UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ADMINISTRACIÓN AVANZADA DE UNA RED EMPRESARIAL

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

ALEJANDRA MA. ELENA DOMÍNGUEZ CASILLAS

MA. GUADALUPE HERNÁNDEZ LOAIZA

JOSÉ TRINIDAD GUTIÉRREZ VÁZQUEZ

JUAN MANUEL TORRES GUTIÉRREZ

Director de Tésis: **Ing. Gloria Mata Hernández**

CIUDAD UNIVERSITARIA **1998.**

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería por la formación académica que nos brindaron.

A los profesores que durante y fuera de clases, nos compartieron sus conocimientos y experiencias.

Y a todas y cada una de aquellas personas que de alguna forma nos brindaron su apoyo, su entusiasmo y su confianza.

Gracias

AGRADECIMIENTOS

A DIOS, por la vida y todas las bendiciones y muestras de amor que recibo de Él cada día.

A TI PAPITO, por ser mi apoyo y ejemplo, gracias por tu amor, entrega y dedicación. Te amo.

A CLAU, LAURITA y CHECO, que a pesar de todo, están siempre conmigo y dispuestos a demostrarme su cariño. Los quiero.

A TERE, LUCY y DANY, por tantos momentos de alegría que me han regalado.

A MI MAMÁ, por haberme dado la vida y por animarme a seguir siempre adelante. Te quiero.

A TODOS MIS AMIGOS, por ser parte de mi vida y ayudarme A construir mi historia. Gracias

Con Cariño

ALE

AGRADECIMIENTOS

A mis Padres, VICTOR MANUEL y CARMEN, porque me han brindado con su apoyo y confianza la oportunidad de ser alguien en la vida, de madurar y crecer como hombre en un camino lleno de obstáculos y dificultades, y porque nunca perdieron la esperanza de verme realizado como profesionista.

A mis hermanos FRIDA, EDITH, VICTOR HUGO, FABIOLA e IVONNE, por que siempre me han impulsado en todo, dandome su cariño y comprensión.

A mis amigos, por haberme escuchado cuando atravesé por buenos y malos momentos, y a todas las personas que nunca han dejado de creer en mí.

A todos ustedes .. Gracias

Juan Manuel Torres Gutiérrez

AGRADECIMIENTOS

Gracias a mis padres, por el impulso que siempre me dieron para seguir adelante y no ceder en los momentos difíciles que tuve que afrontar, por el esfuerzo que hicieron conmigo y la confianza que tuvieron en mí para cumplir la meta de terminar una carrera universitaria.

Gracias por todo

José Trinidad Gutiérrez Vázquez

ÍNDICE

	Prólogo	1
1.	**Introducción**	5
2.	**Redes de Computadoras**	10
	2.1. Modelo OSI	11
	2.1.1. Capas del Modelo OSI	14
	2.2. *Consideraciones de Diseño*	29
	2.3. Protocolos	39
	2.3.1. Funciones de un protocolo de comunicaciones	41
	2.3.2. Clasificación de protocolos	45
	2.3.3. Relación de los protocolos con el modelo OSI	48
3.	**Administración Avanzada de Redes de Computadoras**	69
	3.1. Administración de redes	70
	3.1.1. Esquema general de la administración	71
	3.1.2. Funcionamiento de la red	74
	3.1.3. Mantenimiento de la red	75
	3.1.4. Herramientas administrativas de mantenimiento y desempeño	77
	3.1.5. Planificación	78
	3.1.6. Seguridad en la red	80
	3.1.7. Administración de una red en perspectiva	81
	3.2. Distribución de Software	82
	3.3. Control de Inventarios	85
	3.3.1 Software	85
	3.3.2 Hardware	87
	3.4. Respaldo y recuperación	90
	3.4.1. Almacenamiento en red	98

3.5. Seguridad 108
3.5.1. Tipos de Seguridad 111
3.5.2. Mecanismos de Seguridad 115
3.5.3. Seguridad en los servicios 117
3.6. Monitoreo de la Red 123
3.6.1. Monitoreo de dispositivos y conexiones 124
3.6.2. Monitoreo de Eventos 128
3.6.3. Detección de Fallas 129
3.6.4. Línea de Monitoreo de la Red 129
3.6.5. Software para la administración y el monitoreo de la red 130

4. Infraestructura de Administración Avanzada 133
4 1. Organización 133
4.1.1. Nivel empresarial 134
4 1.2. Nivel de las Direcciones Generales 138
4.1.3. Nivel de las Gerencias Regionales 141
4.1 4. Cableado estructurado 142
4.2. Metodología de trabajo 155
4.3. Recursos Humanos 159
4.3 1. Recursos Humanos en la Red 161
4.4. Capacitación 163
4.5. Hardware y Software 167
4.5.1. Repetidores 168
4.5.2. Concentradores 170
4.5.3. Puentes 172
4.5.4. Ruteadores 175
4.5.5. Brouter 176
4.5.6. Compuertas 177
4.5.7. Interruptor 178
4.5.8. Sistema operativo de red 179

5. **Conclusiones** 181

Anexos

Anexo 1. Servicios de red 183

Anexo 2. Matriz de costos 187

Glosario 191

Bibliografía 213

PRÓLOGO

PRÓLOGO

El presente trabajo de tesis, tiene como objetivo mostrar los elementos de infraestructura requeridos en la administración avanzada de redes de computadoras, relacionados con el sistema adecuado de comunicaciones entre las diferentes redes.

Para lograr lo anterior, debemos tener en cuenta que un centro de administración de redes y sistemas, es una integración de herramientas de hardware y software y de un conjunto de procedimientos y/o tareas que tienen como función principal, auxiliar a todo el personal para resolver cualquier tipo de problema que se presente y dado que se contempla la infraestructura de vanguardia, la hemos denominado administración avanzada.

Así mismo, tampoco hay que olvidar que otro elemento importante para lograr una adecuada administración de redes, es el factor humano, ya que se podrán tener los equipos de comunicación de redes más modernos y el software de administración más eficiente, pero si no se cuenta con el personal actualizado en la administración de redes de cómputo, no se obtendrá el máximo rendimiento de las herramientas mencionadas.

Por lo tanto, este trabajo de tesis es una guía para todos los operadores de redes, que tienen como objetivo lograr una adecuada administración de su red, ya que aún cuando existe mucha información sobre redes de computadoras, ésta se encuentra dispersa en una gran cantidad de obras y no existe una literatura que contemple de forma general, conjunta y concreta todos los aspectos de la administración avanzada de redes, por lo tanto se espera que este trabajo sea de gran utilidad y que permita el uso más eficiente de una red, así como una valiosa herramienta de introducción para aquellas personas que están interesadas en iniciarse en el extraordinario mundo de las redes de computadoras.

Este trabajo se ha desarrollado en capítulos y apéndices. En el primer capítulo

"Introducción", se describe brevemente la historia del surgimiento de las redes, su desarrollo a través del tiempo y los hechos que han marcado su evolución, concluyendo con una explicación de su situación actual, con lo cual se pretende lograr que el lector pueda tener un panorama general de las redes de computadoras y la importancia que éstas han tenido en el desarrollo de las comunicaciones.

En el segundo capítulo titulado "Redes de Computadoras" se presentan aspectos más específicos de las redes de computadoras y las diferentes consideraciones que se deben realizar al momento de planear e instalar una red, comenzando con una descripción del modelo más comúnmente utilizado para la interconexión de sistemas abiertos, conocido como modelo OSI, el cual describe la forma en que se deben interconectar los equipos de comunicación de redes, con el fin de que los equipos fabricados por diferentes proveedores puedan ser compatibles entre sí.

También describimos el análisis preliminar que todo administrador de redes debe realizar para poder instalar una red, determinando las necesidades de los usuarios, las diversas topologías de redes existentes, la velocidad de transmisión requerida, etc., concluyendo con una definición y clasificación de los protocolos de comunicaciones y el papel que desempeñan dentro de la red, así como una descripción de aquellos que son más comúnmente utilizados y la relación que tienen con el modelo de interconexión de sistemas abiertos (OSI).

En el tercer capítulo "Administración Avanzada de Redes de Computadoras", se mencionan las funciones principales de la administración de redes y de todos aquellos elementos necesarios para una eficiente administración avanzada de redes de computadoras, como son:

- Las consideraciones que se deben tener para una adecuada distribución de software y control de inventarios.

- Los medios que existen y las diversas técnicas que se utilizan en el respaldo y

recuperación de información en una red de computadoras.

- La seguridad, tanto de la red como de los diferentes servicios que ésta ofrece, siendo esto un aspecto fundamental para la adecuada operación de una red.

Terminando con un estudio de cómo debe realizarse un adecuado monitoreo de la *red y de algunos programas para el monitoreo de redes.*

En el cuarto capítulo, presentamos la infraestructura de administración avanzada de redes de computadoras, comenzando por describir la organización de una red empresarial típica, planteando la posible evolución de este tipo de redes, a redes con cableado estructurado con capacidad para transmitir voz, datos y video, logrando establecer una red empresarial de mayor capacidad, preparada para los futuros requerimientos de aplicaciones multimedia y videoconferencia.

Se analiza también, la importancia que tienen los recursos humanos dentro de la infraestructura de administración avanzada y el perfil que deben reunir todos aquellos que se encuentren encargados de llevar a cabo la función de administrador de redes, considerando después el aspecto de la capacitación como un proceso de actualización continua que se debe dar y deben tener dichos administradores. Por último, se presenta un estudio de todos los equipos de comunicaciones que son requeridos para la instalación y puesta en operación de una red, lo cual brinda al lector la posibilidad de tener un panorama completo de cómo se puede conformar una red de gran tamaño, concluyendo con la función que desempeña el sistema operativo de red.

Adicionalmente se presenta un glosario de términos, ya que aún cuando se trató de traducir todas las palabras de uso común en las redes del idioma inglés al español, en algunos casos no fue posible encontrar traducción por lo cual en el glosario se puede encontrar una descripción de dichos términos.

Se cuenta también con dos Anexos, en los cuales se presentan con más detalle las consideraciones que se deben tener en las redes de computadoras, como son: el alcance de los servicios ofrecidos por una red, así como el desarrollo y las consideraciones que se deben de realizar para elaborar una matriz de costos, permitiendo con esto dar a conocer aspectos que en ocasiones no se encuentran en otras obras.

Esperamos que este trabajo sea de gran utilidad para aquellas personas que se encuentren trabajando con redes de computadoras o sean administradores de red y que no han tenido a su alcance una obra que los ayude a lograr una administración adecuada de su red, o aquellas que por alguna razón tengan la necesidad de trabajar en una red de cómputo y que les interese conocer de manera clara y sencilla cómo funciona la misma.

CAPÍTULO 1

INTRODUCCIÓN

1. INTRODUCCIÓN

En un principio las redes de datos surgieron como soluciones a necesidades estratégicas del conjunto limitado de organizaciones que poseían varias computadoras que requerían interconectarse, con el objetivo fundamental de compartir recursos, es decir, permitir al usuario de cualquier terminal dentro de la organización, acceder y utilizar todos los servicios y recursos disponibles. Podemos decir entonces, que una Red es el conjunto de cierto número de terminales que intercambian información.

Las primeras redes de computadoras de gran escala fueron los sistemas de reservación de aerolíneas, a principios de los años 60's. El Sistema SABRE de American Airlines, por ejemplo fue construido en 1961. Posteriormente surgieron proyectos como ARPANET y TYMNET a finales de la década de los 60's y CYCLADES a principios de los 70's, que marcaron el gran interés de la comunidad en las telecomunicaciones, por encontrar soluciones que permitieran interconectar máquinas situadas a distancia, en condiciones técnica y económicamente favorables.

En el camino recorrido puede observarse un inicio más bien caótico, en el que no existían normas de compatibilidad, hasta llegar a una convergencia entre la computación y las comunicaciones en donde se propone un sólo tipo de redes de transmisión y donde existe un consenso en el uso de normas que garanticen la independencia entre el usuario y el prestador de servicios.

El ofrecimiento de servicios de comunicación bajo condiciones óptimas de acceso y costo, hacen necesario tomar en cuenta varios factores que pueden ser causa de conflictos durante la integración de un sistema de telecomunicaciones:

- La compatibilidad entre terminales o máquinas, procedentes de distintos fabricantes.

- La independencia de los servicios remotos y la red de interconexión.

- Las restricciones impuestas sobre los servicios ofrecidos cuando las funciones que los soportan son modificadas.

La primera ruptura con los sistemas tradicionales y su jerarquía comenzó a principios de los 70's, cuando algunas minicomputadoras comenzaron a sustituir a los grandes sistemas en algunos sectores del mercado.

