seguridad entre la red privada de una organización y el Internet. El firewall determina cual de los servicios internos y qué servicios externos pueden ser accesados por los usuarios de la red, es decir quien puede entrar para utilizar los recursos de red y quién no. Para que un firewall sea efectivo, todo el tráfico de información hacia y del Internet deberá pasar a través del firewall donde podrá ser inspeccionado. El firewall sólo debe permitir el paso del tráfico autorizado, y el mismo deberá ser inmune a la penetración. Desdichadamente, este sistema no puede ofrecer ninguna protección una vez que un intruso agresor lo traspasa o permanece entorno a éste.

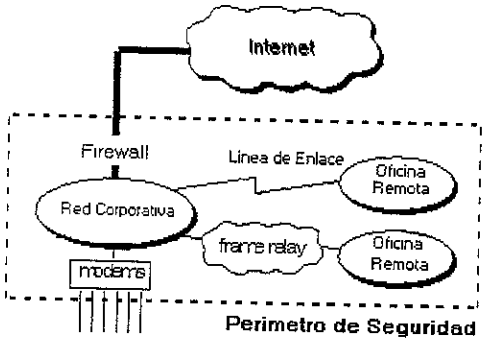


Ilustración 11-1 La Política De Seguridad Crea Un Perímetro De Protección.

Es importante, notar que un firewall de Internet no es solamente un ruteador. El firewall es parte de una política de seguridad integral que crea un perímetro de defensa diseñado para proteger las fuentes de información de la organización. Esta política de seguridad debe incluir publicaciones con las guías de ayuda donde se informe a los usuarios sobre sus responsabilidades, políticas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento de personal. Todos los puntos potenciales susceptibles de ataque en la red deben ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como colocar una puerta de acero en una tienda.

11.1.1.1.Beneficios de un firewall en Internet

Los firewalls en Internet administran el acceso entre el Internet y la red privada de una organización. Sin un firewall, cada uno de los servidores de la red privada está expuesto al ataque de otros servidores en el Internet. Esto significa que la seguridad de la red privada dependería de la "**dureza**" de los mecanismos de seguridad con la que cuenta sus servidores y es tan seguro como la seguridad del sistema más débil.

Los firewalls de Internet permiten que el administrador de la red defina un filtro centralizado con el fin de mantener a usuarios no autorizados (tales, como hackers, crackers, vándalos, y espías) fuera de la red protegida ; impidiendo el ingreso o salida de la red a los servicios potencialmente vulnerables, además de brindar protección con respecto a diversos tipos de ataque de ruteo. Uno de los beneficios clave de un firewall en Internet es que simplifica la administración de la seguridad desde que la protección de la red se consolida en los sistemas firewalls en vez de ser distribuida a cada host en toda la red privada.

Esto debiera ser notado por las organizaciones que tienen conexiones con el Internet, aunque la pregunta que surge es cuando ¿Cuándo ocurrirá el ataque?. Es extremadamente importante que los administradores de la red vigilen y registren todo el tráfico por insignificante que sea de la red a través del firewall. También, si el administrador de la red no toma el tiempo para responder cada señal de alarma y examinar regularmente los registros, el firewall no será necesario ya que el administrador de la red nunca sabrá si el firewall ha sido atacado.

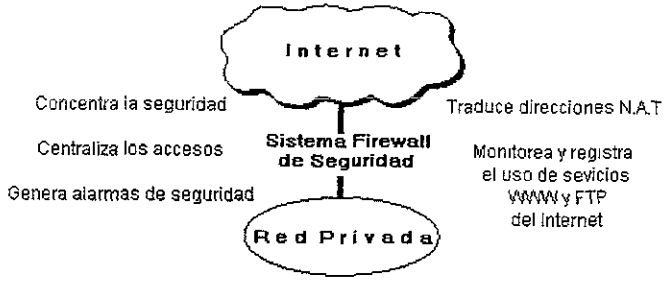


Ilustración 11-2 Beneficios De Un Firewall De Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, misma que ha originado que las direcciones registradas IP, sean un recurso o fuente menos plena. Esto ha suscitado que la compañía que desean conectarse al Internet no les sea posible conseguir un rango de direcciones suficiente; para responder a las demandas de los usuarios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT)[71] esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para renumerar cuando la organización cambie su Proveedor de Servicios de Internet (ISPs)[72] .

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto central de contacto para la organización. Si una de sus metas es proporcionar servicios de información a clientes, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, algunos argumentarán que el despliegue de un firewall de Internet falla, la red privada de la empresa continuará funcionando ya que únicamente el acceso a Internet se ha perdido.

[71] Network Address Translator, de sus siglas en inglés.
[72] Internet Service Providers, ídem

La preocupación que se tiene con respecto a la aportación de múltiples puntos de acceso al Internet, radica en que el administrador de red tiene que filtrar y monitorear cada punto de acceso ¡Dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente¡

11.1.2. Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que no se efectúen o pasen a través de éste.

Por ejemplo, si existe una conexión "**dial-out**" sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una prueba adicional de legitimación por un Firewall Proxy server (FPS)[73] lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones deriva la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar conscientes de que este tipo de conexiones no son permitidas como parte integral de la arquitectura de la seguridad en la organización.

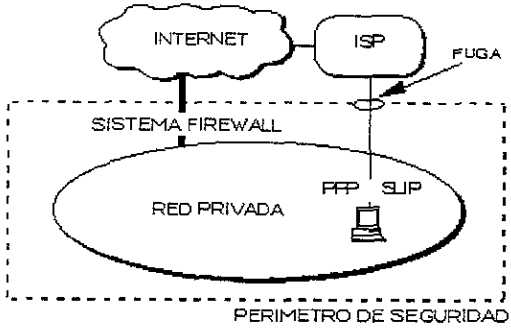


Ilustración 11-3 Conexión Circunvecina Al Firewall De Internet.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y los substraigan del edificio.

[73] Servidor Apoderado del Firewall, de su traducción al español.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo de un Hacker que pretende ser un supervisor o un nuevo empleado despistado, que persuade al usuario menos sofisticado a que revele la contraseña que le permita que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque de la ingeniería social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN[74] para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

La organización debe estar consciente de la necesidad de instalar software anti-virus en cada despacho para protegerse de su llegada por medio de disquetes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, éstos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modifique los archivos relacionados a la seguridad facilitando el acceso a un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce el riesgo de sufrir ataques mediante la transferencia de datos.

11.2. Herramientas del hacker

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de experiencia técnica y además son motivados por diversos factores. Algunos hackers son alentados por el desafío, otros más gozan complicando la vida a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

[74] System Control Antivirus Network, de sus siglas en inglés.

11.2.1. Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar esta información:

- El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.
- El programa TraceRoute puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Los servidores DNS pueden accesarce para obtener una lista de las direcciones IP y sus correspondientes nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y ultima sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

11.2.2. Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.

Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a puertos específicos del tipo de servicio que esta asignado al servidor en cuestión. La corrida del programa presenta

una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.

- Están disponibles varias herramientas del dominio publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS)[75] o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN)[76] , el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información colectada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema de la organización puesta en la mira.

Un administrador de redes inteligente puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determinar que servidores necesitan ser arreglados y actualizados en software.

[75] Internet Security Scanner, de sus siglas en inglés.
[76] Security Analysis Tool for Auditing Networks, ídem

11.2.3. Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar accesar a los servicios específicos de un sistema.

Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones

- Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas del sistema en cuestión teniendo acceso si el ataque original es descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como "**caballos de Troya**" protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras máquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar archivos privados, robarlos y destruir o corromper datos importantes.

11.3. Decisiones básicas para el diseño de un firewall.

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que deben ser direccionadas por el administrador de red:

* La postura sobre la política del Firewall.
* La política integral de seguridad de la organización.
* El costo financiero del "**firewall**".
* Los componentes o la construcción de secciones del Firewall.

11.3.1. Políticas del firewall.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- "No todo lo específicamente permitido está prohibido"
- "Ni todo lo específicamente prohibido está permitido"

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es más importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea un ambiente más flexible al disponer más servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "**facilitar el uso**" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

11.3.2. Política interna de la seguridad

Como se discutió anteriormente, un firewall de Internet no esta sólo - es parte de la política de seguridad total en una organización -, la cual define todos los aspectos en competentes al perímetro de defensa. Para que ésta sea exitosa, la organización debe de saber qué sé ésta protegiendo. La política de seguridad debe basarse en un análisis de la seguridad cuidadosamente conducido. Si no se posee con la información detallada de la política a seguir, aún que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

11.3.3. Costo del firewall

¿Cuánto puede ofrecer una organización por su seguridad?, Un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya está incluido como parte del equipo. Un sistema comercial de firewall provee un incremento más a la seguridad pero su costo puede ser de $32,000 hasta $240,000 pesos dependiendo de la complejidad y el número de sistemas protegidos. Si la organización posee al experto en casa, un firewall casero puede ser construido con software de dominio público pero este ahorro de recursos repercuten en términos del tiempo de desarrollo y el despliegue del sistema firewall. Finalmente requiere de soporte continúo para la administración, mantenimiento general, actualización del software, reparación de dispositivos de seguridad, e incidentes de manejo.

11.3.4. Componentes del sistema firewall

Después tomar decisiones sobre los beneficios previos, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito

Por lo que resta del capítulo, se discutirá cada una de las opciones para la edificación de barreras y se describirá como se puede trabajar junto con ellos para construir un efectivo sistema firewall de Internet.

11.4. Edificando barreras: ruteador filtra-paquetes

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si éste corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP,ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, éste será desplazado de acuerdo a la información en la tabla de ruteo; si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si éstos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

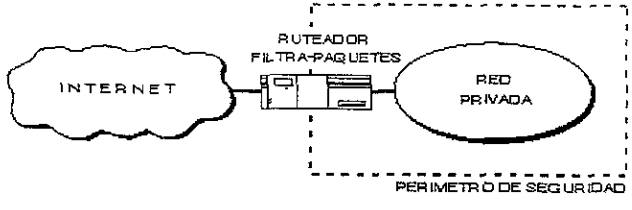


Ilustración 11-4 Ruteador Filtra-Paquetes.

11.4.1. Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el tráfico esta basado en un servicio en específico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado número de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 *y* que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista específica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos específicos.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el tráfico UDP.

11.4.2. Servicio independiente del filtrado

Este tipo de ataques ciertamente es difícil de identificar usando la información básica de los encabezados debido a que estos son independientes al tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques pero son más difíciles de especificar desde entonces las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

Agresiones Originadas Por El Direccionamiento IP.

Para este tipo de ataque, el intruso transmite paquetes desde afuera pretendiendo pasar como servidor interno

- los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema -. El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "**interno**" si el paquete llega en una de las interfaces del ruteador "**externo**".

Agresiones Originadas En El Ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través del Internet. Este tipo de ataques se diseñan para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

Agresiones Por Fragmentación.

Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separar en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores, una agresión pequeñísima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

11.4.3. Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall se despliegan usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no, el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el tráfico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software específico que tenga que ser instalado en cada uno de los servidores.

11.4.4. Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo más difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentemente inocuos se desplazan por el ruteador a un servidor interno. Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el número de filtros utilizados se incrementa. Los ruteadores son optimados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interface apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aún aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el tráfico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio. Por ejemplo, un administrador de red necesita filtrar el tráfico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

11.5. Edificando barreras: gateways a nivel-aplicación

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de proposito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aún cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa nuestros costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el firewall.

11.5.1. Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Un Gateway a nivel-aplicación por lo regular es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer mas seguro un servidor de defensa:

⇒ La plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutara una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del firewall.

⇒ Unicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y legitimación de usuarios son instalados en este servidor.

⇒ El servidor de defensa podrá requerir de una legitimación adicional para que el usuario accese a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología "una-sola vez" de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos). Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

⇒ Cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

⇒ Cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

⇒ Cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El

registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.

⇒ Cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail[77] - puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.

⇒ Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se suscitará un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aún, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa.

⇒ Un Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial. Desde que la aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.

⇒ Cada Proxy corre como un usuario no-previlegiado en un directorio privado y seguro del servidor de defensa.

[77] Correo Electrónico por UNIX.

11.5.1.1.Ejemplo: telnet proxy

La Ilustración 11-5 presenta la operación de un Telnet Proxy en un servidor de defensa. Para éste ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el Gateway a nivel-aplicación.

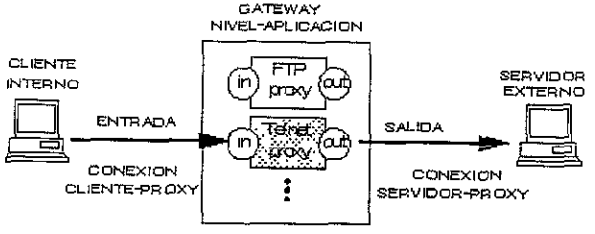


Ilustración 11-5 Telnet Proxy.