La aparición de la computadora personal IBM, a principios de los 80's, supuso que se establecería un nuevo estándar tanto para el uso personal como profesional de las computadoras. A medida que se incrementaba el grupo de usuarios de computadoras, empezó a hacerse evidente que si se lograba conectarlas se obtendrían grandes beneficios, como el compartir las impresoras o los discos fijos.

A medida que las computadoras personales se iban haciendo más poderosas con el uso de procesadores más avanzados y de software más sofisticado, los usuarios de los sistemas basados en grandes computadoras (mainframes) y minicomputadoras comenzaron a romper con sus costumbres.

De acuerdo con sus características de explotación, hay redes privadas de terminales, redes de computadoras y redes públicas para servicio de transmisión de datos. Una red debe de tener como fin una serie de servicios. Las redes de computadoras, locales o de larga distancia, surgieron para hacer posible el compartir de forma eficiente los recursos informáticos (hardware, software y datos) de los usuarios. Se dice entonces que una red es a la vez software y hardware. El hardware está compuesto por los cables e interfaces que conectan entre sí a las computadoras personales y los periféricos. El software controla los archivos y el sistema de comunicaciones.

Las redes están estructuradas fundamentalmente en estrella o en malla; las primeras

convergen en un centro único, en tanto que las últimas tienen una serie de puntos de enlace, los cuales pueden ser iguales o de distintas características (tamaño, importancia de funciones, etc.), pero que tienen en común la posibilidad de optar entre varias alternativas al establecimiento de la conmutación.

En los entornos con grandes computadoras y minicomputadoras, el procesamiento y la memoria se encuentran centralizados. La computadora central se convierte en el núcleo de la organización de proceso de datos, habiendo un equipo de profesionales que tienen como única tarea el trabajar y administrar el sistema. Las terminales conectadas al ordenador central permiten que otros usuarios puedan compartir las posibilidades de cálculo y la memoria de la computadora central.

El servidor de archivos o sistema central se convierte en un lugar para almacenar los archivos y gestionar la red, además de ser el lugar al que se conectan las impresoras y otros recursos compartidos. Las minicomputadoras y grandes computadoras pueden usarse así para ejecutar los procesos más pesados, tales como los cálculos o procesos más intensivos, mientras se distribuyen tareas entre las PC's individuales. La definición más clara de una red es la de un sistema de comunicaciones que permite comunicar a los usuarios y compartir archivos y periféricos.

En su estado actual, las redes de computadoras se han desarrollado lo suficiente para soportar la interconexión de los equipos más heterogéneos. Sin embargo, en ocasiones resulta complicado lograr la compatibilidad entre máquinas que no fueron diseñadas pensando en el intercambio de datos. En contraste, un aparato telefónico de cualquier marca siempre ha podido conectarse a la interfaz para comunicarse por una red que garantiza el acceso a sus servicios cuando se cumplen ciertos requerimientos de normalización.

Con los diferentes fabricantes de computadoras y proveedores de servicios de telecomunicaciones, existe una clara necesidad de asegurar la compatibilidad a nivel

mundial para garantizar a los usuarios de cualquier origen, la conexión con cualquier destino, sin importar la marca de sus equipos o la compañía que presta el servicio.

De acuerdo a lo anterior, un centro de administración de redes y sistemas, es una integración de herramientas de software y hardware, además de personal altamente calificado para aplicar un conjunto de procedimientos y/o tareas que tienen como función principal, auxiliar a resolver cualquier tipo de problema que se presente, para dar una solución de una manera ordenada y secuencial y cumplir con el objetivo de un Centro de Administración de Redes y Sistemas, que es el de proporcionar el mejor servicio en forma integra y centralizada, para las cinco tareas de la administración de redes y sistemas que son:

Administración de Fallas

Es el proceso de aislar y resolver las fallas en la red. Muchos sistemas de administración de redes resuelven esta tarea proporcionando mapas de redes con códigos de color. Generalmente también ofrecen alarmas que son iniciadas por ciertos eventos. Estas alarmas pueden ser audibles, cambiar colores en los mapas o vocear a alguien en forma remota. Aunque las fallas son visibles después de que ocurren, la meta de la administración de redes es aislar y prevenir las fallas antes de que ocurran con la utilización de herramientas de planeación y optimización.

Administración del Rendimiento

Es el proceso de medir y optimizar el rendimiento en el tiempo, recolectando estadísticas acerca del tráfico de la información, efectuando análisis de tendencias y usando después la información para asignar recursos de acuerdo a ésta. Esto también puede llamarse Planeación de la Capacidad.

Administración de la Configuración

Este es el proceso de entender y administrar la configuración de la red en el tiempo. Esto incluye tener un inventario exacto de los dispositivos de la red, incluyendo su ubicación, dirección, identificadores e información de contactos; y tener un mapa que

ilustre la conexión física entre los dispositivos. Esto se conoce como *Topología*.

Debido a que las redes y las configuraciones cambian con el tiempo, la administración efectiva requiere un conocimiento actualizado de la configuración de la red. Para este fin, los mejores sistemas de administración de redes incluyen características como el "autodescubrimiento", que crea automáticamente una lista de los dispositivos de la red; y "autotopología", que toma esta información y forma un mapa de la red.

Administración de la Seguridad

Es el proceso de asegurar la red contra usuarios no deseados. La protección de la red se vuelve más importante conforme la información confidencial se hace disponible en la red. La protección puede ser tan simple como una clave de seguridad, pero puede incluir esquemas más robustos para asegurar el control del acceso y que sólo el personal autorizado pueda acceder la red.

Administración Contable

Esta monitorea la utilización de los recursos de la red en el tiempo Esto incluye el uso que hace un usuario, un departamento, protocolos *específicos ó una aplicación*. La administración contable ayuda al administrador de la red a entender quién está usando más la red mientras proporciona un medio para efectuar los cargos correspondientes o suministra reportes administrativos que muestren los costos y usos de la red.

Si se administra de una manera eficiente a las redes y a los sistemas se puede eliminar o reducir grandemente la falta de disponibilidad del servicio y garantizar que los recursos se estén utilizando adecuada y óptimamente.

CAPÍTULO 2

REDES DE COMPUTADORAS

2 REDES DE COMPUTADORAS

Las redes están compuestas por muchos elementos diferentes (Software y Hardware) que deben trabajar conjuntamente para crear una red funcional. Los componentes que comprenden las partes de hardware de la red incluyen entre otros: tarjetas, adaptadores de red, cables, conectores, concentradores y hasta la computadora misma. También se requiere software especial de red para que el sistema operativo existente y los programas de aplicación de la computadora se puedan comunicar con otras computadoras en la red.

Se han creado estándares que definen la forma de conectar componentes de hardware en las redes y él o los protocolos de uso cuando se establecen comunicaciones por red.

La mayoría de las redes se organizan en una serie de capas o niveles, con objeto de reducir la complejidad de su diseño. El número de capas que la componen, el nombre de cada capa, su contenido y función, varían dependiendo del diseño de cada red.

El modelo más comúnmente utilizado para la interconexión de sistemas abiertos es el desarrollado por la Organización Internacional de Estándares (ISO), conocido como modelo OSI.

2.1 MODELO OSI

En 1977, la ISO International Standard Organization (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 ello lograr la interoperabilidad entre sistemas heterogéneos. Ya 1978 la (ISO) propuso un modelo para comunicaciones de Redes Locales al que titularon The Reference Model of Open Systems Interconnection (OSI, Modelo de Referencia de Interconexión de Sistemas Abiertos). "**Interconexión de Sistemas Abiertos**" significa el intercambio de información entre terminales, microcomputadoras, redes y procesos.

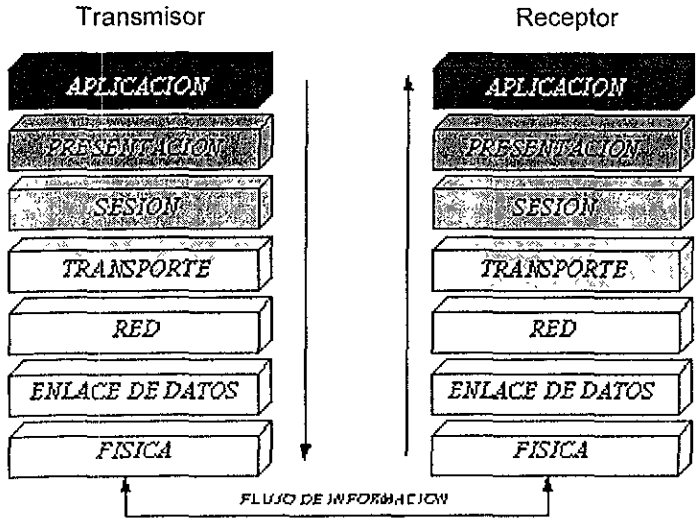
El modelo OSI-Open System Interconection (Interconexión de Sistemas Abiertos) sirve como una guía o una serie de lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos, no especifica en si un estándar de comunicación, sin embargo, muchos estándares y protocolos cumplen con lo que establece el modelo.

Dada la complejidad de los dispositivos de conexión en red y su integración para que operen adecuadamente, el modelo OSI se divide en 7 partes o capas, cada una de las cuales se destinada a una tarea específica.

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

El modelo OSI se fragmenta en siete capas, en donde cada capa ha sido asignada a tareas y responsabilidades específicas. Cada capa se comunica con su similar enviando o recibiendo recursos y es funcionalmente independiente de las capas adyacentes.

El modelo OSI está formado de las siguientes capas:



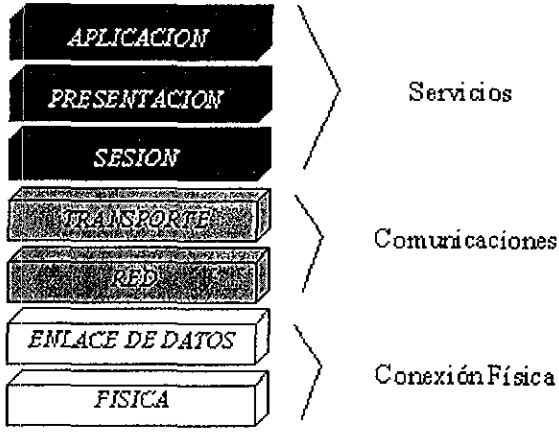
Esquema del modelo OSI

Capa	Unidad de Información	Analogía con la Comunicación Humana
7. Aplicación	Mensaje	Conversación
6. Presentación	Mensaje	Diálogo
5. Sesión	Mensaje	Párrafo
4. Transporte	Datagrama	Oración
3. Red	Paquete	Frase
2. Enlace de Datos	Frame	Palabras
1. Física	Bits	Letras

Analogía del modelo OSI con la forma de comunicación del hombre

El modelo OSI no es tangible, sólo especifica que tareas deben llevarse a cabo en cada capa; más no dice cómo se deben de realizar.

Las capas del modelo OSI se agrupan en tres categorías funcionales como se muestra a continuación:



Categorías funcionales del modelo OSI

- **Conexiones Físicas,** (capas 1 y 2). Estas capas proveen la conexión física a la Red para las capas superiores (capa 3 a 7) y son responsables de mover datos sobre los medios de comunicación de la Red.

- **Comunicaciones,** (capas 3 y 4). Ambas capas son responsables de asegurar que los datos transmitidos lleguen seguros desde el dispositivo transmisor hasta el *dispositivo receptor, son independientes de los medio físico.*

- **Servicios,** (capas 5,6 y 7). Estas capas proveen servicios de Red a los usuarios. Algunos servicios son E-Mail, servicios de compartir archivos e impresión,

emulación de terminal, validación de login y otras.

El modelo OSI fue creado para hacer posible "la definición de procedimientos estandarizados que permitan la interconexión y el subsiguiente intercambio efectivo de información entre usuarios", en donde el término "usuarios" se refiere a sistemas que constan de una o más computadoras, software asociado, periféricos, terminales, operadores humanos, procesos físicos, mecanismos de transferencia de información y elementos relacionados. Estos elementos juntos, deben poder "Realizar procesamiento y/o transferencia de información". Los estándares desarrollados a partir del modelo de referencia permitirán a diversas redes del mismo tipo o diferentes comunicarse fácilmente entre sí, como si constituyeran una misma red.