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un telnet al servidor de defensa donde es autorizado por la tecnología "una-sola vez" de contraseña. Después de ser autentificado, el cliente obtiene acceso a la interface de usuario del Telnet Proxy. Éste únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

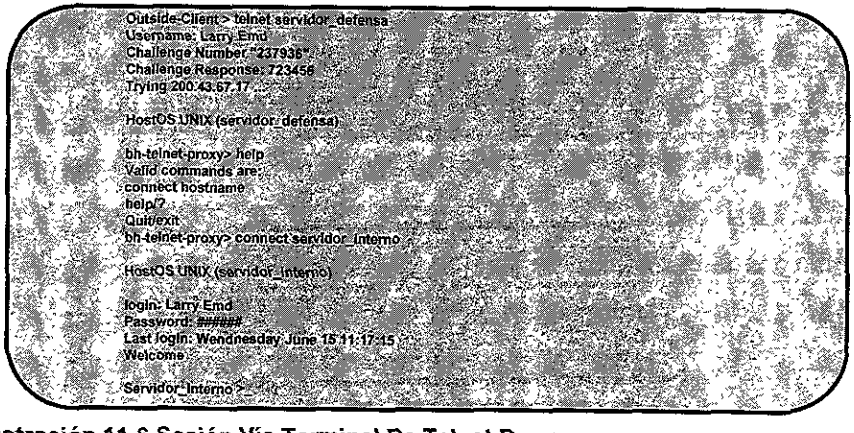


Ilustración 11-6 Sesión Vía Terminal De Telnet Proxy.

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet proxy es un cliente externo.

La presenta la salida en pantalla de la terminal de un cliente externo como la "conexión" al servidor interno una vez establecida. Nótese que el cliente no se está registrando al servidor de defensa - el usuario comienza su sesión autentificándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido seccionar se comunica con el Telnet Proxy -. Después de pasar el intercambio de respuestas, el servidor Proxy limita un conjunto de comandos y destinos que están disponibles para los clientes externos.

La legitimación puede basarse en "algo conocido por los usuarios" (como una contraseña) o "algo que tengan" que posean físicamente (como una tarjeta electrónica) cualquiera de las dos. Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la legitimación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación por un número. Típicamente, se le entrega al usuario su tarjeta desactivada para que él introduzca un PIN[78] y se le regresa la tarjeta, basada en parte como llave "secreta" de encriptacion y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

11.5.2. Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios. Aún cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio está completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de éste tipo son mucho más fáciles de configurar y probar que en un ruteador filtra-paquetes.

11.5.3. Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-

[78] Post Identidy Number, de sus siglas en inglés

aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de telnet.

11.6. Edificando barreras: gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

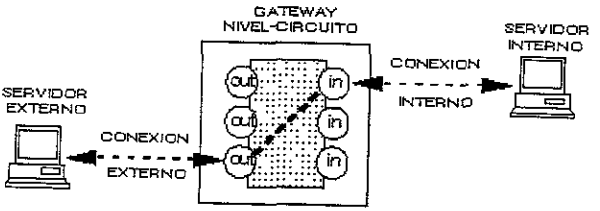


Ilustración 11-7 Gateway Nivel-Circuito.

La Ilustración 11-7 muestra la operación de una conexión típica Telnet a través de un Gateway a nivel-circuito. Tal como se menciono anteriormente, éste gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como un cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

CONCLUSIONES

Como se ha podio ver este documento se basa en los requerimientos funcionales para la familia de redes de computadoras en área local y metropolitana IEEE802, definiendo los requerimientos funcionales, ambiente, y recomendaciones de operación. Así como la definición de los requerimientos para protocolos e interfaces

Esto se debe principalmente a la gran evolución de las redes *Ethernet* y el desarrollo de las tecnologías emergentes en el ámbito de *Internetworking*.

Las redes locales (LAN) como hemos podido ver son sistemas de comunicación que permiten a un número independiente de computadoras comunicarse con otro tipo de redes de datos en una área geográfica reducida como un edificio o campus. En contraste con las redes de banda ancha (WAN) que se pueden interconectar fácilmente a diferentes países del mundo operando a través de las redes publicas switchadas (x.25, Frame Relay, ATM). Las redes locales se distinguen por el modo de uso de paquetes de comunicación y la utilización de la capa de enlace de datos como su interface común. Los canales de comunicación físicos de una LAN poseen un rango alto de datos y un consistente rango mínimo de errores.

Hoy en día el uso singular de este tipo de redes permite trabajar servicios de voz y datos lo cual las define como IVD LAN (redes local integrada de voz y datos) permitiendo la integración de un número independiente de divisas para comunicarse en una MAN o hacia un *Backbone WAN.* Soportando servicios de datos, fax, y otro tipo de información digital codificada. Una IVD LAN difiere de una tradicional LAN en su capa física de integración por el tipo de información manejada; esto se debe principalmente a que una IVD LAN provee el acceso a la red digital de servicios integrados (ISND), WANs y MANs.

Las redes metropolitanas (MAN), se forman entre las redes publicas de switcheo, y se distingue de las demás redes debido a que su configuración geográficamente abarca las ciudades. Contrastando con las redes LAN y WAN.

El éxito de las LANs (Incluyendo las IVD LANs) y MANs se debe a que facilitan la compatibilidad e interoperatibilidad entre los equipos de comunicación construidos por diferentes compañías. Ya que son armados bajo las especificaciones de estándares establecidos para el manejo común de protocolos e interfaces para redes.

La creación y manejo de estos estándares establece que se provea una arquitectura que permita una interconexión efectiva y costos moderados de los componentes de red, y así mismo un costo moderado de su instalación.

La comunicación de datos en modo de paquetes dentro de las LANs (incluyendo IV LANs) y MANs se describe y diseña en términos de conformidad con los servicios definidos por el Standard ISO titulado "Sistemas abiertos de Interconexión — Modelo Básico de Referencia —" (ISO 7498). Donde se concibe la comunicación de datos en modo de paquetes, bajo las capas de enlace físico y de datos.

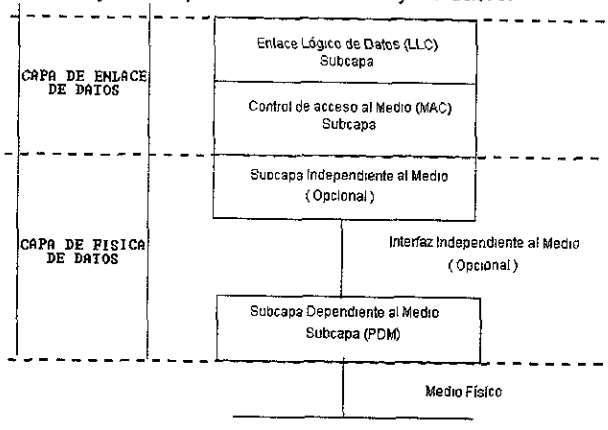


Figura 1 Modelo de Redes de Área Local y Metropolitana.

Las capas de comunicación que se deseen crear para el comité IEEE802 de la familia *Ethernet* se definirán como tal, relativamente de acuerdo a los componentes e independiente a las aplicaciones. Este modelo permite individualizar las capas de servicio y protocolo para ser reemplazados si es necesario sin requerir cambios en las bases de protocolos y las capas de servicios dentro de una arquitectura de red.

No, obstante de esto; cualquier tipo de red de computadoras que se desee instalar (LAN, IVD LAN o MAN) debe de seguir los requerimientos funcionales para la capa física que determina el proyecto IEEE 802:

1. Componentes De Interfaces Para Datos

Los cuales deben ser simples y económicos.

2. Transparencia De Datos

Esta función se realiza en las rutas a través de las redes siendo insensibles únicamente a la combinación del carácter de intercambio o al bit de paridad utilizado por la capa alta del protocolo de transmisión.

3. Intercambio De Datos

La arquitectura de una red de computadoras no podrá excluir el intercambio directo de datos entre cada uno de los componentes que integren a la red. Esta será capaz de transmitir unidades de datos entre cada uno de los componentes de una misma LAN sin requerir de un sistema intermedio a la capa de ruteo de la red.

4. Conexión De Componentes

Todas las redes LANs, IVD LANs, y MANs; soportaran hasta un máximo de doscientos (200) componentes interconectados

5. Rango De Transmisión

El rango de transmisión máxima en todas las redes podrá ser de un millón de bits por segundo.

6. Distancia

Las LANs (incluyendo IVD LANs) podrán soportar hasta un máximo de 100 metros en segmentos de red. Las LANs se integran por diversos componentes interconectados por segmentos de cable a través de la capa física del internetworking operando sobre el medio físico hasta 2 KM de largo.

Las MANs pueden operar distancias hasta de 50 Km.

7. Adición Y Remoción De Componentes

Las redes deben de ser diseñadas para que las interfaces de usuario y las unidades de acceso al medio sean fáciles de añadir o remover. La conexión o desconexión de los componentes en las redes LANs (incluyendo IVD LANs) o MANs no deben de trascender de más de un segundo.

8. Ambiente Compartido De Redes

Cuando varios nodos de una LAN (incluyendo IVD LAN) o MAN tienen la necesidad de compartir recursos tales como medios de banda ancha, medios de acceso, y puertos de multiplexado, podrán proveer un mecanismo que administre y arbitre el uso de estas redes compartidas de tal manera que sea " equitativa" en todos sus nodos.

(Equitativa significa que todos los componentes con un mensaje igual de prioridad podrán tener la misma probabilidad de acceso a la red).

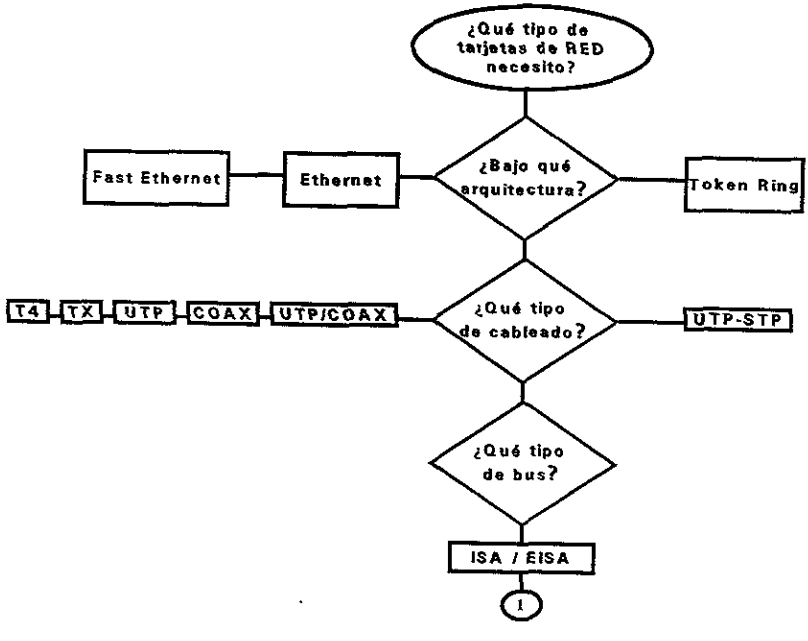
9. Protección Galvánica Y Contra Descargas Eléctricas