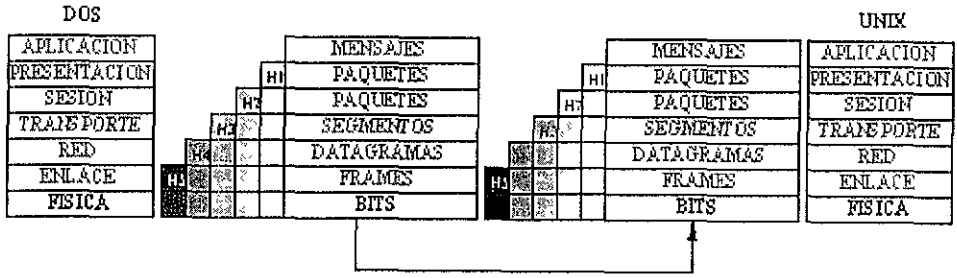
2.1.1 Capas del Modelo OSI

Capa 7	APLICACION
Capa 6	PRESENTACION
Capa 5	SESION
Capa 4	TRANSPORTE
Capa 3	RED
Capa 2	ENLACE DE DATOS
Capa 1	FISICO

Capa Física

La Capa Física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su diseño debe asegurar que cuando un extremo envía un bit con valor 1, éste se reciba exactamente como un bit de ese valor en el otro extremo, y no como un bit de valor 0. Preguntas comunes aquí son cuántos volts deberán utilizarse para representar un bit de valor 1 ó 0; cuantos microsegundos deberá durar un bit; la posibilidad de realizar transmisiones bidireccionales en forma simultánea; la forma de

establecer la conexión inicial y cómo interrumpirla cuando ambos extremos terminan su comunicación; o bien, cuántas puntas terminales tiene el conector de la red y cuál es el uso de cada una de ellas. Los problemas de diseño a considerar son los aspectos mecánico, eléctrico, de procedimiento de interface y el medio de transmisión física, que se encuentra bajo la capa física. Se puede considerar que el diseño de la capa física cae dentro del dominio del ingeniero electrónico.



Capa física del modelo OSI

La Capa Física del Modelo OSI coordina las reglas para la transmisión de bits. Esta capa define:

- Estructuras Físicas de la Red.
- Especificaciones Mecánicas y Eléctricas para utilizar el medio de transmisión (cables).
- Las reglas para la transmisión del bit.

El hardware de conectividad normalmente asociado con la capa Física es:

- Concentradores y Repetidores, los cuales regeneran las señales eléctricas.
- Conectores de los medios de transmisión, los cuales proporcionan la interface mecánica para interconectar los dispositivos al medio de transmisión.
- Módem y codificadores, los cuales realizan la conversión de la señal a digital o

analógica.

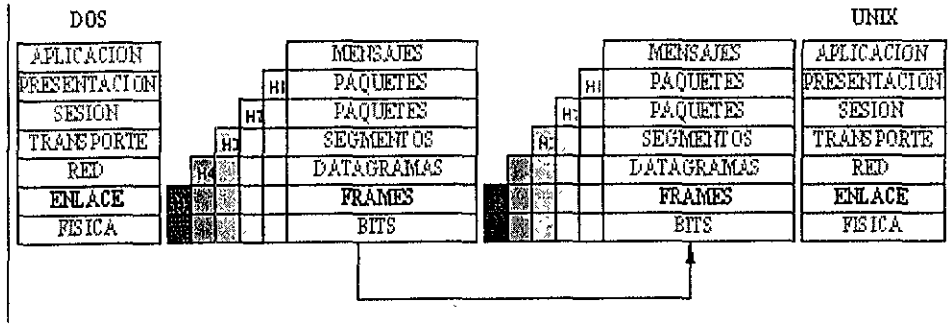
Algunos de los estándares que comprenden esta capa son:

- Cables Ethernet 802.3 (Cable para Ethernet denso, cable para Ethernet estrecho, cable Ethernet UTP).
- El estándar FDDI (Interfaz de datos distribuidos por fibra óptica).

Capa de Enlace

Las funciones básicas de la capa de enlace son:

- Organizar los bits de la capa física (1's y 0's) dentro de los grupos lógicos de información llamados frames (como un byte, un frame es una serie continua de bits agrupados juntos como una unidad de datos).
- Detectar errores cometidos al transmitir datos por el cable de red.
- Controlar del flujo de datos.
- Identificar computadoras en la Red.



Capa de enlace de datos del modelo OSI

Como muchas otras capas, la capa de enlace agrega su propia información de control al frente del paquete de datos. Esta información puede incluir una fuente y una dirección destino (físico o hardware) y una indicación de los protocolos de las capas superiores.

Los siguientes dispositivos de conectividad de red están comúnmente asociados con la capa de enlace:

- Tarjetas de Red.
- Concentradores inteligentes.
- Puentes.

Las funciones de la capa de enlace normalmente se dividen en las siguientes dos subcapas:

- **Control de acceso al medio (MAC).** Controla la forma en que los transmisores comparten un canal de comunicación. Existen protocolos de control de acceso al medio como los siguientes:

  - Carrier Sense, Multiple Access/Collision Detection (CSMA/CD).
  - Carrier Sense, Multiple Access/Collision Avoidance (CSMA/CA).
  - Token-passing.

- **Control de enlace lógico (LLC).** Establece y mantiene el enlace para transmitir frames de datos de un dispositivo al siguiente. Los servicios de la capa de enlace LLC tiene las siguientes funciones:

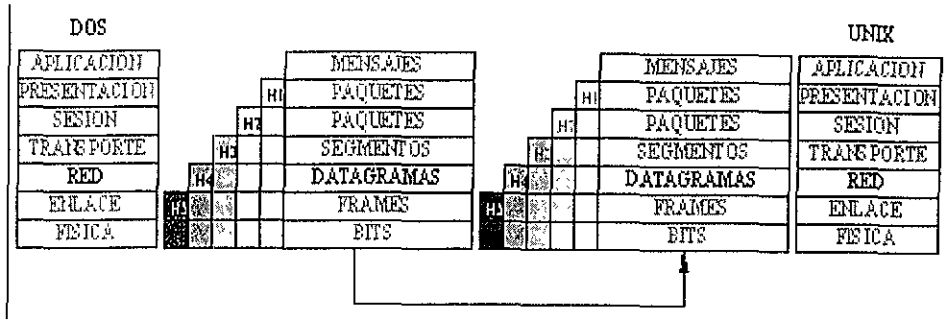
  - Controlar la cantidad de datos transferidos de una computadora a la siguiente (que ayude a prevenir la perdida de datos).
  - Detectar errores de transmisión y retransmitir requerimientos.

Los estándares basados en la capa de enlace de datos incluyen:

- El estándar de enlace lógico 802.2 de la IEEE, punto a punto.
- Los estándares 802.3.
- El estándar Token Ring.
- El estándar ANSI FDDI-Token Ring sobre fibra.

Capa de Red

El objetivo principal de la capa de Red es mover datos a localidades de red especificas. La capa de red describe los métodos para mover información entre múltiples redes independientes (y otras similares), llamadas inter-redes (internetworks).



Capa de red del modelo OSI

La capa de enlace direcciona datos a todos los dispositivos conectados a una red sencilla. La capa de red puede escoger una ruta especifica a través de una inter-red y evitar enviar datos a redes no involucradas. La capa de red hace este switcheo a través del direccionamiento de la capa de red y algoritmos de ruteo. También es responsable de asegurar las rutas correctas de datos a través de una inter-red o redes similares.

Los conceptos de la capa de red se aplican principalmente para:

- Separar lógicamente redes, las cuales deberán tener una dirección única de red.
- Establecer Switcheo, el cual determina como se pueden realizar las conexiones en la inter-red.

La red trabajara con diferentes niveles de servicios de conexión, dependiendo del número de errores esperados en la inter-red.

Las siguientes dos elementos ayudan a direccionar redes y servicios:

- **Dirección de Red Lógica.** Para liberar datos en una inter-red, se debe usar una dirección de red lógica, que es el identificador usado para distinguir lógicamente dos diferentes redes en una inter-red. El dispositivo físico y las direcciones de red lógicas son usadas para mover datos entre dispositivos de una red.

- **Dirección de Servicios.** Cada computadora o dispositivo de red puede desempeñar varias funciones simultáneamente. Cada entidad (hardware o software) debe tener su propia dirección que pueda mandar y recibir datos. Esta dirección puede ser llamada Dirección de Servicio (también es llamada puerto o socket para un protocolo específico). Un servicio de direcciones identifica y especifica un protocolo o proceso de una capa superior. Un servicio de dirección múltiple puede ser asignado a cualquier computadora en que corran varias aplicaciones de red.

El Switcheo

Las inter-redes pueden tener múltiples trayectorias para unir dispositivos emisores con posibles dispositivos receptores. La información puede ser switcheada como si viajara en varios canales de comunicación. Existen diversas técnicas de switcheo de datos:

- **Switcheo de Circuitos.** El switcheo de circuitos es una técnica que conecta al transmisor y al receptor mediante una trayectoria por el tiempo que dure la conversación. Una vez que la conexión es establecida con este tipo de técnica de switcheo, una trayectoria dedicada existe entre ambos finales hasta que la conexión finaliza.

- **Switcheo de Mensajes.** El switcheo de mensajes no establece un trayectoria dedicada entre dos estaciones para una entidad de conversación. Las conversaciones son divididas en mensajes. Cada mensaje es empaquetado con su propia dirección de destino y después transmitido de dispositivo a dispositivo a través de la Red. Los dispositivos intermedios reciben el mensaje, lo almacenan y lo transmiten al siguiente dispositivo. Este tipo de redes es algunas veces llamada strore-and-forward network. El dispositivo de switcheo de mensajes comúnmente es una computadora de propósito general. La cual necesita capacidad de almacenamiento suficiente para almacenar temporalmente mensajes.

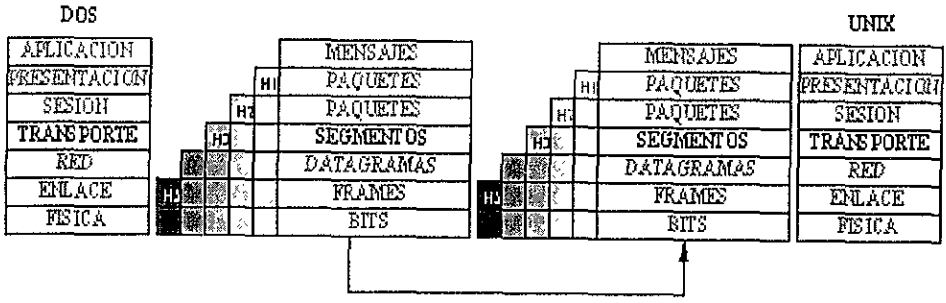
- **Switcheo de Paquetes.** El switcheo de paquetes es una opción que combina las ventajas del switcheo de circuitos y mensajes minimizando las desventajas de ambos. Existen dos métodos de switcheo de paquetes:

  - Switcheo de datagrama de paquetes.
  - Switcheo de paquetes de circuito virtual.

En ambos métodos de switcheo de paquetes, los mensajes son fragmentados en pequeñas partes, llamadas paquetes. Cada paquete es etiquetado por su origen, destino y dirección de nodos intermedios apropiados. Los paquetes tienen una longitud máxima estrictamente definida y pueden ser almacenados en RAM.

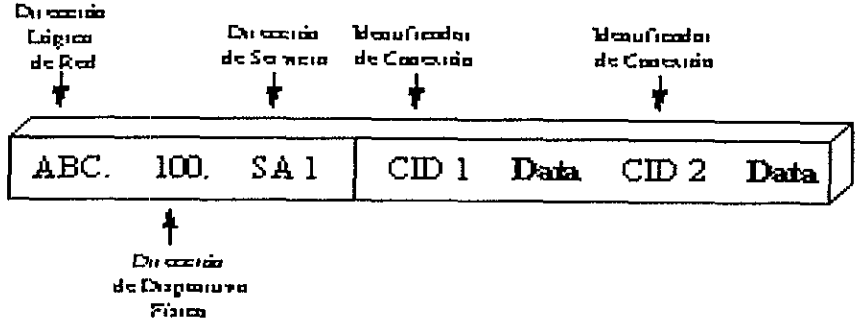
Capa de Transporte

La capa de transporte está diseñada para esconder las complejidades de la estructura desde las capas superiores.



Capa de transporte del modelo OSI

La función principal de la Capa de Transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, llamadas segmentos, como se muestra en la siguiente figura, y pasarlos a la capa de red asegurando que todos ellos lleguen correctamente al otro extremo. Además, todo este trabajo se debe hacer de manera eficiente, de tal forma que aísle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.



Esquema de como se van agregando los mensajes

Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones de la red con objeto de mejorar dicho caudal. Por otra parte, si la creación o mantenimiento de la conexión de una red resulta costosa, la capa de transporte podría multiplexar varias conexiones de transporte sobre la misma conexión de red para reducir dicho costo. En todos los casos, la capa de transporte se necesita para hacer el trabajo de multiplexión transparente a la capa de sesión.

La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red. El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes en el mismo orden en que fueron enviados. Sin embargo, el transporte de mensajes aislados sin garantizar el orden de distribución y la difusión de mensajes a distintos múltiples es otra posibilidad de servicio de transporte. El tipo de servicio se determina cuando se establece la conexión.

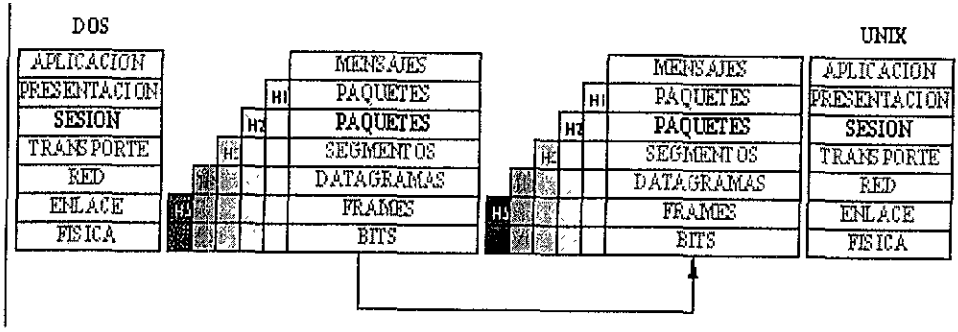
La capa de transporte es una capa de tipo origen-destino o extremo a extremo. Es decir, un programa en la máquina origen lleva una conversación con un programa parecido que se encuentra en la máquina destino, utilizando los encabezados de los mensajes y los mensajes de control.

Además de multiplexar varios flujos de mensaje en un canal, la capa de transporte debe ocuparse del establecimiento y liberación de conexiones a través de la red. Esto requiere algún mecanismo de denominación, de tal forma que un proceso en una máquina tenga una manera de describir con quién desea conversar. También debe haber un mecanismo para regular el flujo de información, de manera que un host muy rápido no pueda desbordar a otro más lento.

Algunos de los mensajes generados por las entidades de red son demasiado largos para la capa de red e inferiores. La capa de transporte maneja la división de esos mensajes y puede combinar diversos mensajes pequeños que son deseados para el mismo destino.

Capa de Sesión

La Capa de Sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utilizan en algunas aplicaciones. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.



Capa de sesión del modelo OSI

Uno de los servicios de la capa de sesión consiste en gestionar el control de 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 quien tiene el turno.

Otro de los servicios de la capa de sesión es la sincronización. Proporciona una forma para insertar puntos de verificación en el flujo de datos, con objeto de que, después de alguna caída, solamente tengan que repetirse los datos que se encuentren después del último punto de verificación.

La capa de sesión asiste a las peticiones de servicio para el establecimiento y mantenimiento de las comunicaciones. En la práctica ésta función se divide en tres tareas:

- **Establecimiento de conexión.** El establecimiento de conexión incluye todas las subtareas necesarias a ser desempeñadas, así que las entidades reconocen cada una y la comunican. A menudo estas subtareas incluyen:

  - Verificar las cuentas de los usuarios y sus contraseñas.
  - Establecer números de identificación de conexión.
  - Determinar que entidad comienza la conversación.

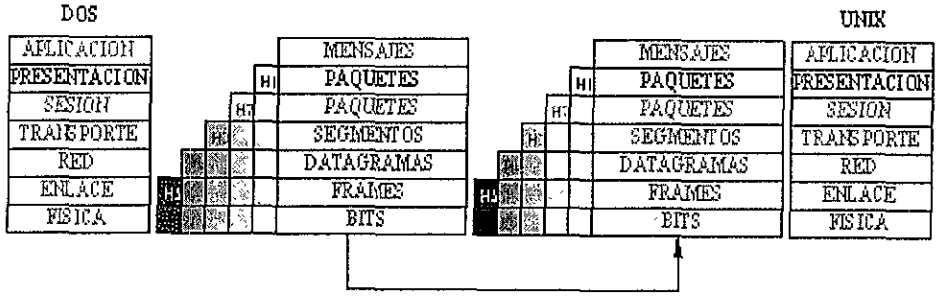
- **Transferencia de datos.** Las tareas de transferencia de datos mantienen la comunicación o conexión y pasan mensajes entre dos entidades. Las siguientes tareas son comúnmente desempeñadas:

  - Transferencia de datos actual.
  - Reanudación o interrupción de comunicaciones.

- ***Emitir conexión.*** *La conexión liberada es la tarea que termina una sesión de* comunicación. Esto puede ser hecho entre dos entidades. El servicio de petición (o proveedor) puede entonces reconstruir la sesión o reiniciar la comunicación usando una nueva sesión.

Capa de Presentación

La capa de presentación transforma los datos a un formato (transfiere la sintaxis) que pueda usarse para entender cada aplicación de red y de las aplicaciones que estén corriendo. La capa de presentación puede también comprimir o expander y encriptar y desencriptar datos.



Capa de presentación del modelo OSI

La Capa OSI de Presentación realiza ciertas funciones que se necesitan frecuentemente para buscar una solución general para ellas, más que dejar que cada uno de los usuarios resuelva los problemas. En particular y, 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.

Las computadoras pueden tener diferentes códigos para representar las secuencias de caracteres (ASCII y EBCDIC), enteros, etc. Para posibilitar la comunicación de las computadoras con diferentes representaciones, la estructura de los datos que se van a intercambiar puede definirse en forma abstracta, junto con una norma de codificación que se utilice en el cable. 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.

La capa de presentación está relacionada también con otros aspectos de representación de la información. Por ejemplo, la compresión de datos se puede utilizar aquí para reducir el número de bits que tienen que transmitirse y el concepto de criptografía se necesita utilizar frecuentemente por razones de privacidad y autentificación.

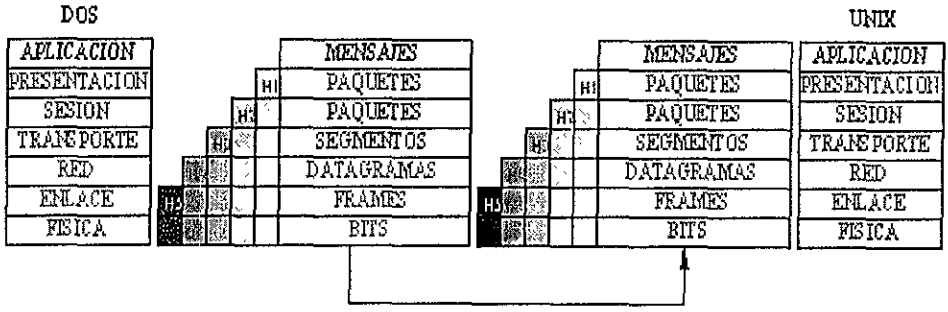
La encriptación se realiza comúnmente mediante software y es considerada parte de la capa de presentación. Los siguientes dos métodos son comúnmente usados para notificar a las entidades el método de encriptación utilizado:

- **Llaves Privadas.** El método de Llave privada utiliza sólo una Llave. Las entidades de red que tiene la Llave son capaces de encriptar y desencriptar cada mensaje. Por lo tanto, la Llave se debe mantener privada. La Llave puede ser establecida por el administrador de red. *Sin embargo, cada vez que la Llave es cambiada,* todos los dispositivos deben actualizarse (preferentemente no usando la red para pasar la nueva Llave).

- **Llaves Públicas.** Las entidades de red que usan métodos de llaves públicas están provistas de una llave secreta y de valor conocido. Una entidad crea una llave pública manipulando el valor conocido y el valor secreto de la llave. La entidad que inicia la comunicación envía su llave pública al o los receptores entonces la otra entidad matemáticamente combina su propia llave secreta con la llave pública que le fue provista para establecer el valor mutuo de encriptación. Tener sólo la llave pública es una ayuda mínima para los usuarios no autorizados. La complejidad de la llave encriptada resultante es muy compleja para ser calculada en un tiempo razonable.

Capa de Aplicación

La capa de aplicación incluye todos los tópicos y funciones especificadas en cada servicio de red. En otras palabras, las seis capas inferiores incluyen las tareas y tecnologías que generalmente soportan los servicios de red, mientras la capa de aplicación provee los protocolos necesarios para desempeñar las funciones especificas de los servicios de red.



Capa de aplicación del modelo OSI

La Capa de Aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos de terminales incompatibles en el mundo. Considérese la situación de un editor orientado a pantalla que desea trabajar en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de pantalla, de secuencias de escape para insertar y borrar texto, de movimientos de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracta, con lal que los editores y otros programas pueden ser escritos para tratar con ella. Con objeto de transferir funciones de la terminal virtual de una red a un terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software deberá emitir la secuencia

de comandos apropiados para que la terminal real ubique también su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la capa de aplicación.

Otras funciones de la capa de aplicación es la transferencia de archivos. Distintos sistemas de archivo tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las líneas de texto. La transferencia de archivos entre dos sistemas diferentes requiere de una solución a éstas y otras incompatibilidades. Este trabajo, así como el correo electrónico, el trabajo a distancia, el servicio de directorio y otros servicios de propósito general y específico, también corresponden a la capa de aplicación.

Cabe recordar que aunque los fabricantes de hardware y los de software son los usuarios principales del modelo OSI, una comprensión general del modelo llega a ser benéfica para el momento en que se expande la red o se conectan redes para formar redes de área amplia (WAN).

2.2 CONSIDERACIONES DE DISEÑO

El diseño y manejo de la infraestructura de una red desde el principio no es una tarea sencilla. Muchos aspectos de diseño y administración pueden ser analizados basado en los objetivos de la compañía, las necesidades de los usuarios, el equipo y el software existente, protección de la inversión y otros.

El mayor cambio en la creación de una red es el diseño, la adquisición y la instalación de la infraestructura. La infraestructura es el fundamento físico de la red y consiste en los medios de comunicación físicos, dispositivos intermedios (puentes, ruteadores), sistemas operativos de red y protocolos de transporte, servidores (todo tipo), enlaces de área ancha y administración de proyectos para manejarlo como un todo.

La infraestructura es la base fundamental en la que toda la información debe ser transportada y en donde todas las aplicaciones de red deben operar. Primero se necesita desarrollar un análisis de necesidades para aprender más acerca de la compañía y como una red puede ser la mejor ayuda para alcanzar los objetivos de la misma.

Las consideraciones de diseño son las siguientes:

Objetivos de la Compañía

Comprendiendo los objetivos de la compañía es posible visualizar como se pueden mejorar sus beneficios en una red.

Crecimiento a Futuro

Todas las compañías tienen objetivos a largo y corto plazo. Un apropiado diseño de la red debe soportar estos objetivos.

Es importante el diseño flexible para que la red pueda crecer y cambiar para adaptarse al crecimiento futuro, adquisiciones de la compañía o cambios en la tecnología. Diseñar con flexibilidad usualmente significa diseñar la red alrededor de los estándares aceptados por la industria.

Grupos de Trabajo

Para diseñar una red alrededor de las necesidades de la compañía y de los usuarios.

a) Necesidades de los Usuarios

El diseño de toda red comienza y termina con los usuarios. Como una regla, la red debe mejorar el desempeño del trabajo de los usuarios.

La red debe actuar como una herramienta con la que puedan crecer los usuarios. En otras palabras, la red debe permitir a los usuarios crecer con el uso de la herramienta mejorando el desempeño de su trabajo.

b) Necesidades de los Grupos de Trabajo

Para diseñar la red alrededor de las necesidades de la compañía y de los usuarios. Se debe ver como una gran fotografía sobre todos los objetivos de la compañía. Una vez comprendido esto, se puede examinar partes más pequeñas de la red, como grupos de trabajo, usuarios, etc.

Los grupos de trabajo son donde el trabajo es concluido. Un grupo de trabajo consiste de un grupo de usuarios quienes comparten objetivos de trabajo comunes.

Seguridad

La importancia de la seguridad varía de una compañía a otra. La seguridad es la más grande preocupación. Sin embargo, como las compañías confiaron más y más en las

computadoras para procesar sus negocios, la seguridad de los datos y los recursos de la red, son requeridos para mantener a los negocios en operación, siendo esto lo más importante.

Algunas de las áreas de seguridad que necesitan ser consideradas son las siguientes:

- Autentificación del Login para recursos críticos.
- Seguridad física de los dispositivos de recursos físicos.
- Nivel de seguridad de los datos que viajan sobre la red.
- Respaldo de datos críticos (Tolerancia de Fallas).