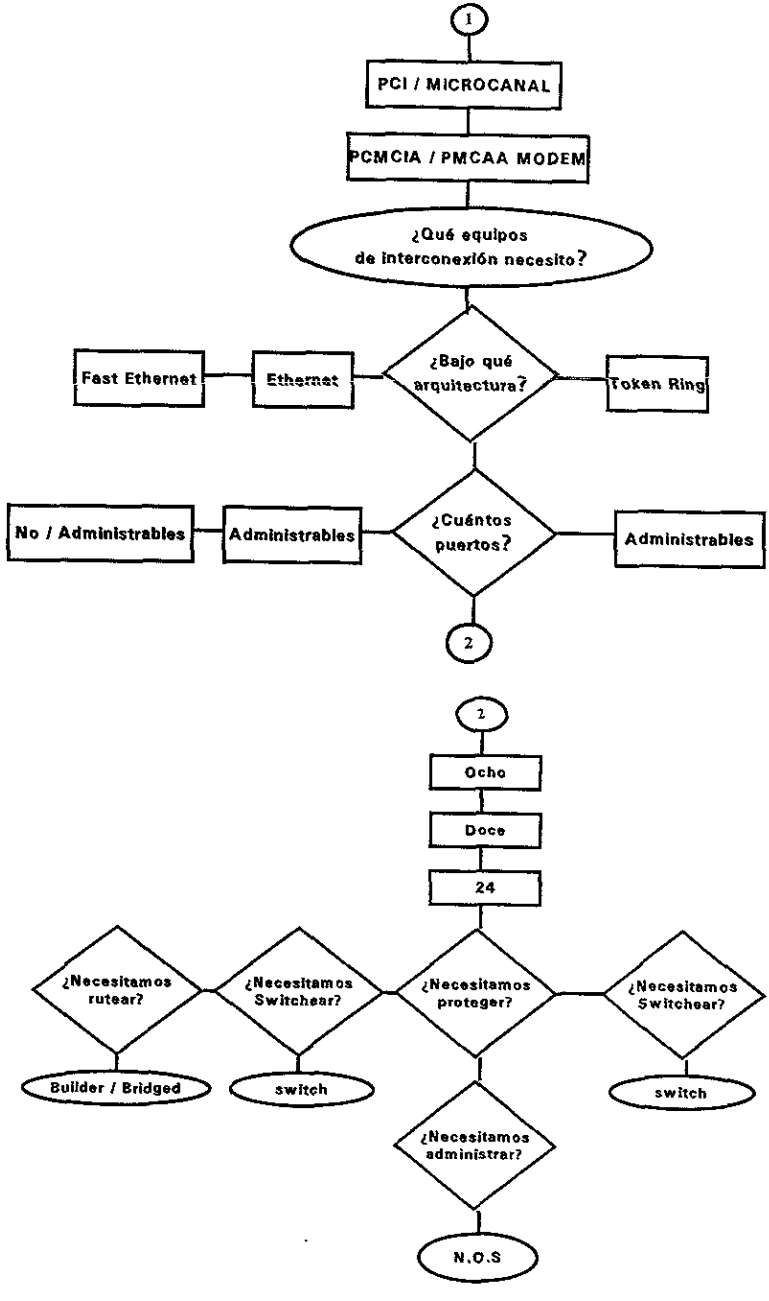
Todas las instalaciones de redes de cómputo deberán de proveer protección contra descargas eléctricas de cualquier índole, en todas las interfaces de datos y de usuario.

Esta claro que no basta observar los anteriores requerimientos, ya que estos son más fáciles de mantener en el ámbito de usuarios; también existen los requerimientos funcionales derivados de los criterios de desarrollo de estándares para redes y un sin fin de caracteres presentados por la sociedad de IEEE a los principales desarrolladores de estándares y software para redes. Existen además los estándares de interconexión creados por el ANSI y CITT.

Por más pequeña que sea la red local a interconectar esta debe de seguir un algoritmo de diseño que nos permita sacar el mejor provecho del trabajo en grupo a través de las interfaces de usuario conectadas en red; no solo debemos basarnos en el costo de nuestra arquitectura, ni en el éxito rotundo de la tecnología de redes en boga, ni tampoco en lo exitoso del software para monitoreo y administración de red, así como el costo de operación en la seguridad de datos.

Algoritmo de conectividad en redes de cómputo




1
PCI / MICROCANAL
PCMCIA / PMCAA MODEM
¿Qué equipos de interconexión necesito?
¿Bajo qué arquitectura?
Fast Ethernet
Ethernet
Token Ring
¿Cuántos puertos?
No / Administrables
Administrables
Administrables
2
2
Ocho
Doce
24
¿Necesitamos rutear?
¿Necesitamos Switchear?
¿Necesitamos proteger?
¿Necesitamos Switchear?
Builder / Bridged
switch
switch
¿Necesitamos administrar?
N.O.S

En primer punto debemos de observar cual es la necesidad de intercomunicación dentro de mi ambiente de trabajo basado en el equipo de cómputo, siendo de primera instancia la instalación de una red local con una arquitectura, topología y protocolo definidos. Con sus ventajas e inconvenientes respectivamente.

Como segundo término se debe de seleccionar el medio físico para interconectar mis computadoras en una área local definida: Coax, UTP, etc., adicionalmente necesito determinar que adaptador de red es factible de instalarse en mis equipos de cómputo por su arquitectura de componente: ISA (8 Bits), EISA (16 Bits), PCI (32 Bits), etc.,

Una vez seleccionado lo anterior debemos de escoger el equipo de interconexión para la arquitectura manejada por mis adaptadores de red: Ethernet, Fast Ethernet, etc., conteniendo el número de puertos necesarios para conectar el equipo de cómputo.

Como último término se debe definir si se desea interconectar con redes internas o redes externas públicas o privadas.

La interconexión de redes internas se ejecuta con equipos de switcheo para compartir recursos entre diferentes redes, estas a su vez homologadas por sus protocolos en la capa de transferencia de datos y la interconexión externa que abarca las unidades de ruteo tales como los bridges, builders, y switches donde la transferencia se lleva a cabo de protocolos orientados a la conexión permitiendo compartir recursos de diversos sistemas y aplicaciones dentro de una área geográfica conjuntando distintos grupos de trabajo en red (LANs hasta 2 Km., y MANs hasta 50 Km.).

No solo basta interconectar, como ya se ha visto anteriormente, debemos de seleccionar con extremo cuidado el tipo de sistemas de seguridad que se han de incluir para la protección del trafico de datos a través de la red (Firewalls)

Esto se logra homologando protocolos por medio de un sistema operativo (N.O.S.) y adicionando programas en el ámbito de aplicación para administrar y monitorear el desempeño del equipo de computo interconectado a la red.

Esto es solo el comienzo ya que hoy en día para ser parte de una red global de intercomunicación de computadoras debemos basarnos en las reglas que definen las organizaciones mundiales que son responsables del proyecto de informática más grande y ambicioso de este mundo el "**Internet**".

En primer plano debemos de respetar la normatividad de comunicaciones digitales en nuestra región debido a que las compañías telefónicas son las responsables de los servicios de enlace que permiten el ingreso a las redes conmutadas "**frame relay**" y posteriormente a las redes principales de conexión fronteriza con Backbone del Internet en los Estados Unidos de Norteamérica.

La importancia de las líneas telefónicas se destaca debido al uso del "**post**", el cual ha permitido que a través de las líneas telefónicas basadas en conexión de cable UTP cualquier persona en el mundo se pueda conectar desde su computadora mediante un "**módem**" a las redes públicas de datos para trabajar desde su casa, oficina u otro lugar de trabajo a otra computadora en cualquier parte del mundo.

Aquí la conectividad local difiere un poco debido a que el adaptador de red utilizado es una tarjeta FAX/MODEM conectada en mi equipo de cómputo con un rango de transmisión estándar de 28,800Kbps a 56Kbps, un protocolo dirigido a la conexión (PPP) o uno dirigido al enlace de datos (SLIP), además de poseer una línea telefónica digital definida por los servicios telefónicos locales.

Análogamente; si yo deseara tener una red local con servicios de Internet mediante el uso de una línea telefónica, tendría que formar una pequeña central telefónica (claro, mediante el uso de un conmutador) para que pudiese interconectar mis computadoras a un puerto de comunicaciones primeramente interno (tarjetas módem o de red), que posea una arquitectura que me permita la intercomunicación entre ellas (Ethernet, Fast Ethernet, 100Vg- Anylan, Iso-ENET,Token-Ring, etc.), un tipo de cableado e interconexiones que me comuniquen entre si a las computadoras (10BaseT, 2OBaseT, FDDI, etc.), y secundariamente elementos externos (RAS, HUB/LAN-WAN, Switch/FAST-MAN, etc.), enlaces digitales, (ISND, Troncales o DS0, etc.), unidades de comunicación remota (Microondas, TDM, Satelital, etc.). Y finalmente el software que permita la administración y comunicación de los componentes de red así como unidades de seguridad para respaldo de datos privados y públicos (Firewalls en el ámbito de aplicación y datos).

Concretamente las tecnologías aquí expuestas son parte del desarrollo que exigen los medios de comunicación a los sistemas de cómputo actuales, hoy son las computadoras pero el hecho de interconectar a todo el mundo al Internet creará nuevas tecnologías emergentes basadas en todos los medios de transmisión posibles.

El A.T.M. a 6 años de desarrollo sigue siendo el caballo de batalla para obtener comunicaciones de voz, vídeo y datos lo más rápido posible incrementando el ancho de banda utilizado por los principales medios de transmisión. No obstante, a que a últimas fechas se ha declarado al Internet Ipv4 como agotado, el desarrollo de software ha permitido que se creen nodos virtuales y así el ingenio del ser humano es capaz de sacar el mayor provecho a las tecnologías que parecen ser marcadas como obsoletas.

El caso de México es muy importante para los países de Hispanoamérica ya que el desarrollo de las tecnologías de 1er. Mundo en Internet está a la vuelta de la esquina, la electrónica en comunicaciones actual ya no es de desarrollo como en los años 70´s, ahora se torna consumista pero de ahí que el gran reto del ingeniero sea el tener los conocimientos necesarios para crear y desarrollar un proyecto de conectividad que brinde a la sociedad las ventajas de la tecnología reflejadas en su economía y bienestar social.

BIBLIOGRAFÍA

Referencias Estándares y Modelo OSI

Libros de Texto

"Ethernet Networks, Design, Implementation" por Gilbert Held. , John, Wiley & Son, 1996, ISBN: 0-471-12706-X.

Estándares y Modelo OSI pagina 47~58 cap. 2 Networking standards

Administración de Redes pagina 380~392 cap. 10 Managing The network

"Redes globales de información con Internet y TCP/IP; Principios básicos, protocolos y arquitectura" por Duglas E. Commer, 3ra. Ed. Prentice Hall Hispanoamericana, ISBN 968-8880-541-6, 1995.

Modelo ISO Pagina 12-15 cap. 1Introducción y panorama general

Redes Locales (LAN) Pagina 17-36 cap. 2 Reseña de tecnologías subyacentes de red

Protocolos TCP/IP Pagina 91-229 Cap. 7~13:

Protocolo Internet: entrega de datagramas sin conexión pag91~108

Protocolo Internet: ruteo de datagramas IP pag111~121

Protocolo Internet: mensajes de error y control (ICMP) pag125~139

Extensiones de dirección de sub-red y super-red pag. 141~158

Estratificación de protocolos por capas pag 161~178

Protocolo de datagrama de usuario (UDP) pag 181~190

Servicio de transporte de flujo confiable (TCP) pag 193~229

Redes Virtuales pagina 305 cap. 18 TCP/IP en redes ATM

Administración de Redes pagina pag. 155~471 cap. 26 Aplicaciones: manejo de Internet (SNMP. SNMPv2)

Firewalls y seguridad en Internet pag 479~494 cap. 28 Seguridad de Internet y diseño del muro de seguridad

Indice World Wide Web para paginas relativas a Conectividad

"Cisco - Corporate News & Information"

http://www.cisco.com/public/Corp_root.shtml

"Cisco - Educational Archive and Resources Catalog"

http://sunsite.unc.edu/cisco/

"Cisco - Public Information"

http://www.cisco.com/public/pubsearch.html

"3com - Latinoamérica"

http://www.3com.com/lat/

"3com -Public Information"

http://search.3com.com/index.html

"3com - Document center"

http://www.3com.com/util/dcenter.html

"Alantec - Resources"

http://alantec.and.com/company/company.html

"Hp - Networking"

http://www.hp.com/ahp/Networking/

"Cabletron - Support"

http://www.cabletron.com/support/

"Lantronix - Tutorials"

http://www.lantronix.com/htmfiles/mrktg/catalog/etnetba.htm

"Interphase - Resources"

http://www.iphase.com/Public/

Indice World Wide Web para paginas relativas a Revistas Electrónicas

"Soluciones Avanzadas"

http://www.fciencias.unam.mx/revista/soluciones.html

"LAN Times"

http://www.lantimes.com/

"NET companies"

http://www.tile.com/

Referencias generales TCP/IP, Firewall Y Administración De Redes.

Libros de Texto

"Building Internet Firewalls" por D.Brent Chapman y Elizabeth Zwicky, O'Reilly & Associates, 1995, ISBN: 1-56592-124-0.

"Firewalls and Internet Security: Repelling the Wily Hacker" por Bill Cheswick y Steve Bellovin, Addison-Wesley, 1994, ISBN: 0-201-63357-4.

"Practical UNIX Security" por Simson Garfinkel y Gene Spafford, O'Reilly & Associates, 1991, ISBN: 0-937175-72-2.

Request for Comments

RFC 1244: Site Security Handbook / P. Holbrook and J. Reynolds. - July 1991

RFC 1636: Report of IAB Workshop on Security in the Internet Architecture (February 8-10, 1994) / R. Braden, D. Clark, S. Crocker and C. Huitema. - June 1994

RFC 1704: On Internet Authentication / N. Haller and R. Atkinson. - October 1994.

RFC 1858: Security Considerations for IP Fragment Filtering / G. Ziemba, D. Reed, P.Traina. - October 1995.