Infraestructura Existente

Raramente los diseñadores de red entran en una situación donde ellos están creando una red para nada. Lo que significa que es mejor tener alguna porción de la infraestructura de la red. Los grupos de trabajo existentes pueden proveer información estadística acerca de las necesidades y requerimientos de los usuarios.

El cambio para los diseñadores es integrar mucho del hardware y protocolos existentes en una red totalmente interoperable, o proveer un camino para migrar a ese estado. Es importante tener cuidado en que por ahorrar algo de dinero se puede comprometer la estructura y el desempeño integro de la red.

Administración

La administración de la red consta de muchos aspectos, como detectar errores en los medios de comunicación (cable, media) para enfilar a los usuarios en las aplicaciones de red.

Características de los Tipos de Red Existentes

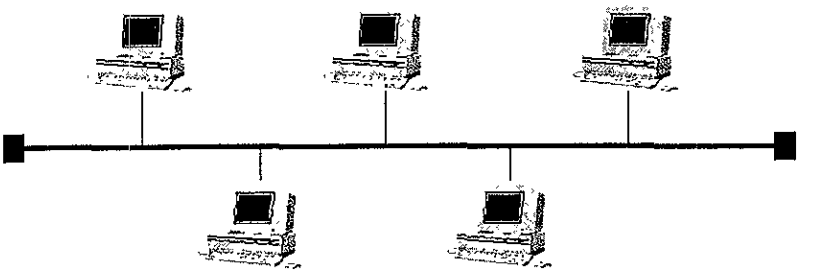
Una importante parte en el diseño de una LAN es escoger un método de acceso a medios de comunicación. Los métodos de acceso a medios de comunicación están basados en las necesidades de los grupos de trabajo. Cuando se diseña una inter-red el impacto de la selección de medios de comunicación debe ser considerado, no sólo con el criterio LAN en mente.

Existen protocolos de acceso a medios de comunicación:

- Ethernet (IEEE 802.3 y Ethernet II).
- Token Ring (IEEE 802.5).
- Interface de Fibra de Datos Distribuidos (FDDI) ANSI X3T9.5 -- Fiber Data Distribuited Interface.

Ethernet

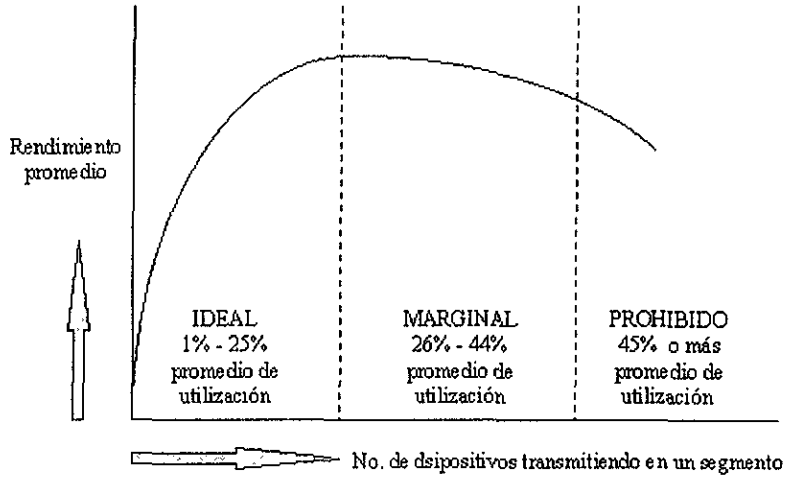
Ethernet es un método de acceso de 10 Mbps, actualmente se encuentran implementaciones de esta red a 100 Mbps. Acceso equivalente significa que cualquier dispositivo puede transmitir datos a través de otro dispositivo que no esté transmitiendo en forma concurrente.



Topología Ethernet

Ethernet fue originalmente desarrollado por Xerox a finales de los 70´s y después mejorado por el Instituto de Ingenieros Electrónicos Electricistas (IEEE). La especificación Xerox es conocida como Ethernet II. La especificación IEEE es conocida como IEEE 802.3 (ISO 8802-3).

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

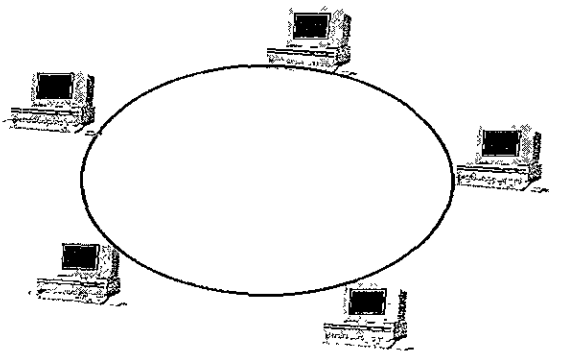


Ancho de banda utilizable por Ethernet

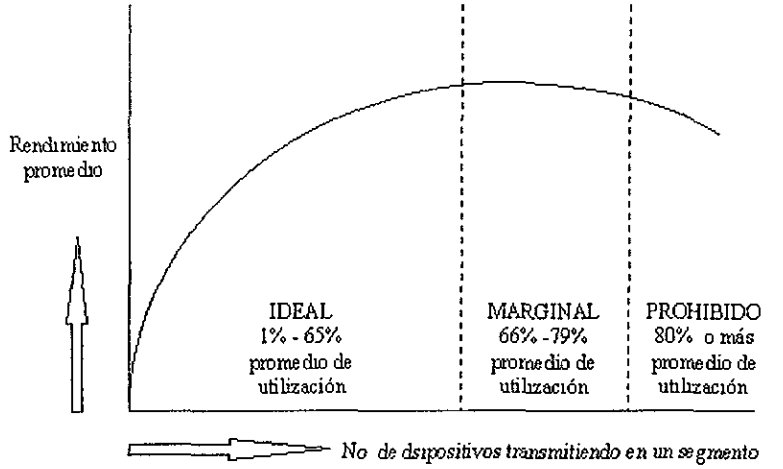
Token Ring

Para transmitir datos en una red token ring, una estación primero debe recibir el token. Un token es un bit muestra o modelo que cuando es capturado por un dispositivo le permite transmitir datos en un tiempo especifico. Cada estación tiene su turno para accesar a la red lo que hace a token ring un método de acceso

determinístico.



Topología Token Ring



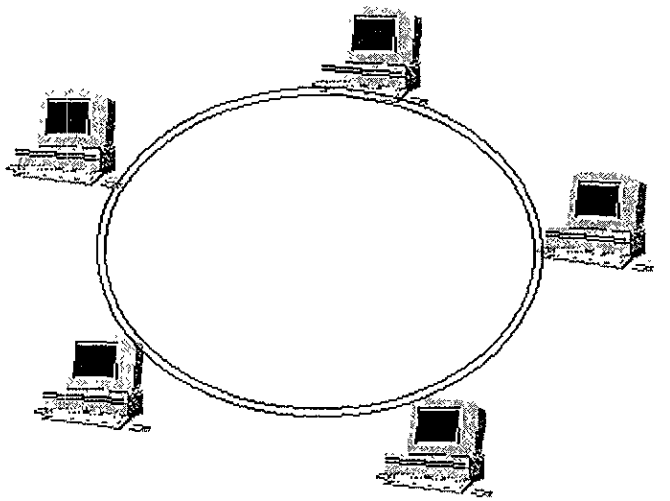
Ancho de banda utilizable por Token Ring

Anillo Modificado (Token Ring)

También conocida como Estrella-Anillo. El anillo se encuentra dentro de un ruteador de señal que puede ser un MSAU (Multistation Acces Unit), que hoy en día se está sustituyendo por concentradores inteligentes, al cual se conectan uno a uno los nodos formando una estrella. La señal siempre pasa por el ruteador. Comúnmente este arreglo utiliza cable par trenzado (UTP o STP) a 4 o 16 Mbps. La ventaja de utilizar esta topología y no el anillo físico es que si una estación falla o se desconecta, el concentrador de inmediato cierra el anillo evitando la caída de la red.

FDDI

Fiber Distributed Data Interface (FDDI) es el primer estándar de acceso (ANSI X3T9.5) a medios de comunicación de fibra óptica. Este método es similar a token ring ya que requiere dispositivos para capturar un token en orden para transmitir. FDDI difiere de token ring en que el primero tiene un ancho de banda de 100 Mbps y el segundo de 4 a 16 Mbps.



Topología FDDI

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

Utiliza como medio principal de cableado fibra óptica y muy recientemente el cable UTP categoría 5 y cable STP.

Con esta topología se pueden alcanzar velocidades de 100 Mbps compartidas entre cada uno de los dispositivos conectados al doble anillo redundante.

Seleccionando el Sistema Operativo de Red (NOS)

El sistema operativo de red permite acceso por las estaciones de trabajo de los usuarios a los recursos de la red. Recientemente el sistema operativo fue identificado con el software de archivos y con el de servidor de impresión que incluían el software de las estaciones o cliente. *Las versiones actuales de los sistemas operativos de red* ofrecen muchos servicios:

- Servidores de comunicación.
- Servidores de correo.
- Servidores de bases de datos.
- Administración de servidores.

Existen diferentes criterios para determinar o escoger un sistema oprativo de red, estos son:

- Todos los sistemas operativos de red en la inter-red deben ser los mismos. Esto simplifica el compartir datos y recursos entre las LAN y minimiza las tareas de ruteo de múltiples protocolos.

- El lugar de trabajo rara vez tiene sólo un ambiente de computación. Por ejemplo es usual encontrar estaciones de trabajo DOS, Macintosh, UNIX en el mismo campus de una compañía. Por esta razón los sistemas operativos de red y sus servidores deben soportar todos o la mayoría de estos ambientes nativos.

- Los sistemas operativos de red en un ambiente de inter-redes deben soportar algunos tipos de servicios de directorio. Esto provee recursos a la inter-red que para los usuarios sean mucho más fáciles de implementar y controlar.

Dialogar con Múltiples Protocolos

Soportar múltiples ambientes de usuario significa que la inter-red debe ser capaz de soportar múltiples protocolos de transporte; una regla que puede ser de utilidad para la integridad de múltiples protocolos de transporte en las LAN o en la inter-red es evitar las puertas de acceso (Gateways) siempre que sea posible. Un gateway es un dispositivo o servicio que puede traducir uno o varios protocolos en orden para proveer servicios. Estos son ineficientes y crean un cuello de botella en la LAN o en la inter-red. Los gateways no representan problema con las capas mayores de los protocolos.

Categorías Funcionales de Modelo OSI

Las limitaciones de los medios de comunicación LAN radica en que cada dispositivo está limitado por el número de dispositivos que pueden estar conectados a un cable, *la distancia que viaja una señal en un medio se vuelve ya sea muy débil o la fase es* inteligible. Los repetidores y los puentes ayudan a superar estas limitaciones.

Los dispositivos intermedios caen en las siguientes categorías:

- Repetidores, usados para superar la distancia de los medios de comunicación y las limitaciones de los dispositivos.

- Puentes, superan las limitaciones del ancho de banda.
- Ruteadores, son dispositivos usados para conectar LAN´s en una MAN y ambientes WAN independientes del medio de comunicación.
- Gateways, son utilizados para conectar sistemas que no tienen protocolos en común.

2.3 PROTOCOLOS

Al utilizar una red de computadoras, es muy común ver como las computadoras se comunican entre sí, pero para que esto pueda llevarse a cabo es necesario contar con los elementos que permitan establecer dicha comunicación, uno de estos elementos son los protocolos de comunicación.

Los protocolos de comunicación de datos son usados para coordinar el intercambio de información entre diferentes dispositivos de la red. Ellos establecen el mecanismo para que dos computadoras dentro de una red puedan entenderse.

Un protocolo es un conjunto de reglas que definen la forma en que debe efectuarse la comunicación en la red, incluyendo el formato, la temporización, la secuencia, la revisión y la corrección de errores.

Los protocolos de comunicación han evolucionado, permitiendo mayor confiabilidad en el uso de los mismos. Los teleimpresores fueron diseñados y desarrollados alrededor de 1915, esto permitió la comunicación humana a través de estos equipos, constituidos básicamente por impresores y teclados, naturalmente en las técnicas para el control de la comunicación se emplearon protocolos humanos. El advenimiento de los equipos de perforación y lectura de cintas de papel en los años 40's, creó la necesidad de establecer centros de conmutación, en los cuales se efectúa el control de las comunicaciones, en este caso el operador del teleimpresor tecleaba un mensaje el cual se transmitia al centro de conmutación, generando una cinta perforada en la que los primeros caracteres contenían información sobre el destino del mensaje, que se leía en forma visual, para que posteriormente, en forma manual, se alimentara a una lectora de cinta de papel, conectada al teleimpresor al que se diría el mensaje.