Hojas electrónicas de Internet para Seguridad y Firewalls

"A Toolkit and Methods for Internet Firewalls" por Marcus J. Ramus y Frederick M. Avolio de Trusted Information Systems, Inc.

http://web1.cohesive.com/original/ centri/usenix.htm

"Almost Everything You Ever Wanted To Know About Security (but were afraid to ask)" mantenida por Alec Muffett"

http://www.cis.ohio-state.edu/hypertext/faq/usenet/ security-faq/faq.html

"How to Set up a Secure Anonymous FTP Site" por Christopher Klaus de Internet Security Systems, Inc."

http://www.cis.ohio-state.edu/hypertext/faq/usenet/computer-security/ anonymous-ftp-faq/faq.html

Indice World Wide Web para paginas relativas a Seguridad

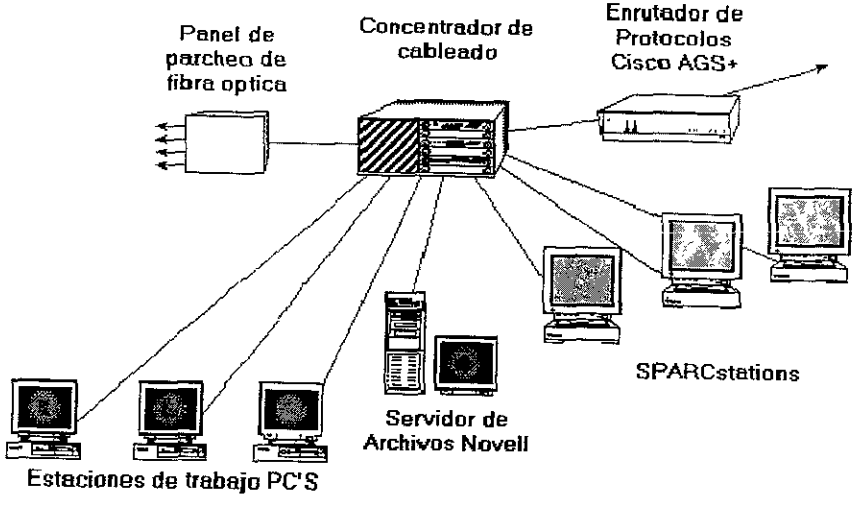
http://lcweb.loc.gov/global/internet/security.html Librería del congreso que contiene links hacia documentos con información pertinente a la seguridad de computadoras.

http://www.telstra.com.au/pub/docs/security/ Pagina de Telstra que contiene links hacia documentos con información pertinente a la seguridad de computadoras.

http://web1.cohesive.com/original/centri/info.htm#Pagina de aplicaciones Cohesive Systems' contiene links a documentos de seguridad en redes.

http://www.netsurf.com/nsf/v01/01/resource/firewall.html Indice General de paginas que contienen documentos acerca de Firewalls

Apéndice A Implementación De Una Red De Computadoras De Area Local A Banda Ancha.



Este apéndice presenta a continuación un prototipo de red local con comunicación a redes de área amplia sin importar el tipo o tamaño del proyecto, y se ejemplifica con la conexión típica de un sistema de Red *Ethernet* a 10MBps con opciones de switcheo, compartiendo servidores Novell y Unix, así como clientes, que pueden ser DOS 6.22 y release, Windows 3.11 WFW, Windows 95, etc., cualquier sistema operativo con o sin interfaz gráfica con conexiones de red; interconectado a varias redes por medio de un ruteador Cisco y cuenta con un DSU de fibra óptica para interconectarse a redes de comunicación publicas o privadas.

Un proyecto de informática debe de observar los siguientes puntos:

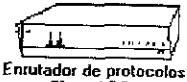
1. Definir las características de la empresa, institución o corporación, objetivos y perfiles.
2. Definir las necesidades y/o oportunidades a corto, mediano y largo plazo.
3. Análisis costo/beneficio del proyecto.
4. Análisis de sistemas candidatos/alternativos.
5. Definición de tecnología a aplicar, desde aplicaciones de sistemas, sistemas de mantenimiento, administración y control.
6. Factibilidad física, y técnica.
7. Factibilidad de los recursos humanos, tomando en cuenta el soporte a los usuarios.
8. Seguridad de los sistemas, integridad de la información, comunicaciones y centro de cómputo.
9. Auditibilidad. La estructura informática debe tener la facilidad para ser auditada.
10. Mantenimiento de los sistemas (hardware y software).
11. Sistemas de recuperación en casos de desastre (DRP).

Tomar demasiados puntos en un proyecto, puede hacer que este se lleve demasiado tiempo en su planeación, sin embargo la puesta en marcha de éste, es mucho más fácil teniendo los puntos anteriores documentados.

Herramientas gráficas como *Pert, Gantt* y *Ruta Critica* nos permiten evaluar y encontrar cuellos de botella en la implantación de estos.

Las indicaciones anteriores no solo se concentra en el desarrollo de un nuevo proyecto, su aplicación puede llevarse a cabo en uno ya existente, cabe mencionar que este mismo se puede aplicar al llegar al punto 11 y comenzar de nuevo, siendo esto el principio de la retroalimentación con el cual siempre los sistemas se mantienen utilizables y no obsoletos.

Enseguida se resumen las funciones que ejecutan cada uno de los componentes de la red de cómputo.


Enrutador de protocolos Cisco AGS+

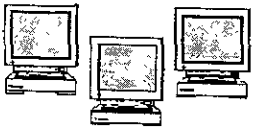
El ruteador de protocolos Cisco AGS+ (router), se encarga del enlace de la Red *WAN* con la Internet. Tiene capacidad para tarjetas de comunicaciones de diferentes tipos, generalmente esta equipado con dos tarjetas, una de las cuales cuenta con dos puertos seriales de alta velocidad (2Mbps), y la otra con dos puertos seriales de baja velocidad y dos puertos *Ethernet* 10BaseT. El cual opera con un procesador Motorola 68020 a 16MIPS @30 MHz con 16MB de RAM, también puede rutear y puentear (brinding/ruteador) concurrentemente la más amplia Implementación de protocolos de comunicación en uso hoy en día, estos incluyen: *OSI, TCP/IP, X.25, DDN X.25, HDLC, Novell IPX*, etc. Una tarjeta de control de ambiente monitorea continuamente las condiciones de temperatura, dando de baja el equipo si existe un peligro por alta temperatura, o voltaje.

Concentrador de Cableado ONline System Concentrator Chipcom de 6 y 17 slots, soportan los protocolos de red *Ethernet*/IEEE 802.3 sobre varios medios, IEEE 802.5 *Token Ring* y ANSI *FDDI*, cuentan con:

- Un módulo controlador que supervisa el tráfico entre los canales (buces) internos del concentrador.
- Un módulo manejador el cual tiene un puerto serial, este módulo inteligente soporta el protocolo de administración de red más usado en la actualidad el SNMP (Simple Network Managment Protocol) por medio del cual se puede acceder al concentrador desde cualquier punto de la red y hacer cualquier clase de modificaciones a los estados de los puertos, - proporciona una arquitectura tricanal que permite tener tres redes lógicas independientes; los concentradores de cableado de 6 y 17 slots pueden tener 6 y 17 módulos respectivamente, contando cada módulo con 12 puertos cada uno. Los módulos con que cuentan pueden ser *UTP, FDDI, BNC* y *AUI*.


Concentrador de cableado

Parte de este proyecto utiliza el protocolo de red *Ethernet* sobre *FDDI*, ya que cada concentrador cuenta con un módulo de fibra con dos puertos cada uno, los cuales son utilizados para enlazar las unidades de computo (el 'backbone' de dicha red esta formado con FDDI), y *UTP*, Debido a la existencia de cableado estructurado con par trenzado(UTP) en las unidades de computo.



SPARCstations

Estaciones de Trabajo SUN: En el centro de computo de este proyecto se cuenta con tres estaciones de trabajo de las cuales 2 de ellas se emplean como servidores.

SUN SPARCstation 10 modelo 41 que cuenta con un procesador SuperSPARC a 50 Mhz, 96 MB de memoria RAM, con 2700MB en disco duro y Sistema Operativo Solaris 1.1 por medio del cual puede atender a varios usuarios distribuidos en la unidad del computo central, y se emplea como servidor.

SUN SPARCclassic que cuenta con 32 MB de memoria RAM, con 1.05 GB en disco duro y Sistema Operativo Solaris 1.1 por medio del cual puede atender a varios usuarios distribuidos.

Servidor de Archivos Novell Netware 3.11

Servidor Novell 3.11: Leading Edge 486 DX33 como servidor de archivos. La cual funciona para una Red interna en la Unidad de computo, donde se puede obtener una variedad de software.

Estaciones de Trabajo: Se cuenta con varias computadoras para el uso del personal involucrado en el diseño y puesta en marcha de la Red.

El cableado UTP, se utiliza para interconectar el grupo de trabajo (Clientes) y servidores al concentrador (*HUB), Ethernet* solo ocupa 4 hilos (2 pares), es normal instalar 8 hilos (4 pares), cuando el error de comunicación está en el cable solo basta cambiar uno o dos pares para corregirlo.

Para cumplir con las normas de la *IEEE*, es importante tomar en cuenta el pareado de los cables como se puede observar en la siguiente figura, los colores y su asignación, tanto como para las rosetas como de los conectores RJ45, y el cable y sus componentes deben de ser del nivel 5, de tal manera que sus señales viajen adecuadamente con la calidad y cantidad determinada.

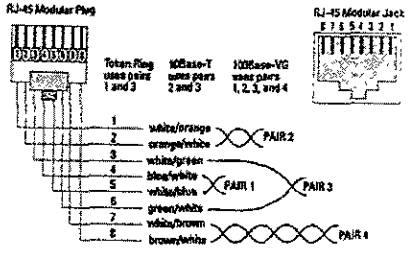


Ilustración 1Interconexiones RJ45 y su código de colores.

1. - Blanco/Naranja	2 - Blanco/Naranja	3. - Blanco/Verde	4. - Azul/Blanco
5. - Blanco/Azul	6. - Verde/Blanco	7 - Blanco/Café	8. - Café/Blanco

La ventaja de utilizar un cableado estructurado radica en lo multifuncional de su conector RJ45; ya que podemos emigrar entre diferentes arquitecturas a redes locales de alta velocidad; Token Ring (usando los pares 1 y3), 10 BASET (usando los pares 2 y 3), y 100BASEVg o 100FaseBaseT (usando todos sus pares disponibles).

Este tipo de redes suelen llamarse *Peer To Peer* (Punto a Punto), y nos permiten utilizar los recursos que tenemos entre terminales, al tener varios equipos configurados como servidor y terminal/cliente al mismo tiempo, es difícil determinar que equipos deben de encenderse primero, él ponerlos en sincronía es una tarea difícil de realizar pero no imposible gracias a los protocolos de administración podemos conseguir operadores *RMON* y crear un *bach file* que al encender los equipos, corra las funciones de sincronía evitando problemas a los usuarios.

El cableado de *Fibra Óptica* generalmente es realizado por las compañías prestadoras del servicio de conexiones digitales, debido a que se separan canales de troncales X.25 o Frame Relay con transporte de datos, voz y vídeo, a través de transmisiones de *Rx* (Rayos X) y Tx (Infrarrojos) de unidades publicas o privadas (Telmex, AvantelMCI, At&t, etcétera).

Dependiendo del *NOS* los recursos asignados pueden ser administrados incluyendo niveles de acceso, grupos de trabajo, y propiedades. Tantas combinaciones para configurar los recursos hacen que el trabajo de diseño sea más completo, una vez realizado este paso, el mantenimiento requerido es como el de cualquier red con servidores dedicados.

Apéndice B Firewalls: Ejemplos de Aplicación

Implementación de sistemas de seguridad.

Firewall, Ejemplo #1: Ruteador Filtra-Paquetes.

Los sistemas más comunes de firewall consisten en no mas que un Ruteador filtra-paquetes desplegado entre la red privada y el Internet. Este desempeña las funciones típicas de ruteo para desplazar él trafico entre las redes como si se estuviese usando las reglas de filtrado de paquetes para permitir/rechazar. Típicamente, las reglas de filtrado son definidas estrictamente tanto que los servidores en la red privada tienen acceso directo al Internet mientras los servidores en el Internet tienen acceso limitado al sistema de red privada. La postura externa de este tipo de sistemas firewall es probablemente "No todo lo específicamente permitido es denegado"

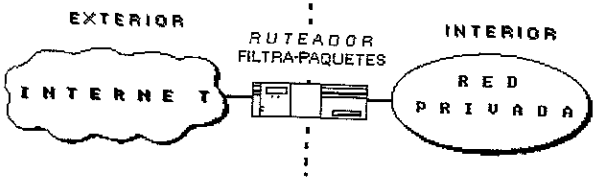


Ilustración 1. - Sistema Firewall: Ruteador Filtra-Paquetes.