Cuando los centros de conmutación fueron automatizados, por los años 50's, surgió la necesidad de usar caracteres de control, de manera que el equipo pudiese

diferenciar entre texto y dirección; adicionalmente, de acuerdo a diferentes aplicaciones específicas, se usaron muchos otros caracteres de control que conformaron finalmente la cobertura del protocolo tal como se conoce actualmente.

La evolución continuó, dirigida principalmente por las necesidades de la industria de la conmutación de mensajes. Tuvieron lugar las estandarizaciones, se empezaron a tratar los problemas de detección y corrección de errores, así como la necesidad para el control de dispositivos, ya con un enfoque para el establecimiento de comunicación entre equipos.

Un gran paso fue la implementación en forma dominante del protocolo síncrono binario (BISYNC) de IBM; pero retrospectivamente, podemos ver fallas en este protocolo como la inexistente transparencia al usuario, ya que en dicho protocolo se emplean caracteres de control; esto impide que todos los caracteres del código sean empleados como parte de un texto. Además el control de dispositivos está mezclado con el control de la transmisión, de tal manera que fueron necesarias diferentes implementaciones para diferentes dispositivos y aplicaciones.

En un principio los protocolos fueron creados por cada fabricante de equipo de comunicaciones y computadoras, con el fin de brindar a sus clientes la posibilidad de comunicar a sus computadoras entre sí, esto permitió la existencia de un sin número de protocolos, debido a que cada fabricante creaba su propio protocolo. Con el paso del tiempo y ante la necesidad de conectar computadoras que no eran del mismo fabricante, se establecieron estándares que permitían que dos computadoras de diferentes fabricantes pudieran comunicarse sin problema.

Al final de este periodo de evolución, la industria de la computación, reconocía la importancia de la transparencia e independencia del dispositivo, de tal manera que los procedimientos de comunicación pudieran ser usados independientemente del contenido del mensaje o características de los equipos a comunicarse. Aquí las agrupaciones de estándares comenzaron a trabajar hacia una nueva generación de

protocolos estándares, aunque IBM anticipándose a estas organizaciones creó el protocolo Control de Enlace de Datos en modo Síncrono (SDLC), al que también se le conoce como protocolo con orientación a bit. Posteriormente la organización de estándares publicó el protocolo Control de Enlace de Alto Nivel (HDLC) y el Instituto de estándares nacional americano publicó el Control de Procedimientos Avanzado para Comunicación de Datos (ADCCP).

En el mundo de las comunicaciones de hoy, existe un gran número de protocolos en uso, desarrollados por diferentes fabricantes, algunos se han convertido en estándares para la industria de las comunicaciones.

Actualmente los protocolos son creados por organizaciones de estándares de redes y proveedores de equipo de comunicaciones, con la finalidad de que todos los productos que estén en el mercado sean compatibles.

2.3.1 Funciones de un protocolo de comunicaciones

Un protocolo de comunicaciones debe realizar las siguientes funciones:

- **Sincronización** entre las partes a comunicar. La transmisión implica la existencia de un medio propicio para la comunicación, técnicamente, este medio puede ser un canal de microondas, una línea telefónica, fibra óptica, etc., de tal forma que para lograr la comunicación o intercambio de información, es evidente que debe existir sincronización.

  El propósito primario de un protocolo, es precisamente la conversión de transmisión en comunicación, a través de la adquisición y mantenimiento del sincronismo entre las máquinas a comunicar (en un ambiente de proceso remoto) de tal manera que se establece y mantiene un estado conocido en la máquina remota.

- **Control de acceso** para el acceso de los equipos. En las redes donde predominan determinadas configuraciones o modos de conexión, y que le dan a la red una característica especial, es necesario algún tipo de control del acceso y utilización de los recursos de la red. Existen diferentes tipos de control que se adaptan a cada aplicación y van desde la ausencia virtual de control (sistemas en CONTENCION) hasta la alternativa de un control centralizado muy marcada, dependiendo también de los niveles de tráfico, tiempo de respuesta, costos, etc.

  La forma más simple de controlar un canal de comunicación es manteniéndolo en contención, es decir, las terminales conectadas a un canal, compiten por su acceso, de tal forma que si una terminal tiene un mensaje que enviar a la central de proceso, realiza una solicitud de acceso; si el canal está desocupado, la terminal hace uso de él, de otra manera la terminal debe esperar.

  Para este tipo de control, el programa de comunicaciones almacena las solicitudes de envío de terminales y se atienden mediante la regla que establece que las primeras entradas son atendidas prioritariamente (FIFO) o algún otro tipo para el manejo de colas. Esta alternativa de contención tiene desventajas, ya que no es controlable el tiempo de acceso al canal de comunicación, lo cual no es recomendable para redes con enlaces multipunto con demasiado tráfico, por lo que los procedimientos de contención son ideales en los sistemas donde la utilización de los canales de comunicación es baja.

  Otro procedimiento para el control de acceso a los canales de comunicación que se emplea comúnmente en enlaces multipunto, se basa en el envío continuo y programado de "invitaciones a transmitir", actividad que se conoce como poleo (POLLING). Existen dos tipos de poleo; el ROLL CALL POLLING y el HUB POLLING.

  En el primero, el programa de comunicaciones envía el mensaje de POLL, de

acuerdo a una secuencia preestablecida, la cual (según el software residente) es modificable de acuerdo a las necesidades; es decir, si tenemos puertos con líneas multipunto de tráfico elevado, es posible asignar una secuencia del POLL a los diferentes puertos y líneas, de tal manera que en esos puertos y líneas, el POLL se realice un mayor número de veces. Si una terminal al recibir un POLL no tiene datos por transmitir, envía un mensaje de rechazo que le indica a la estación transmisora esta situación. Si la terminal desea transmitir, la información contenida en el área de almacenamiento de la terminal es enviada como respuesta a un POLL.

En el sistema HUB POLLING se incluye una superposición lógica de un canal en loop, sobre el cual fluye el POLL, dicho mensaje es pasado de una estación a la siguiente; de tal manera que si una estación tiene información por enviar, al momento de recibir el POLL, la información se envía entonces sobre el canal físico de transmisión, en caso contrario dicha estación pasa el POLL a la estación siguiente.

Con este control de acceso se tiene un mejor aprovechamiento de la línea, además de que los caracteres de control disminuyen en número; otra ventaja importante se tiene en una mejora notable del tiempo de respuesta y ahorros que se reflejan en número de puertos utilizados y líneas, ya que es posible conectar más terminales a una misma línea. Las desventajas de estos procedimientos están relacionadas con la confiabilidad de las técnicas de control de acceso en conexiones loop, además de las modificaciones de hardware necesarias en los equipos terminales.

- **Intercambio de datos y actividades de interrupción y desconexión.** Un factor muy importante para cualquier protocolo es la existencia de un código para la representación de los caracteres a transmitirse dentro del mismo código, contar con un grupo de caracteres que pueden ser usados como caracteres de control, los cuales constituyen un alfabeto de propósito especial.

Los caracteres de control son usados para el establecimiento de un enlace de datos, transferencia de mensajes, interrupciones y terminación del enlace.

Para ello, se establece la conexión física entre las partes a comunicar y se establece un enlace de datos, en ese momento, la información es transferida con un formato específico, el cual generalmente está compuesto por tres partes: encabezado, texto y terminador. La información contenida en el encabezado depende de la aplicación en uso, pudiendo contener información sobre prioridad del mensaje, clasificación de seguridad, procedencia, longitud del mensaje, destino, fecha, etc.

El texto es toda la información útil la cual no debe ser alterada en su tránsito a la estación receptora o viceversa. El propósito del terminador puede ser diferente ya sea para separar mensajes que están siendo transmitidos sobre un enlace de datos, para provocar una desconexión o cambio de dirección de la comunicación, *para forzar ciertas longitudes de bloques orientados a mejorar la eficiencia en la* transmisión o para almacenar información destinada a usarse en chequeos de paridad con el mensaje

- **Detección y control de errores.** Una de las inevitables consecuencias de la transmisión de datos sobre medios de comunicación que excedan cien metros, es la ocurrencia de errores. De aquí la importancia de la creación de sistemas para obtener una protección contra los errores.

Una posibilidad es ignorar los errores, aunque esto sólo se justifica en sistemas con aplicaciones muy específicas. En esta situación un operador de terminal puede inferir el verdadero significado de un mensaje de error.

Cuando los errores no pueden ser ignorados, se puede recurrir a sistemas que involucran primero una detección e inmediatamente una retransmisión, pudiendo

estos funcionar en forma manual o automática.

2.3.2 Clasificación de protocolos

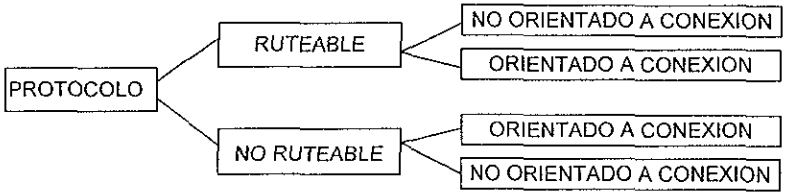
En una red de área local (LAN) todos los nodos conectados requieren de un protocolo de comunicaciones que pueda transportar información de un nodo a otro. Estos protocolos operan en diferentes capas del modelo OSI.

Así encontramos que en las primeras dos capas del modelo OSI se definen los protocolos que se encargan de accesar el medio físico de comunicaciones; así como de generar los paquetes correspondientes a una determinada tecnología de LAN como Ethernet, Token Ring, FDDI, entre otras.

Cada paquete 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 encapsuló la información en un paquete. También se encarga de *entregarla o recibirla desencapsulada del paquete al medio, según sea el caso de* transmitir o recibir respectivamente.

Una primera clasificación de los protocolos, es con relación al tipo de enlace que realizan al momento de establecer comunicación entre dos computadoras.

Una de las principales características de los protocolos superiores a la capa 2 del modelo OSI, 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 o no orientado a la conexión.



Protocolos Orientados a la Conexión

Los protocolos orientados a la conexión son aquellos en los que dado que el proceso de comunicación entre los nodos se realiza miles de veces durante una sesión normal de trabajo el efecto final es como si ambos nodos mantuvieran una comunicación constante entre ellos como si fuera una conexión virtual.

La mayoría de los protocolos ruteables que opera en la capa 3 del modelo OSI no es orientada 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.

Protocolos No Orientados a la Conexión

Los protocolos no orientados a la conexión, son como el correo ordinario, no garantizan que la información transmitida se envíe íntegramente.

Una de las ventajas de los protocolos no orientados a la conexión 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 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.

Protocolos Ruteables

Un protocolo ruteable puede definirse como aquel que "interpreta" origen y destino de la información que lleva consigo en sus paquetes, como un ente lógico denominado red. Cada segmento físico de LAN es definido como una dirección lógica.

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 puede llevar también el número de nodo -- MAC Adress -- origen (Número de casa del remitente) y el número de nodo destino (Número. de casa del destinatario).

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

Protocolos No Ruteables

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

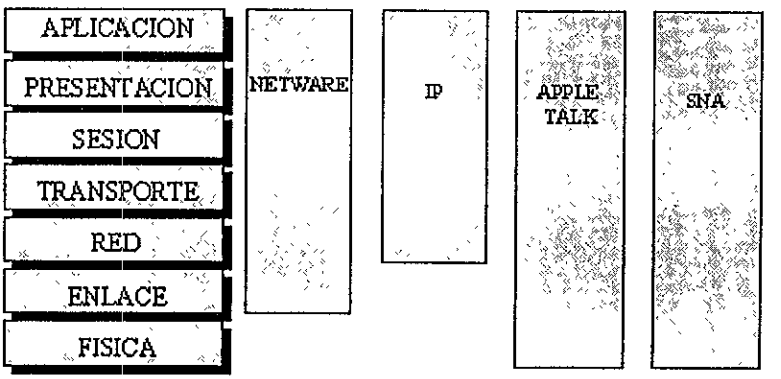
Al conectar varios segmentos físicos de red entre sí, es decir, al crear una inter-red,

ya sea con segmentos de LAN o con segmentos de WAN debemos utilizar un dispositivo conocido como puente. Un puente es un elemento de comunicaciones que sólo propaga las direcciones físicas de los nodos. Por esta razón, los puentes permiten extender los segmentos físicos de red y hacen parecer a los protocolos no ruteables, como una sola red a todos los segmentos interconectados con puentes. No existe el concepto de red lógica desde el punto de vista de los protocolos no ruteables, por lo que a estos protocolos sólo les interesa saber las direcciones física de cada nodo.

2.3.3 Relación de los protocolos con el modelo OSI

Un protocolo es un conjunto de reglas formalizadas, convenciones y estándares. Una Suite de Protocolo indica un grupo de especificaciones que pueden utilizarse juntas. Un Stack de Protocolo es la suite ordenada en jerarquía lógica.

Los protocolos funcionan en diferentes capas del modelo OSI como se muestra a continuación:



Relación de los protocolos con el modelo OSI

Actualmente, existe un gran número de protocolos que se utilizan en aplicaciones muy diversas, y en distintos tipos de redes, la importancia de cada uno de ellos dependerá del tipo de red que se desee instalar, así como los servicios que se desee dar a los usuarios

A continuación se presentan algunos de los protocolos existentes actualmente en el mercado:

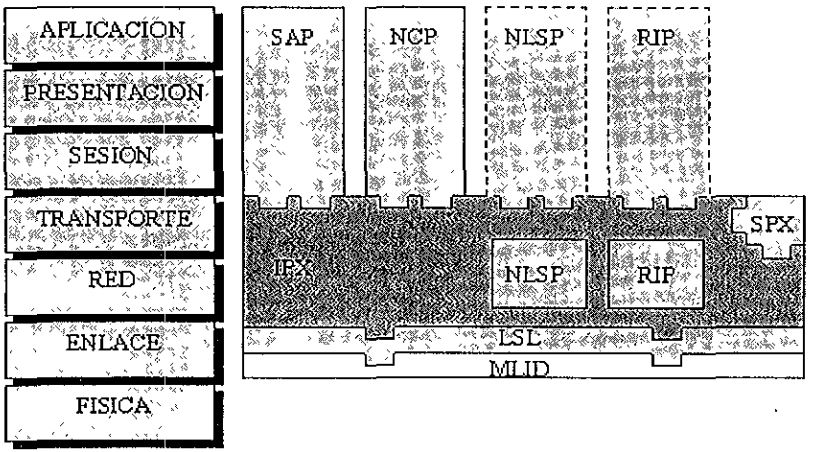
Netware

NetWare es el sistema operativo más usado en redes LAN hoy en día. Creado por Novell, Inc. e introducido al mercado en los 80's. El sistema completo de NetWare provee servicios de archivos, impresión, aplicaciones y bases de datos.

Desde su introducción en el mercado la aceptación de NetWare ha ido creciendo debido a su flexibilidad. NetWare puede correr con varios stacks de protocolos de transporte, enlaces tecnológicos y plataformas de computadoras. También soporta comunicaciones con gran número de sistemas operativos, incluyendo DOS, Macintosh, OS/2, Windows NT, UNIX y VMS.

Suite del Protocolo NetWare en Modelo OSI

El protocolo NetWare es modular y por capas. La suite del protocolo no es nativa en las siete capas del modelo OSI; sin embargo desde que todas las redes de computadoras tienen direcciones similares y métodos, el protocolo NetWare puede estar asignado o agrupado.



Suite del protocolo NetWare en el modelo OSI

Sumario del Protocolo NetWare

- Multiple Link Interface Driver (MLID). Nombre que le dio Novell a un driver de tarjeta de red. Específicamente es una pieza de software que cumple con la arquitectura de la interface ODI (Open Data-link Interface).
  Un MLID no se liga directamente a un stack de protocolo individual ya que puede estar concurrentemente BOUND a varios stacks.

- Link Support Layer (LSL). Es la interface entre el MLID y las capas superiores del stack de protocolo. Interpreta la identificación de protocolo de cada paquete y lo pasa al stack apropiado.

- Internetwork Packet eXchange (IPX). Es un protocolo de la capa de red no orientado a la conexión Derivado de XNS's Internetwork Datagram Protocol (IDP).

- Router Information Protocol (RIP). También fue derivado de XNS. RIP es un protocolo de descubrimiento de ruta vector de distancia que utiliza un contador de hop (saltos) para determinar el costo.

- NetWare Link Services Protocol (NLSP). Protocolo de descubrimiento de ruta link-satate modelado después de un protocolo de ruteo.

- Sequenced Packet eXchange Protocol (SPX). Es una extensión de IPX que provee paquetes orientados a la conexión en la capa de transporte.

- NetWare Core Protocols (NCP). Es un COMPRISED de numerosas llamadas a funciones que soporten los servicios de red.

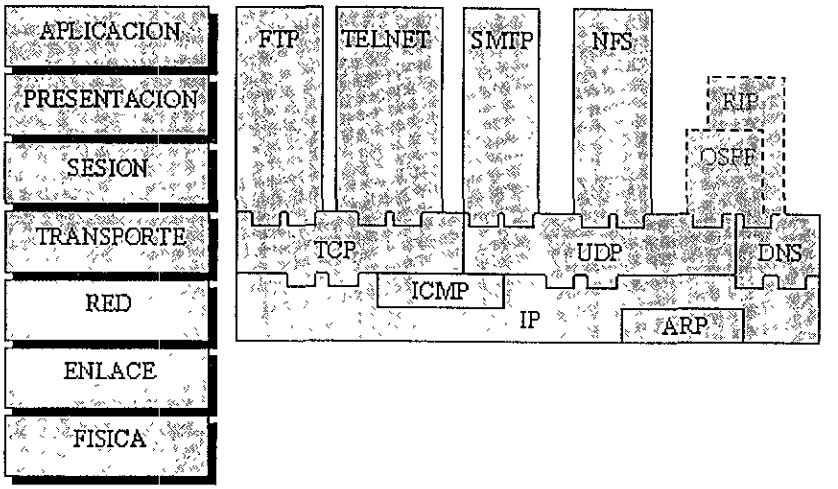
- Service Advertising Protocol (SAP). Los servidores NetWare utilizan SAP's para avisar de sus servicios.

Protocolo Internet

La suite del Protocolo Internet fue desarrollada por el Departamento de la Defensa de los Estados Unidos y varias organizaciones investigadoras en los 70's. Hoy en día es el conjunto de protocolos de comunicación y aplicaciones usadas para conectar sistemas heterogéneos. Los mejores dos protocolos conocidos en la suite son Transmission Control Protocol (TCP) e Internet Protocol (IP), comúnmente referida como TCP/IP; sin embargo la suite del grupo es llamada Protocolo Internet.

Suite del Protocolo de Internet en el Modelo OSI

La suite de Protocolo Internet especifica funciones correspondientes a las capas del modelo OSI superiores a la capa de enlace.



Suite del protocolo IP en el modelo OSI

Sumario del Internet Protocol

- Internet Protocol (IP). Es una switcheo de paquetes no orientado a la conexión en la capa de red que realiza la selección de direcciones y rutas.

- Internet Control Message Protocol (ICMP). Trabaja con IP para proveer la información de error y otra información de control.

- Routing Information Protocol (RIP). Es un protocolo de descubrimiento de ruta distance-vector. Las implementaciones RIP periódicamente envían broadcast a sus tablas de ruteo a través de la red.

- Open Shortest Path First (OSPF). Fue desarrollado para las direcciones RIP más débiles. Es un protocolo de descubrimiento de ruta link-satate que provee la habilidad especifica de descubrir la topología específica de la red.

- Domain Name System (DNS). Es un sistema de base de datos distribuida que desempeña la resolución de nombres y direcciones de las aplicaciones del cliente. Los servidores DNS mantienen la estructura jerárquica de nombre para que los hosts individuales puedan usar nombres lógicos para la identificación humana.

- File Transfer Protocol (FTP). Habilita a un usuario a transferir archivos entre dos computadoras en red.

- Simple Mail Transfer Protocol (SMTP). Es un protocolo de ruteo de correo electrónico que utiliza TCP/IP para rutear los mensajes entre diferentes hosts en la red

- Remote Terminal Emulation (TELNET). Permite a los usuarios accesar aplicaciones en el host sobre la red con computadoras personales que funcionan como terminales.

- Network File System (NFS). Fue desarrollado por SUN Micro Systems y es actualmente el nombre asociado a la familia de protocolos que comprende la plataforma Sun ONC (Open Network Computing).

- TCP y User Datagarm Protocol (UDP) son protocolos host-to-host. IP e Internet Control Message Protocol (ICMP), mueven datos a través de la red conectando recursos y máquinas destino.

  TCP (Transmision Control Protocol - Protocolo de Control de la Transmisión), es el protocolo de transporte primario de Internet, además suministra confiabilidad a IP. Es un protocolo orientado a la conexión que acepta mensajes de cualquier longitud que provengan de un protocolo de capas superiores y proporciona comunicación full-duplex, números de reconocimiento y transporte de flujo controlado a otra estación que corra TCP.

TCP garantiza la confiabilidad del flujo del enlace orientado a la conexión nodo a nodo, y confía el material a IP para que se haga cargo de fragmentarlo y reensamblarlo tanto como se requiera.

TCP requiere que la conexión sea establecida entre dos procesos que necesiten comunicarse. Este proceso emplea un cierto tiempo y esfuerzo necesario para ampliar desde el principio hasta el fin de una sesión que afecte el establecimiento o caída de la conexión. Durante el establecimiento de la conexión, los parámetros fundamentales que son usados desde el principio hasta el fin para establecer la conexión incluyen el uso de socket, número de secuencia de datos y tamaño de la ventana para el control del flujo.

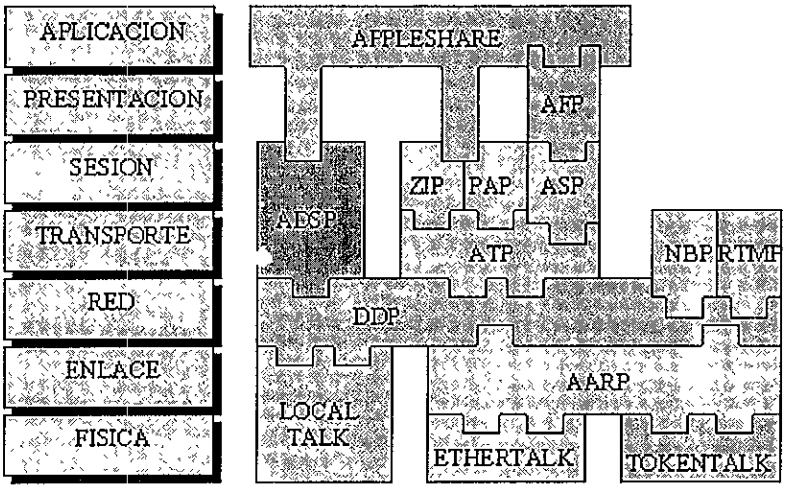
El punto final de la conexión de TCP es llamado socket, el cual es la combinación de la dirección de red, dirección del nodo y número de socket del nodo local. El socket es un concepto lógico que facilita procesar múltiples aplicaciones para usar el servicio de transporte de TCP en la misma computadora.

Apple Talk

Apple Computer inició el desarrollo de la suite del protocolo Apple Talk en 1983, el cual fue creado como la arquitectura de red para las computadoras Apple Macintosh. Hoy en día Apple Talk provee conectividad para una variedad de sistemas de cómputo, incluyendo PC's IBM corriendo MS-DOS, Mainframes IBM, Digital Equipment VAX y varias computadoras UNIX.

Suite del Protocolo AppleTalk en el Modelo OSI

La suite del protocolo Apple Talk fue desarrollada después de que el modelo de referencia OSI fuera concebido.



Suite del protocolo Apple Talk en el modelo OSI

Sumario del Protocolo AppleTalk

Los protocolos de acceso de enlace LocalTalk, EtherTalk y TokenTalk (LLAP, ELAP y TLAP), son integraciones de Apple de las tecnologías de las capas física y de enlace de datos, para mantener consistencia en las convenciones de nombre. Apple se refiere a los protocolos sobre Ethernet como EtherTalk y sobre Token Ring como TokenTalk.

- Apple Talk Adress Resolution Protocol (AARP). Desde que ELAP y TLAP utilizan direcciones predefinidas de dispositivos físicos, AARP es usado por Apple Talk para mapear las direcciones Apple Talk, es decir, las direcciones físicas predefinidas en ELAP y TLAP.

- Datagram Delivery Protocol (DDP). Es el protocolo primario de la capa de red que provee servicios no orientados a la conexión entre dos sockets (el socket es como una Dirección de Servicio).