Aunque, si bien para comenzar un sistema firewall este es la opción más barata y transparente para el usuario final, este posee todas las limitaciones de un Ruteador filtra-paquetes tal como la exposición al ataque por filtros configurados impropiamente y ataques que son "encubiertos" por los servicios permitidos. Desde que el intercambio directo de paquetes esta permitido entre los sistemas externos e internos, la exención de que sufra un ataque esta determinado por él numero total de servidores en los cuales esta permitido él trafico por el Ruteador filtra-paquetes. Esto significa que cada servidor accesado directamente desde el Internet necesita de un soporte sofisticado de autenticidad en usuarios y necesariamente deberá ser examinado regularmente por el administrador de la red por posibles señales de ataques perpetrados. Aun, si un simple Ruteador filtra-paquetes es penetrado, cada sistema en la red privada podrá estar comprometido a la seguridad del sistema.

Firewall, Ejemplo #2: Servidor Firewall De Resguardo.

El segundo ejemplo de Firewall, de la ilustración 2, emplea ambos sistemas un Ruteador filtra-paquetes y un servidor de defensa. Este sistema firewall provee un nivel mas alto de seguridad que el ejemplo anterior porque se implementa los dos sistemas: seguridad en el ámbito de red (filtrado-empaquetado) y a nivel aplicación (servicios Proxy). Aun, el intruso tiene que penetrar a los sistemas por separado antes que la seguridad del sistema pueda ser comprometida

Para este sistema firewall, se configura un servidor de defensa entre la red privada y el Internet con un Ruteador filtra-paquetes. Las reglas de filtrado en el Ruteador expuesto son configuradas para los sistemas externos teniendo únicamente acceso el servidor de defensa, él trafico direccionado a todos los sistemas internos es bloqueado. Desde que los servidores internos residen en una misma red como el servidor de defensa, la política de seguridad de una organización determina cuando los servidores internos tendrán acceso directo al Internet, o si ellos requieren del uso de servicios Proxy en el servidor de defensa. Los usuarios internos pueden forzar el uso de servicios Proxy por la configuración de las reglas de filtrado del Ruteador para aceptar únicamente trafico interno originándose del servidor de defensa.

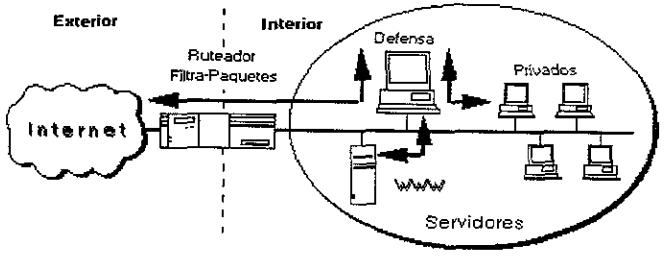


Ilustración 2. - Sistema Firewall: Servidor De Respaldo (Servidor De Defensa Simple-Homed).

Uno de los beneficios del firewall es que permite instalar un servidor de información publica provisto por servicios Web y FTP compartiendo un lugar en el segmento de red formado por el Ruteador filtra-paquetes y el servidor de defensa. Si se requiere de alta seguridad, el servidor de defensa puede correr los servicios proxy que requieran ambos usuarios (internos y externos) para acceder al servidor de defensa una vez que se comuniquen con el servidor de información. Si se adecua un nivel de baja seguridad, el ruteador podrá ser configurado para permitir a los usuarios externos tener acceso directo a los servicios públicos de información de la compañía o corporativo.

Un sistema de seguridad más uniforme puede construirse utilizando un sistema dual homed de servidores de defensa en la ilustración 3. Un servidor de defensa dual-homed posee dos interfaces de red pero la habilidad propia del servidor reside en direccionar él trafico entre las dos interfaces derivadas de servicios Proxy desabilitados. La topología forza a todo él trafico destinado a la red privada atravesar el servidor de defensa y provee seguridad adicional si a los usuarios externos se les concede acceso al servidor de información publica.

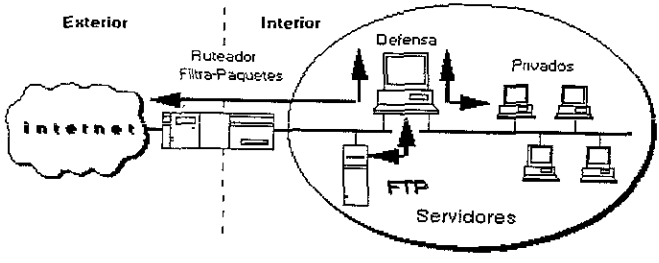


Ilustración 3. - Sistema Firewall: Servidor De Respaldo (Servidor De Defensa Dual-Homed).

Aunque el servidor de defensa es un sistema interno este puede ser accesado directamente desde el Internet, el conjunto de posibilidades abiertas del sistema a cualquier ataque esta limitado por este servidor. De cualquier modo, si se les permite a los usuarios sesionar en el servidor de defensa, el conjunto de posibilidades de atentar contra el sistema se expande incluyendo la red privada interna. De tal manera que es más fácil para un intruso comprometer un servidor de defensa estando sesionando en él. Es muy critico proteger y resguardar un servidor de defensa, por lo cual no debe de estar permitido su uso a los usuarios.

Firewall, Ejemplo #3: " Zona Desmilitarizada " o Subred De Resguardo Firewall.

El ejemplo final de firewall, vea la ilustración 4, emplea dos Ruteadores filtra-paquetes y un servidor de defensa. Con esto se crea el sistema mas seguro de Firewalls ya que los dos soportan la seguridad de la red y la seguridad a nivel-aplicacion mientras define una "Zona Desmilitarizada" (DMZ)[1] en la red. El administrador de la red asignara el lugar del servidor de defensa, los servidores de información, los puertos de módem, y otros servidores públicos en la red DMZ. Las funciones del DMZ son aisladas a pequeña escala entre el Internet y la red privada. Típicamente, el DMZ esta configurado para que los sistemas en Internet y los sistemas en la red privada puedan únicamente tener acceso a un limitado número de sistemas en él, pero la transmisión directa del trafico que cruce la red DMZ esta prohibido.

[1] Demilitarized Zone, por sus siglas en ingles

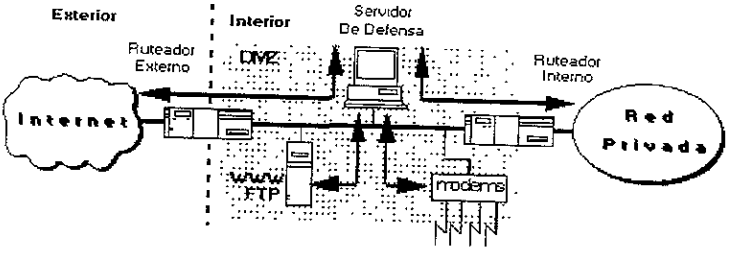


Ilustración 4. - Sistema Firewall: Respaldo De Sub-Red.

Para él trafico de venida, el ruteador externo esta proyectado contra los ataques estándar (fuentes de direccionamiento IP substraídas, fuentes de ruteo transgredidas, etc.) y administra el acceso a Internet por la red DMZ. Se permite a los sistemas externos el acceso únicamente al servidor de defensa (y posiblemente al servidor de información). El ruteador interno provee una segunda línea de defensa, administrando el acceso DMZ por la red privada aceptando únicamente él trafico originado del servidor de defensa.

Para él trafico originado en Internet, el ruteador interno administra el acceso a la red privada por la red DMZ. Esto permite que únicamente los sistemas internos accedan al servidor de defensa (y posiblemente al servidor de información). Las reglas de filtrado en el ruteador externo requieren del uso de servicios Proxy únicamente aceptando este él trafico de Internet por medio del servidor de defensa.

Estos son distintos beneficios importantes para el uso de un sistema firewall de subred de resguardo:

⇒ Un intruso tendrá que acceder a los tres componentes por separado (sin detección) para infiltrarse a la red privada - el ruteador externo, el servidor de defensa, y el ruteador interno.

⇒ Ya que el ruteador externo únicamente "anuncia" la red DMZ al Internet, los sistemas en este no tienen acceso a la protección de la red privada. ¡Esto permite la administración de la red para asegurarse que la red privada es "invisible" y que únicamente los sistemas seleccionados en el DMZ son "conocidos" por el Internet a través de la tabla de ruteo y los servicios intercambiables de información DNS[2]!.

⇒ Ya que el ruteador interno únicamente "anuncia" la red DMZ a la red privada, los sistemas privados no tienen acceso directo al Internet. ¡Esto garantiza que los usuarios internos pueden únicamente acceder al Internet vía servicios Proxy residentes en el servidor de defensa!.

[2] Domain Name Service, Servicio provisto por Internet (v. Cap. TCP/IP)

⇒ El ruteador filtra-paquetes direcciona él trafico a los sistemas especificados en la red DMZ eliminando la necesidad de desarrollar al servidor de defensa como un dual-homed.

⇒ El ruteador interno soporta grandes paquetes a través de un servidor de defensa dual-homed cuando funciona como el sistema final de un firewall entre la red privada y el Internet.

⇒ Ya que la red DMZ es diferente a la red privada, se puede instalar un traductor de direcciones (NAT)[3] en el servidor de defensa para eliminar la necesidad de re-enumerar o re-segmentar en sub-redes a la red privada.

[3] Network Address Translator, por sus siglas en ingles

Apéndice C[1] Servicios de Conexión y Enlaces Digitales al Internet en México.

Servicios de Conexión a Internet

Para conectar una computadora o una red local de computadoras (LAN), y una red metropolitana de computadoras (MAN) al Internet, se necesita contar con un servicios de conexión a Internet:

@ Conexión Dial-UP.

@ Conexión Lan-DIAL.

@ Conexión Vía Línea Dedicada (Enlace Dedicado).

Conexión Dial-Up

Es un servicio que se ofrece a computadoras personales, ya que desde la oficina, casa o escuela por medio de un módem se interconecta a una compañía de servicios de acceso a Internet (ISP) como **Datanet®**, **Spin®**, **Internet Directo®**, etc. Y a otras compañías que además de prestar conexión ofrecen servicios de valor agregado (**America On Line™** , **Compuserve™** de México, etc).

Características del enlace

- Acceso gráfico y de datos al Internet.
- Enlaces soportados de 9.6Kbps hasta 56Kbps.

Lo único que se necesita es tener una línea telefónica e instalar un módem con protocolos de conexión *SLIP / PPP* en una computadora personal con cualquier sistema operativo que sea compatible con el manejo de paquetes de comunicación *TCP/IP* para 16 y 32 Bits. (DOS 6.22 o Avanzado, Win3 0 o Avanzado, etc.) Y el pago del servicio debido a que el acceso es por redes privadas.

Conexión Lan-Dial

Las ventajas de este servicio se deben principalmente a los *Sistemas Operativos de Red* (N.O.S., de sus siglas en ingles). Debido a que puedo tener varias computadoras interconectadas con tarjetas de red *Ethernet* a un concentrador (*Hub)* y a su vez a un servidor con módem, el cual administrara las conexiones al Internet teniendo la red local conexión *TCP/IP.*

Características del enlace

Posee las mismas características que un enlace *Dial-Up* pero se necesita satisfacer requerimientos adicionales, según el *ISP* que provee el servicio.

A continuación se señala algunos de los requerimientos:

- Servidor de Red.

Computadora x86 de cuarta generación con 16 Mbs de memoria (mínimo), con Módem 33,600 Mbps (mínimo), Línea telefónica, conexión de red local (TCP/IP), y Software de enlace LAN.

- Computadoras de Red.

Computadoras x86 de cuarta generación (mínimo 8Mbs RAM y 8Mbs en Disco Duro, y conexión *TCP/IP* de cada máquina).

Cabe además mencionar que dependiendo del tipo de servicios de Internet que presta el ISP se cobra primas adicionales por diferentes conceptos: horas de conexión, número de claves e-mail, capacidad de almacenamiento en Disco duro, servicios privados de Telnet, FTP, Gopher, servidores NNTP, WWW, etc.

Conexión vía Línea Dedicada

El establecimiento de una conexión a Internet de estas magnitudes esta basado prácticamente en el uso y la disposición de servicios para comunicación entre computadoras en el ámbito metropolitano y regional, es más un ISP posee este tipo de conexiones para prestar servicios subarrendados de comunicaciones digitales y servicios básicos de Internet.

Generalmente son empresas o instituciones que necesitan contar con una conexión a Internet totalmente Digital a velocidades desde 64Kbps hasta 2.048 Mbps prestadas por la red publica telefónica o privada.

Desde una simple computadora conectada vía telefónica a una red local, hasta cientos de computadoras, estaciones de trabajo, servidores CISC, RISC y Mainframe de un edificio corporativo son parte diaria del tráfico de Internet a través de un *Enlace Dedicado.*

Características del enlace

- Acceso gráfico, voz, datos y vídeo al Internet.
- Velocidades desde E0 (64Kbps) hasta E1 (2.04Mbps)
- Trafico 24 Hrs del día. Todo el año.

Opciones de enlace digital

- RDI (Red Digital integrada).
- Microonda digital.

Estos enlaces se cotizan por separado con los carriers[1] telefónicos como **Teléfonos de México, AvantelMCI México, Iusanet de México, AT&T de México**, etc.

Requisitos del enlace

Dependiendo del número de canales DS-0 que se desee contratar y si se cuenta o no con RDI en las instalaciones, generalmente se necesitará:

- Una línea G.703 (o varias), contratada a **Telmex** o algún otro carrier.
- Un ruteador con puerto de red local (*Ethernet, Token Ring, FDDI, Etc.*) y un puerto serial (o varios).
- Un *CSU / DSU* (o varios) o un *MX*.
- Software de Administración TCP/IP para el ruteador que permita realizar conexiones tipo *HDLC* o *PPP*.

Contratación y operación

El hecho de establecer un *Enlace Digital Dedicado* permite infinitas aplicaciones dentro del *Internetworking* proporcionando una gama completa de servicios de voz, datos y vídeo.

- Acceso 24 hrs. Al día a Internet.
- Registro de dominio en Internet.
- Instalación del servidor DNS primario.
- Disposición de direcciones IP clase "C", una o varias, de acuerdo al número de canales contratados.

Primero la empresa debe ya contar con una infraestructura de red bajo cableado estructurado, si no contase aún con esto, varios *Carriers* ofrecen servicios de valor agregado que incluye diseño y desarrollo de redes, ventas de equipo de red, servidores, capacitación y asesoría técnica.

Aún dentro de la legislación de comunicaciones establecida por la Secretaria de Comunicaciones y Transportes, no existe la tarifación sobre la magnitud del tráfico en los *Enlaces Digitales.* Solo existe un cargo único por contratación y un cargo mensual que depende solo del número de canales DS-0 que se hallan requerido al *Carrier* local.

---

[1] Prestadores de servicios de enlaces.

Enlaces digitales disponibles en México

Hoy en día el hecho de poder proveer servicios de Internet en México, es un gran mercado cautivo para las redes telefónicas privadas y un gran reto a las redes públicas para ofrecer conexiones fiables, rápidas y seguras.

Los casos que expondremos aquí son:

~ Internet Directo®, **Telmex**

~ InternetMCI™, **Avantel**

~ Access Network™, **At&t**

Debido a su participación dentro del mercado actual de telecomunicaciones en México recién liberado.

Telmex

Ofrece la experiencia de la infraestructura Básica de telecomunicaciones en México. Con su área de servicios Telecorp pone a disposición de los usuarios empresariales y corporativos una amplia gama de enlaces:

- Red digital integrada.
- Enlaces privados locales, nacionales, internacionales y de cruce fronterizo (E-0, DS-0, E-1,y E-1 punto - multipunto).
- Enlaces a Internet vía **Sprint**™ internacional por 7 canales de 1.5 Mbps.
- Troncales digitales, y analógicos.
- Enlaces satelitales de voz y datos.
- Vídeo enlace digital (Videoconferencia)
- Red pública de datos (Frame Relay)

Entre otros de gran importancia para grupos corporativos nacionales e internacionales que requieran de eficiencia y rapidez en la transmisión de señales de voz, datos y vídeo.

AvantelMCI

Cobertura

Avantel Frame Relay está disponible en todo el país. El servicio se ofrece de manera local en veintisiete ciudades.

Avantel ha construido una red de telecomunicaciones que no tendrá rival en lo que se refiere a confiabilidad, flexibilidad y capacidad de respuesta. La Red **Avantel** proporcionará una gama completa de servicios de voz, datos y de valor agregado desde y hacia cada teléfono en México.

Avantel realizará en total una inversión de $1,800 millones de dólares en la construcción de su red en cinco etapas. En la primera fase, terminada en agosto de esté año Avantel invirtió un total de $600 millones de dólares para construir su red **Avantel Frame Relay**, que crea un Triángulo de Cristal, con 5,300 Km. de fibra óptica, enlazando a México, D.F., Guadalajara y Monterrey junto con otras 30 ciudades.

Durante los próximos seis años, **Avantel** instalará 15,000 kms. adicionales de una red de fibra con tecnología *SONET* completamente digital. Cabe mencionar que en 1997, **Avantel** proporcionará servicios a más de 60 ciudades.

Ventajas del frame relay

Frame Relay es la tecnología preferida en todo el mundo para servicios de telecomunicaciones de datos, los clientes logran ahorros directos comparando con soluciones similares basadas en "líneas privadas". El servicio ofrece a los negocios una conexión directa de alto rendimiento, con la flexibilidad que requieren las soluciones *cliente-servidor*, *LAN* a *LAN*, *LAN* a *host* y de cómputo centralizado.

AVANTEL Frame Relay es un servicio basado en los estándares del Frame Relay Forum, organización fundada en 1990 por la industria de telecomunicaciones y cómputo con el interés por desarrollar e implementar Frame Relay sobre la base de estándares internacionales.

La red **Avantel Frame Relay** ha sido diseñada para la transmisión de datos de alto desempeño mediante enlaces de alta velocidad y el uso eficiente del ancho de banda. Ofrece cobertura nacional y es la más flexible en opciones para la selección de velocidades de puertos y Tasa Comprometida (CIR - Commited Information Rate) para Circuitos Virtuales.

La red **Avantel Frame Relay** tiene cobertura nacional y es una de las mas flexibles con respecto a opciones para la selección de velocidades de puertos y circuitos virtuales.

Durante 1994, *Frame Relay* fue el servicio de datos de mayor crecimiento en la industria. En los próximos años, es clara una tendencia creciente del mercado mundial de productos y servicios basados en esta tecnología debido al alto desempeño y bajo costo de la tecnología.

Avantel Frame Relay se ofrece en México con los mismo estándares de calidad que en Estados Unidos reciben los clientes del servicio **MCI HyperStream.**™

Características del cliente

Avantel Frame Relay es la mejor solución de comunicación a clientes con:

Redes locales en dos o más localidades a interconectar:

Redes LAN - LAN:

Servicios de Archivos	e-mail	Groupware
Netware	SMTP	Lotus Notes
Windows NT	MS-Mail	Exchange
Banyan Vines	MHS	Groupwise
DEC Pathworks	cc: Mail	DEC LinkWorks

Avantel Frame Relay ofrece una solución de telecomunicación de datos para aplicaciones :

Cliente servidor

SAP		Hosts a host
Informix	Lan a hosts	Redes Unix
Oracle	Emulación de Terminal	DECNet
SQL Server	Transferencia de archivos.	APPN
Sybase		HP

SNA: Opción a líneas asíncronas para conexión de controladores de comunicaciones/terminales remotos.

Internet MCI de Avantel™

Ofrece enlaces dedicados desde 64kbps, hasta 2.048 Mbps. , Eliminando los altos costos del arrendamiento de circuitos internacionales. Proporcionando acceso directo al backbone de Internet con una velocidad de 622Mbps (OC12), proporcionando 5 niveles de redundancia, garantizando así una conexión confiable y libre de errores al 100% al interconectar redes LANs y WANs al Internet. El backbone OC12 vía **MCI** incluye:

- ≈ Intercambio de mensajes en Internet.
- ≈ Ejecución de software en computadoras remotas.
- ≈ Funcionalidad en transferencia a escala de archivos.
- ≈ Alta de sus propios servidores en Internet, gopher o www.
- ≈ Comunicación entre consumidores, arrendadores, y prestadores de servicios.

Las líneas de acceso privado son interconectadas mediante POPs, DS3 a gateways cercanos a **InternetMCI** los clientes pueden rentar servicios de conexión dedicada a velocidades de 56Kbps (DS0 y DDS) a T1 (1.544Mbps), NtxT1(3Mbps, 4.5Mbps y 10 Mbps) y troncales DS3. El servicio vía NxT1 provee diferentes anchos de banda convenientes a sus necesidades.

Los servicios digitales de enlace directo vía **Hyperstream™** e **internetMCI** son proporcionados mediante los siguientes puertos:

56/64 Kbps. 512 Kbps. 128 Kbps. 1472/1536 Kbps. 256 Kbps.

Cabe mencionar que las conexiones Direct Access NxT1, o *Ethernet* están siendo desarrolladas y pronto podrán estar disponibles.

AT&T Alestra

Es una de las principales compañías de telecomunicaciones mundiales con representación en México de ya hace 25 años.

Sus principales servicios son:

AT&T Frame Relay

AT&T Frame Relay es un servicio cada vez más popular para todas aquellas compañías que requieren transporte de información a

Alta velocidad como una mejor alternativa costo beneficio. El servicio puede ser utilizado por aquellas compañías que necesiten

Ampliar su capacidad de transmisión de datos o que busquen establecer enlaces de datos entre sus oficinas distribuidas geográficamente.

Algunas aplicaciones del servicio **AT&T** Frame Relay son:

- Conexión de redes de área local y centros de computo (servidor a servidor).
- Aplicaciones en línea tipo cliente/servidor.
- Transmisión de imágenes y gráficas.
- Respaldo periódico de grandes volúmenes de información.
- Manejo de bases de datos distribuidas.

AT&T Líneas Privadas Digitales

Los servicios **AT&T** Líneas Privadas Digitales pueden ser utilizados para extender la cobertura de negocios de las compañías y reducir los costos de telecomunicaciones utilizando el personal de **Alestra** dedicado a la administración de los servicios.

Estos servicios son una herramienta efectiva que proporcionará una ventaja competitiva y un incremento en la productividad para compañías con múltiples localidades nacionales o internacionales.

Aplicaciones típicas que pueden ser desarrolladas sobre el servicio **AT&T** Líneas Privadas Digitales son:

Interconexión LAN/WAN, Transporte multimedia (voz, datos y vídeo), procesamiento de imágenes, consulta a bases de datos, servicios de telemercadeo, transferencia de archivos, CAD/CAM (manufactura asistida por computadora), videoconferencia y redes de telefonía y conmutadores.

Una línea privada puede ser considerada como una extensión física de la red local del cliente (LAN - Local Area Network) para transportar servicios de voz (enlaces entre conmutadores, enlaces remotos de telefonía, extensiones remotas, etc.), servicios de datos (conexiones LAN/WAN - Wide Area Network

- entre computadoras, microcomputadoras, minicomputadoras, terminales remotas y entre todo tipo de redes de cómputo locales) y servicios de vídeo (videoconferencia, vídeo monitoreo, vídeo en tiempo real, etc.) todo sobre el mismo enlace físico. El enlace es administrado completamente por el cliente.

Información técnica

El servicio **AT&T** Líneas Privadas Digitales está definido como un canal digital transparente y no conmutado entre dos oficinas de un cliente que no requieren ningún tipo de señalización.

El servicio "end to end" o "extremo a extremo" está compuesto de dos elementos, la línea privada en él core de la red de **Alestra** que es la combinación de los tres anillos *SDH* interconectados de la red y el acceso que es la sección que completa un circuito privado hasta la oficina del cliente.

Tipos de Servicios

Circuitos E0/DS0: Enlaces digitales dedicados síncronos punto a punto a una velocidad de 64 kbps entre dos oficinas del cliente. El servicio se ofrece para enlaces Domésticos, a Estados Unidos con **AT&T** y al resto del mundo (WorldSource Services).

N x E0 o IBR: Enlaces digitales dedicados punto a punto en velocidades múltiplo de 64 kbps. Las velocidades típicas de este servicio son 128, 256, 384, 512, 768 y 1,024. **Alestra** puede ofrecer cualquier velocidad intermedia entre 128 y 768 kbps. Los servicios pueden ser domésticos, a Estados Unidos o al resto del mundo (WorldSource Services).

E1: Enlaces digitales dedicados punto a punto entre dos oficinas del cliente a una velocidad E1. El E1 se ofrece canalizado en 32 ranuras de tiempo (cada una equivale a un E0). La ranura de tiempo cero está dedicada a sincronización de red por lo que la velocidad efectiva del servicio es de 1,984 kbps (31 x E0). El servicio se ofrece con cobertura nacional, a Estados Unidos y al resto del mundo (WorldSource Services)

AT&T WorldSource Services: A través de WorldPartners **Alestra** ofrecerá líneas privadas internacionales al resto del mundo. Estos servicios son ofrecidos utilizando una sola plataforma tecnológica bajo la filosofía de SPOC y OSS. Los servicios WorldSource cubrirán los rangos de velocidad E0, NxE0 y E1.

Servicios Futuros: N x E1 (velocidades intermedias de 8, 10 y 16 Mbps para transmisión dedicada en enlaces punto a punto); E3 (servicio a 34.368 Mbps); STM-1 (enlaces digitales dedicados punto a punto a una velocidad de 155 Mbps en plataforma SONET); Servicios Satelitales (transmisión y recepción de voz, datos y vídeo a velocidades de 64 kbps y hasta 2 Mbps en redes Satelitales punto a punto o multipunto); Servicios por Demanda (servicios disponibles sobre la base de reservación).

Cobertura

En la primera fase del servicio **Alestra** ofrece el servicio **AT&T** Líneas Privadas Digitales "punto a punto" en las 20 ciudades que integran la red de fibra óptica de **Alestra**, las cuales se listan a continuación:

México	Matamoros	Saltillo	Morelia
Monterrey	Cd. Victoria	Torreón	Pachuca
Guadalajara	San Luis Potosí	León	Toluca
Nvo. Laredo	Aguascalientes	Celaya	Cuernavaca
Reynosa	Zacatecas	Querétaro	Puebla

En esta misma fase se incorporarán servicios" de cruce fronterizo internacional en las ciudades de Tijuana y Cd. Juárez.

---

[1] Toda la información aquí presentada es propiedad intelectual de la empresa que se representa y es de dominio público.

" Para más información sobre los servicios de telecomunicaciones aquí citados, favor de contactar a los representantes locales de sus servicios telefónicos.

GLOSARIO

A ADVANCED RESEARCH PROJECTS AGENCY NETWORK. Vea ARPANET

ARPANET.

(Advanced Research Projects Agency Network). Red experimental con fines militares establecida en los setenta, en la cual se probaron las teorías y el software en los que esta basado Internet. ARPANET era una red experimental que apoyaba la investigación militar, en particular la investigación sobre cómo construir redes que pudieran soportar fallas parciales (como las producidas por los bombardeos) y aún así funcionar. La red fue diseñada para requerir un mínimo de información de las computadoras que forman parte de ella. La filosofía era que cada computadora en la red se pudiese comunicar, como un elemento particular con cualquier computadora.

ATM.

(Asynchronous Transfer Mode): Modo de transferencia asíncrono. Estándar CCITT para retransmisión de celdas (cell relay) en el cual la información para diferentes tipos de servicio (voz, vídeo y datos) se transmite en pequeñas celdas de tamaño fijo. También, modo de transmisión BISND en el cual se usa una versión acelerada de multiplexaje asíncrónico por división de tiempo (ATDM) para transferir flujos múltiples de información en un canal de comunicación.

B BASES DE DATOS DISTRIBUIDAS.

Bases de datos que se pueden encontrar en diversas partes del planeta y que se presentan ante el usuario como una base de datos única. Un ejemplo de ello es el DNS (Domain Name Service) en que se basa Internet, donde las direcciones de las computadoras se encuentran en diversas computadoras (cada una encargada de un dominio), y que se presentan ante el usuario como una base de datos única con todos los dominios del planeta.

BINARIO.

Archivo que contiene códigos y caracteres que sólo pueden ser utilizados por tipo específico de software. Los más comunes son los archivos ejecutables, gráficos y documentos con formato.

BIT. (Binary DigIT).

Unidad mínima de almacenamiento de la información. Su valor puede ser 0 ó 1 ó verdadero o falso.

BLOQUEO (BLOCKING).

1) En algunos sistemas se requiere que los mensajes tengan un tamaño específico considerando la frecuencia en que ocurren los errores. Bloqueo se refiere a la segmentación de mensajes largos en pequeñas partes, para que estos puedan cumplir con los requerimientos de tamaño especificados. 2) Término usado en referencia a un PBX ("Private Branch Exchange" o cualquier otro equipo de comunicación), que a veces no puede dar servicio a un usuario por falta de un

canal de comunicación. Se dice que el usuario está "bloqueado".

BPS.

Baudios por segundo. Numero de cambios que sufre la señal por segundo y es indicativo de la cantidad de bits por segundo que se están transmitiendo. Un puede aumentar la velocidad de enlace si utiliza compresión de datos. Para aprovechar la máxima velocidad de un módem, tanto el proveedor como el usuario deben de tener módems que operen a la máxima velocidad y utilizar ambos la compresión de datos.

BYTE.

Conjunto de 8 bits. Suele representar un valor asignado a un carácter.

BGP (Border Gateway Protocol).

Protocolo de compuerta o pasarela exterior utilizado en NSFnet. Han aparecido cuatro versiones mayores de BGP

BRIDGE. Vea Puente

BROADBAND.

Se refiere a la técnica de cable coaxial en la cual varias señales moduladas (generalmente sobre frecuencias diferentes, ver multiplexor) sobre varias portadoras se transmiten sobre un solo cable coaxial.

BROUTER

Dispositivo que combina las funciones de un puente (bridge) y un "router". Los brouters pueden encaminar uno o más protocolos tales como TCP/IP y XNS, y proveer un puente para todo tráfico de datos. Contrasta con "bridge", "router" y "gateway".

BUFFERS.

Espacio de almacenaje temporero. Los datos pueden ser almacenados aquí a la antes o después de la transmisión. Un buffer se puede usar para compensar las diferencias que existen entre la velocidad de transmisión y la velocidad de procesamiento.

Buffer.

Es un dispositivo o un área en memoria que es usado para almacenar datos temporeramente.

C

CACHE

Esta es una cantidad de RAM reservada para mantener datos que van a ser accesados nuevamente. El segundo acceso, que va a encontrar los datos en RAM, es muy rápido.

CABLEADO

Columna vertebral de una red que utiliza un medio físico de cable, casi siempre

del tipo de red de área local (LAN), que lleva la información de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

CALL PACKET

Bloque de datos que lleva direcciones y otra información que se necesita para establecer un circuito virtual conmutado (SVC) X.25.

CARRIER (PORTADORA)

Señal que se usa para "acarrear" o transportar señales de base de banda sobre un medio de comunicación. La frecuencia de la portadora es usualmente más alta que la frecuencia de la señal de base de banda.

CCITT X.25

Estándar internacional que define protocolos de comunicación de conmutación de paquetes ("packet-switched comunication") para redes privadas o públicas.

CHANNEL (CANAL)

También se le denomina circuito, línea, "path". Es un medio, físico o lógico, para mover datos en una dirección. Un canal puede ser SIMPLEX si los datos se envían siempre en una sola dirección o HALF DUPLEX si se envía información en ambas direcciones alternadamente. Dos canales se pueden combinar para proveer transmisión FULL DUPLEX. Frecuentemente nos referimos a estos dos canales como un canal FULL DUPLEX.

CHECKSUM (Suma de verificación)

Número entero calculado a partir de una secuencia de octetos que son tratados como enteros en una suma para calcular su valor total. Una suma de verificación se utiliza para detectar errores que aparecen cuando una secuencia de octetos se transmite de una máquina a otra.

Por lo general, el software del protocolo calcula una suma de verificación y la anexa al paquete que se está transmitiendo. En la recepción, el software de protocolo verifica el contenido del paquete recalculando la suma de verificación y comparándolo con el dato obtenido de la transmisión. Muchos protocolos TCP/IP utilizan una suma de verificación de 16 bits, calculada por complemento aritmético a uno con todos los campos enteros en el paquete almacenados en el orden de octetos de la red.

CIRCUITO CONMUTADO (CIRCUIT SWITCHED)

Ruta de transmisión dentro de una red conmutada (por ejemplo la red telefónica o un conmutador telefónico de una empresa) en la que se crea una ruta cuando una estación origen especifica una estación de destino y esa ruta se mantiene por la duración de la llamada.

CLIENTE.

a) Una aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red.

b) Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio.

Vea Modelo cliente-servidor

COLUMNA CENTRAL DE RED (backbone)

Backbone. Línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una vía con gran ancho de banda. Un backbone conecta dos puntos o redes distanciadas geográficamente, a altas velocidades.

CONECTION ORIENTED Orientado a la conexión.

Término empleado para describir transferencias de datos posteriores al establecimiento de un circuito virtual

CONECTIONLESS Sin conexión.

Término empleado para describir transferencias de datos sin la existencia de un circuito físico.

CRC. (Cyclic Redundancy Code).

Número entero calculado a partir de una secuencia de octetos utilizados para detectar errores que aparecen cuando una secuencia de octetos se transmite de una máquina a otra. Por lo general, el hardware de red de conmutación de paquetes calcula un CRC y lo añade a un paquete cuando se transmite. Durante la recepción, el hardware verifica el contenido del paquete recalculando el CRC y comparándolo con el valor enviado. Aún cuando hace a las computadoras más caras, un CRC detecta más errores que una suma de verificación que se vale de métodos de suma.

Vea Checksum

CSMA/CD

Característica del hardware de red que al operar permite que varias estaciones compitan por el acceso a un medio de transmisión escuchado para saber si el medio está ocupado, y mecanismo que permite al hardware detectar cuando dos estaciones intentan transmisiones simultáneas. Ethernet utiliza CSMA/CD

CSU (Channel Service Unit).

Unidad de servicio al canal. Dispositivo de interfaz digital que conecta equipos terminales de usuario al ciclo (loop) telefónico digital local.

CSU/DSU/ROUTER

Cuando se trata de llevar a cabo un servicio de acceso corporativo, es importante tomar en cuenta un CSU/DSU el cual nos permite descanalizar la línea digital en

una interface adecuada para su posterior interconexión con el ruteador

DATAGRAMA

Agrupamiento lógico de información enviada como unidad de la capa de red en un medio de transmisión, sin el establecimiento preciso de un circuito virtual.

El término paquete, frame, segmento y mensaje también se emplean para describir agrupaciones lógicas de información en varios niveles del modelo de referencia OSI y en otras áreas de la tecnología. Los datagramas IP son las unidades primarias de información en Internet.

DIALUP. Vea Línea Conmutada

DIRECCIÓN ELECTRÓNICA (address).

Dirección de un usuario en Internet. Por medio de ella es posible enviar correo electrónico a un usuario. Esta es única para cada usuario y se compone por el login de un usuario, arroba y el nombre del servidor de correo electrónico. p.e. usuario@computadora.com

DIRECCIÓN IP.

La dirección del protocolo de Internet (IP) es la dirección numérica de una computadora en Internet. Cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como 132.248.53.10

DNS (Domain Name Service)

Sistema de base de datos distribuida en línea y utilizado para transformar nombres de máquinas en direcciones IP que puedan leer los usuarios. Los servidores DNS, a través de Internet, implantan un espacio de nombres jerárquico que permite a las localidades contar con libertad para asignar nombres de máquinas y direcciones. DNS también soporta transformaciones separadas entre destinos de correo y direcciones IP.

Vea Bases de datos distribuidas

ENRUTADOR

Elemento que determina la trayectoria más eficiente de datos entre dos segmentos de red. Operan en la capa superior del modelo OSI a la de los puentes la capa de red- no está limitado por protocolos de acceso o medio.

Vea Gateway, Puente

EGP (Exterior Gateway Protocol).

Protocolo utilizado por un ruteador, en un sistema autónomo, para anunciar la dirección IP de la red de tal sistema hacia un ruteador en otro sistema autónomo.

ENCAPSULATIÓN (encapsulación)

Técnica utilizada por los protocolos estratificados por capas en el cual un

protocolo de nivel inferior acepta un mensaje de un protocolo de nivel superior y lo coloca a la sección de datos de su trama de bajo nivel. La encapsulación implica que los datagramas que viajan a través de una red física cuentan con una secuencia de encabezados de los que el primero proviene de la trama de red física, el siguiente del protocolo de Internet (IP), el siguiente del protocolo de transporte, y así sucesivamente.

FDDI (Frequency Division Multiplexing)

Tecnología de red token ring basada en fibras ópticas. FDDI especifica una razón de transferencia de datos a 100 Mbps utilizando luz con una longitud de onda de 1300 nanómetros, limitando las redes a 200 Km de longitud aproximadamente y con repetidores cada 2 Km o menos.

FIREWALL (muro de seguridad)

Configuración de ruteadores y redes colocados entre la organización interna de una red de redes y su conexión con redes de redes externas, con el fin de proporcionar seguridad.

Software que reside dentro de una computadora de alta capacidad, cuya función es garantizar la seguridad de LAN interna y prevenir el acceso de intrusos (Hackers) que en un momento dado intenten accesar a la LAN interna para realizar vandalismos electrónicos. Entre las funciones principales adicionales son NAT (Network Address Translation) la cual permite el cambio de direcciones homologadas a no homologadas, también permite el manejo de dominios dual, POP etc.

FRAME RELAY

Retransmisión de marcos. Protocolo empleado en la interfaz entre dispositivos de usuario y equipo de redes. Es más eficiente que X 25, protocolo del cual generalmente se considera reemplazo.

FRAME (trama)

Literalmente, un paquete transmitido a través de una línea serial. El término deriva de los protocolos orientados a carácter que añaden caracteres especiales de comienzo-de-trama y de fin-de-trama cuando transmiten paquetes. Este término se utilizó a lo largo de esta tesis para nombrar a los objetos que transmiten las redes física.

GATED (GATEway Daemon)

Programa que corre un enruteador o ruteador que utiliza un IGP para reunir información de ruteo desde dentro de un sistema autónomo, y un EGP para anunciar la información a otros sistemas autónomos.

GATEWAY (compuerta)

Originalmente los investigadores utilizaron la gateway (compuerta) IP para referirse a las computadoras dedicadas al ruteo de paquetes; los vendedores han

adoptado el término ruteador. Compuerta significa, ahora, programa de aplicación que interconecta dos servicios (por ejemplo una compuerta de e-mail)

HARDWARE ADDRESS (dirección de hardware)

Dirección de bajo nivel utilizada por las redes físicas. Cada tipo de hardware de red tiene su propio esquema de direccionamiento (por ejemplo, una red Ethernet las direcciones son de 48 bits).

HELLO

Protocolo utilizado en la red de columna vertebral NSFNET. Hello resulta interesante pues elige rutas con un tiempo de retardo mínimo.

HOST (anfitrión)

Cualquier sistema de computadora de usuario final que se conecta a una red. Los anfitriones abarcan desde computadoras personales hasta supercomputadoras. compare con ruteador

IGP (Interior Gateway Protocol)

Término genérico aplicado a cualquier protocolo utilizado para difundir accesibilidad de red e información de ruteo dentro de un sistema autónomo Aun cuando no es el único estándar IGP, el RIP está entre los más populares.

IETF (Internet Engineering Task Force)

Grupo de personas vinculado de cerca con el IAB, que trabaja en el diseño y la ingeniería del TCP/IP y la red global de Internet. El IETF se divide en áreas, cada una de las cuales cuenta con una administración independiente. Las áreas, a su vez, se dividen en grupos de trabajo.

INTERNET PROTOCOL vea IP

INTEROPERABILITY (interoperabilidad)

Capacidad del software y hardware en máquinas diversas, de vendedores diferentes para comunicarse con éxito Este término es el que describe mejor el objetivo del enlace de redes, cuya meta es definir un ambiente de red abstracto independiente del hardware, en el que sea posible construir una computación distribuida, en el ámbito de transporte de red, sin conocer los detalles de las tecnologías subyacentes.

INTRANET.

Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno. Por ejemplo, muchas compañías tienen servidores World Wide Web disponibles solo para sus empleados.

IP (Internet Protocol)

Protocolo estándar que define a los datagramas IP como la unidad de información que pasa a través de una red de redes y proporciona las bases para el servicio de

entrega de paquetes sin conexión y con el mejor esfuerzo. El IP incluye el control ICMP y los protocolos de mensaje de error como parte integral. El conjunto de protocolos completo es conocido como TCP/IP siendo estos los más importantes.

ISDN. Red Digital de Servicios Integrados. (RDSI)

(Integrated Services Digital Network). En español se abrevia RDSI. En el servicio de ISDN las líneas telefónicas transportan señales digitales en lugar de señales analógicas, lo que aumenta considerablemente la velocidad de transferencia de datos a la computadora. Si se cuenta con el equipo y el software necesarios, y si la central telefónica local ofrece ISDN y el proveedor de servicios lo soporta, el ISDN es posible utilizarlo. La velocidad de transferencia que puede alcanzar ISDN es de 128,000 bps, aunque en la práctica las velocidades comunes son de 56,000 o 64,000

LÍNEA CONMUTADA.

Se refiere al tipo de conexión que se establece usando un emulador de terminal y un módem

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 el IEEE 802.2 que incluye variantes sin y con conexión.

MAC (Media Access Control)

Se trata en general de los protocolos de hardware de bajo nivel utilizado para accesar una red en particular. La Subcapa MAC se encarga de los asuntos de acceso al medio de comunicaciones, como por ejemplo determinar si se usará token passing (paso de estafeta) o contention (competencia).

El término dirección MAC se utiliza con frecuencia como sinónimo de dirección física.

MIB (Management Information Base)

Conjunto de variables (bases de datos) que un ruteador mantiene corriendo SNMP. Los administradores pueden obtener o almacenar estas variables. El estándar actual es MIB-II.

MODELO CLIENTE-SERVIDOR.

El modelo cliente-servidor se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que poseen el recurso. Los clientes sin embargo no dependen totalmente del servidor. Ellos pueden realizar los procesamientos para desplegar la información (por ejemplo en forma gráfica). El servidor los provee únicamente de la información sin hacerse cargo de otros procesos. El tráfico en la red de esta forma

se ve aligerado y las comunicaciones entre las computadoras se realizan más rápido

MÓDEM.

Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados (ISDN), mediante un proceso denominado de modulación (para transmitir información) y demodulación (para recibir información), de ahí su nombre. La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 Kbps, sin embargo los más comerciales actualmente son los de 28 Kbps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems se dividen en internos (los que se colocan en una ranura de la computadora) y en externos (que se conectan a un puerto serial de la computadora). Instalación Módems Internos. Estos deben ser configurados antes de ser instalados. Es necesario mover los puentes (jumpers) para indicar un puerto (COM) y una interrupción (IRQ). Módem Externos. La instalación requiere de un cable (DB25 o de 25 agujas macho a 25 agujas hembra o a 9 agujas hembra) que conecte directamente al puerto serial de la computadora. Es necesario asegurarse que no sé esta utilizando un puerto compartido con otro elemento de hardware (p.e. un mouse). Para ello debe instalarse en COM2 o COM4 si el mouse esta instalado en COM1 o en COM1 o COM3 sí el mouse esta instalado en COM2. La interrupción (IRQ) depende del puerto donde este instalado

Vea Acceso conmutado, Script, SLIP, PPP.

MULTI-HOMED HOST (anfitrión múltiple)

Anfitrión que utiliza el TCP/IP y que tiene conexiones con dos o más redes físicas.

NFS (Network File System)

Protocolo desarrollado por SUN Microsystems Incorporated que utiliza el IP a fin de permitir que un conjunto de computadoras coopere para accesar los sistemas de archivos de otras, como si éstas fueran locales.

NIC (Network Information Center)

Antecesor de INTERNIC (INTERnet Network Information Center) que proporciona información sobre servicios de Internet y documentos de protocolos. Además, INTERNIC maneja el registro de las direcciones IP y los nombres de dominio.

NSF (National Science Foundation)

Dependencia gubernamental de Estados Unidos que inició algunas de las investigaciones y desarrollos de Internet.

NSFNET (National Science Foundation NETwork)

Se utiliza para descubrir la red de columna vertebral en Estados Unidos, que es administrada por la NSF.

P POP. Protocolo de Oficina de Correos (Post Office Protocol)

Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita la entrega de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta. Los mensajes enviados a la aplicación cliente son inmediatamente eliminados del servidor, sin embargo las aplicaciones modernas pueden omitir este paso.

PPP (Point to Point Protocol)

Protocolo utilizado para enmarcar al IP cuando se envía a través de una línea serial. Vea también SLIP.

PROTOCOL (protocolo)

Descripción formal de formatos de mensajes y reglas que dos o más máquinas deben seguir para intercambiar mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de máquina a máquina (por ejemplo, el orden en el que los bits de un octeto se envían a través de un cable) o del intercambio entre programas de aplicación (por ejemplo, la forma en que un programa transfiere un archivo a través de una red de redes). La mayor parte de los protocolos incluye descripciones intuitivas de las interacciones esperadas así como especificaciones más formales, utilizando modelos de máquinas de estado finito.

PUENTE. (bridge).

Los puentes son dispositivos que tienen usos definidos. Primero, pueden interconectar segmentos de red a través de medios físicos diferentes; por ejemplo, no es poco común ver puentes entre cable coaxial y de fibra óptica. Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI)

R RDSI (Red Digital de Servicios Integrados) vea ISND

REPEATER (repetidor)

Dispositivo de hardware que extiende las LAN. Un repetidor copia señales eléctricas de una red física a otra. No son muy populares.

RIP (Routing Información Protocol)

Protocolo utilizado para difundir información de ruteo dentro de un sistema autónomo. El RIP deriva de un protocolo del mismo nombre desarrollado originalmente por Xerox

S SCRIPT.

Secuencia de comandos que se le dan a un módem. Esta secuencia puede ser por ejemplo para asignar una configuración al módem (velocidad, compresión de datos, etc.) o para realizar tareas específicas (llamar al proveedor, colgar, etc.). A veces es necesario modificar un Script o cadena de inicio que le establece al

módem las condiciones iniciales (por ejemplo cambiar ATDT que establece una línea telefónica por tonos a ATDP que indica una línea telefónica por pulsos, etc.)

SLIP (Serial Line Internet Protocol)

Es una implementación de TCP/IP por líneas seriales. Para conectar un módem a Internet es necesario establecer un protocolo SLIP o PPP En el caso de RED UNAM la conexión se realiza por SLIP y por un programa que realiza la conexión y establece los sockets o canales de comunicación de las aplicaciones, de esta manera se permite la transferencia de paquetes a la computadora local

Vea PPP.

SMTP (Simple Mail Transfer Protocol)

Protocolo estándar del TCP/IP para transferir mensajes de correo electrónico de una máquina a otra. SMTP especifica cómo interactúan dos sistemas de correo y el formato de los mensajes de control que intercambian para transferir el correo.

SPANNING TREE

Técnica que detecta un enlace dentro de una red y redunda en las rutas de los bloques lógicos, asegurando que exista una ruta única entre dos conexiones de LANs, se utiliza en una red puenteada IEEE 802.1

SNMP (Simple Network Management Protocol)

Protocolo estándar utilizado para monitorear anfitriones, ruteadores y las redes a las que están conectados. La segunda versión del protocolo se conoce como SNMPv2.

Vea también MIB

SSL Capa de conexiones Seguras. (Secure Sockets Layer)

Utiliza una llave de 40 bits para encriptar la información proporcionada de manera confidencial, ya sea a un proveedor, una base de datos, etc.

TCP (Transmisión Control Protocol)

Protocolo de control de transmisiones corresponde a la capa 4 del modelo OSI y ofrece una transmisión confiable de datos.

TOKEN PASSING (Paso de ficha).

Protocolo que se utiliza en redes Arcnet y Token Ring, y que se basa en un esquema libre de colisiones, dado que la señal (token) se pasa de un nodo o estación al siguiente nodo. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un sólo paquete viajará a la vez en la red. TOKEN RING. Red local desarrollada por IBM que utiliza el protocolo de acceso Token Passing y que utiliza un ancho de banda de 4 y 16 Mbps. Utiliza la topología de anillo.

THROUGHPUT

Producción. trabajo útil. Cantidad de información que llega, y que posiblemente pasa, a un punto en particular en un sistema de red.

UDP (User Datagram Protocol)

Protocolo estándar TCP/IP que permite a un programa de aplicación en una máquina enviar un datagrama hacia el programa de aplicación en otra máquina. El UDP utiliza el protocolo de Internet (IP) para entregar datagramas. Conceptualmente la diferencia importante entre los datagramas UDP y los IP es que el UDP incluye un número de puerto de protocolo, lo que permite al emisor distinguir entre varios programas de aplicación en una máquina remota dada. En la práctica el UDP también incluye una suma de verificación opcional en el datagrama que se está enviando.

VIRUS.

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente

b) Tratar de pasar desapercibidos para causar el mayor daño posible

c) Adueñarse de las funciones principales (infectar los archivos de sistema).

El CERT es un organismo que proporciona soporte a los administradores de sistemas en situaciones semejantes

X.25

Recomendación CCITT que define el formato de los paquetes para transferencias de datos en redes públicas. Muchos corporativos poseen redes X.25 que les dan acceso a terminales remotas. Esas redes se pueden usar para otro tipo de datos incluyendo los protocolos de Internet, DECnet y XNS

Fuentes

Seminario de conectividad avanzada, versión 4.2 Intersys de México, S.A. de C.V.

Glosario de Términos y Recursos de Internet, por Alma Elida García Meza y Israel Ortega Cuevas;

e-mail:alma@vegetarians.com

Glosario de Términos de Teleprocesamiento y Redes Por Dr. Eduardo Rivera Porto

e-mail:erporto@ns.inter edu

http://msip.lce.org/erporto/indice.htm