- Routing Table Maintenance Protocol (RTMP). Desempeña las funciones de descubrir rutas para crear y mantener las tablas de ruteo Apple Talk.

- Zone Information Protocol (ZIP). Se usa el concepto de zona para organizar lógicamente los servicios y proveerles nombre en la inter-red.

- Name Binding Protocol (NBP). Apple Talk utiliza los nombres para identificar cual es el curso de referencia de una entidad.

- Apple Talk Transaction Protocol (ATP). Es un aviso de una transacción no orientada a la conexión.

- Apple Talk Sesion Protocol (ASP). Es un estándar en la capa de sesión OSI diseñado para optimizar las funciones de los servicios de archivos.

- Printer Access Protocol (PAP). Es muy similar a ASP. También es un protocolo de la capa de sesión de OSI.

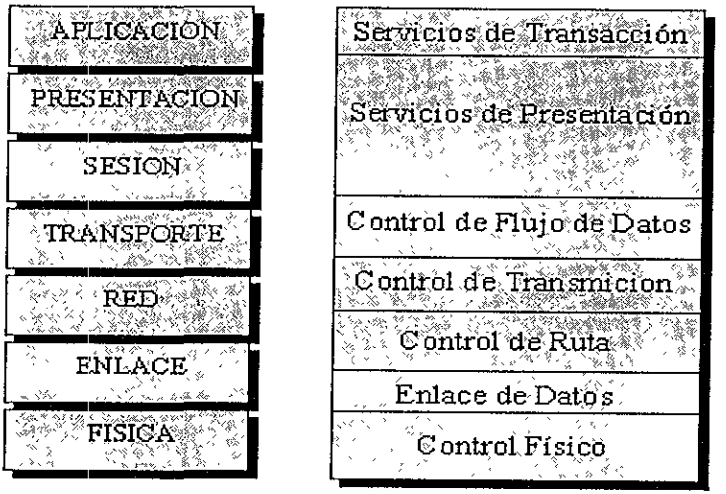
Sistema de Arquitectura de Red (SNA)

SNA es una arquitectura propietaria de IBM; como SNA no define un stack sencillo de protocolos, describe las características generales del hardware y software de las computadoras requerido para la interconexión.

En su primera versión en 1974, SNA soportaba solo redes jerárquicamente organizadas, con hosts, controladores de comunicaciones, controladores de CLUSTERS y terminales. La arquitectura original fue alterada por IBM en 1984 para soportar procesamiento distribuido y administración de red.

Suite del Protocolo SNA en el Modelo OSI

SNA es una arquitectura o modelo, no un stack de protocolo:



Suite del protocolo SNA en el modelo OSI

Capas de SNA

- Control Físico. Es lo concerniente a las características y procedimientos físicos y mecánicos de un medio físico de comunicación y de sus interfaces.

- Enlace de datos. SNA define el protocolo SDLC para implementar enlaces de comunicación donde la comunicación master o primaria con la esclava o secundaria, y un IBM Token Ring en redes peer-to-peer.

- Control de Ruta. Incluye funciones como ruteo, fragmentación y reensable de datagramas y control de flujo.

- Control de Transmisión. Provee un servicio de conexión punto a punto y provee servicios de encriptación y desencriptación.

- Control de Flujo de Datos. Controla las peticiones y es responsable del procesamiento, determina de quien es el turno de TALK, mensajes de grupos e interrupciones del flujo de datos en peticiones.

- Servicios de Presentación. Especifica los algoritmos de traducción de los datos, además de coordinar la compartición de recursos y sincronización de operaciones.

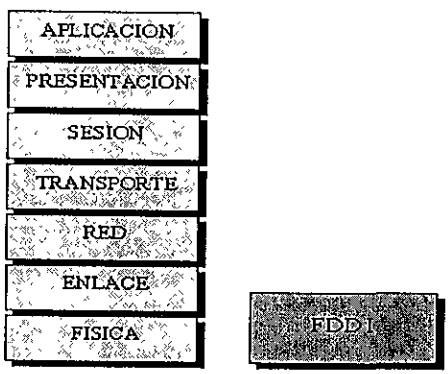
- Servicios de Transacción. Provee servicios de aplicación en forma de programas para implementar el procesamiento distribuido o administración de servicios.

Interfase de Datos de Fibra Distribuida (FDDI)

FDDI fue desarrollado por American National Standards Institute (ANSI). FDDI es considerado un protocolo WAN el cual también puede ser usado en MAN's o LAN's.

Suite del protocolo FDDI en el Modelo OSI

FDDI incluye las especificaciones de las capas física y enlace de datos del modelo OSI:



Suite del protocolo FDDI en el modelo OSI

Sumario del Protocolo FDDI

FDDI especifica un anillo lógico Token Passing de 100 Mbps que puede ser construido de fibra óptica o par trenzado. Es muy similar al IEEE 802.5, aunque ambos utilizan token-passing como método de acceso al medio.

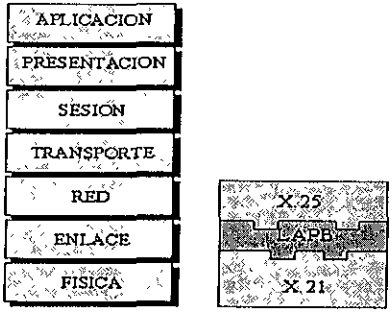
FDDI está basado en un anillo dual con contador rotante. Si un evento del medio falla, el tráfico de la red puede ser redireccionado por un nodo de red o concentrador que esté físicamente enlazado a los dos anillos. Estos dispositivos son llamados Dual-Attached Stations (DAS), los cuales pueden proveer cargas balanceadas entre los dos anillos.

Recomendación X.25

La International Telegraph & Telephone Consultative Committee (CCITT) que actualmente es conocida como International Telecomunications Unit (ITU) definió la recomendación X.25 en 1974. X.25 se basó en el switcheo de paquetes de red por Datapac, Tymnet y TELNET. X.25 es actualmente considerado un stack de protocolo WAN.

Suite del protocolo X.25 en el Modelo OSI

X.25 es una especificación para ligar a una computadora físicamente con una red de switcheo de paquetes y transmitir datos. Existen tres niveles:



Suite del protocolo X.25 en el modelo OSI

- Nivel 1. Incluye reglas de conectividad de la capa física, actualmente referenciadas a los estándares X.21, X21.bis y V.32.

- Nivel 2. Provee el mecanismo para crear una trayectoria de datos orientados a la conexión, definido como Link Access Procedures-Balanced (LAPB) protocol.

- Nivel 3. Define como pasan los paquetes entre un equipo terminal de datos (DTE), como computadoras y un equipo conmutado de paquetes (DCE).

Frame Relay

Fue desarrollado para direccionar implementaciones similares a X.25, pero asume un menor rango de error de red. Considerado un protocolo WAN.

Frame Relay es un servicio orientado a conexión que emplea PVC's y SVC en forma similar a la de conmutación de paquetes. Sesiones múltiples (de hasta 100 PVC's) pueden realizarse sobre un solo circuito físico a través de velocidades T1 y E1 fraccionadas, y hasta un T1 y E1.

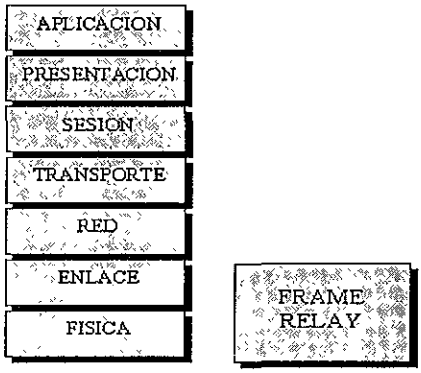
Frame Relay es sólo un servicio de transportación y no emplea el proceso del paquete de X.25, lo que garantiza un control de errores y flujo de polo a polo. Las necesidades de telecomunicaciones modernas han hecho necesarios el surgimiento de nuevos estándares y en el caso de la comunicación de redes de área amplia multipunto surge el estándar Frame Relay. Éste no es otra cosa que una derivación de la tecnología denominada de conmutación de paquetes, es decir, un protocolo de comunicación muy similar a X.25 mediante el cual, cualquier usuario puede conectar su nodo a un servicio de comunicación provisto normalmente por una empresa pública de transmisión de datos.

Al estar conectado al servicio de comunicación, el nodo puede tener acceso mediante circuitos virtuales a cualquier otro nodo que se encuentre conectado,

también a este proveedor de servicios de comunicación, formando lo que se puede entender como una nube de circuitos virtuales.

Suite del protocolo Frame Relay en el Modelo OSI

A Frame Relay solo le conciernen las funciones de la capa física y de enlace de datos del modelo OSI:



Suite del protocolo Frame Relay en el modelo OSI

Sumario del Protocolo Frame Relay

Es una especificación de protocolo y un tipo de servicio de red pública que provee eficientemente las funciones de la capa de enlace en circuitos virtuales conmutados o virtuales. Frame Relay ofrece las capacidades de 56 Kbps a 1.544 Mbps.

ATM

Asinchronous Transfer Mode (ATM) es uno de los estándares de red B-ISDN y cell relay. En el mercado se considera como protocolo WAN, aunque normalmente es considerado como un protocolo LAN, MAN y WAN.

ATM (Modo de Transferencia Asíncrona) es un estándar muy reciente que define

técnicas de alta velocidad, tanto para redes de área local (LAN) como para redes de área amplia (WAN), por lo cual toda la industria está a la expectativa de sus avances.

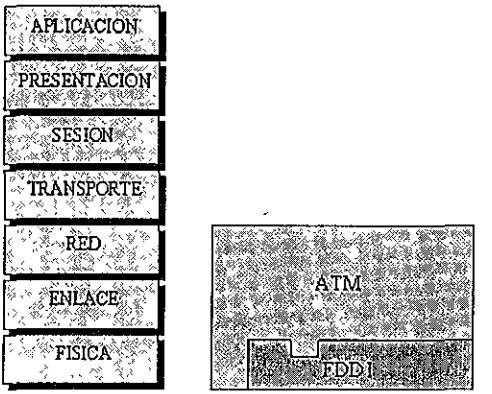
ATM es una técnica de red que usa un medio conmutado es decir mediante switcheo de paquetes. Puede ser instalado tanto sobre cable par trenzado como fibra óptica, esto explica el porqué ATM soporta velocidades de transmisión que varían desde los 25 MB hasta 622 MB, y se tiene planes de llevar esta velocidad hasta 2.488 GB.

ATM tiene la característica de transmitirse de manera asíncrona, puesto que no utiliza tramas convencionales como en las otras técnicas de redes locales, en lugar de esto, ATM crea celdas de información de tamaño fijo de 53 bytes. 5 bytes son usados por el encabezado y los resultados de esto son la simplificación y la reducción de los costos del hardware, además de una gran flexibilidad.

Un punto muy importante es que ATM aprovecha al máximo la velocidad de un medio físico, puesto que no crea tramas con información de control de errores; la eficiencia de los medios físicos ha llegado a ser bastante confiable, y no es necesario un control de errores tan intensivo. Por otro lado, al tratar de obtener interoperabilidad entre ATM y otras técnicas de red se necesitará de un mecanismo de conversión.

Debido a que ATM puede servir a todo tipo de configuraciones de red (incluso redes mundiales) y para distintos tipos de nodos y aplicaciones, es impredecible el tráfico transmitido y por lo tanto, asíncrono. Gracias a que el tamaño de las celdas es fijo, el retraso en ATM puede calcularse sin problemas. Al tener tan altas velocidades de transmisión pueden implementarse aplicaciones interactivas basadas en multimedia o audio y vídeo garantizados.

Suite del protocolo ATM en el Modelo OSI



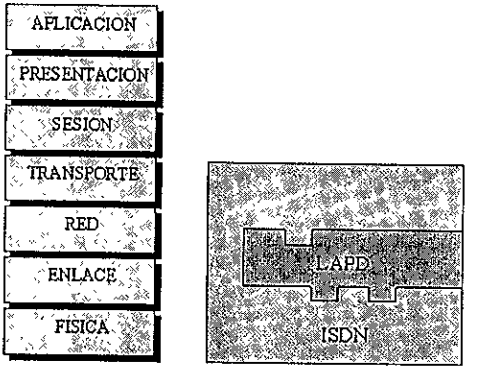
Suite del protocolo ATM en el modelo OSI

ISDN Y B-ISDN

Integrated Services Digital Network (ISDN) es un conjunto de estándares internacionales iniciados por el CCITT ahora ITU, que provee la estandarización para integrar las transmisiones de voz y datos en redes telefónicas digitales. Broadband ISDN se refiere a la especificación ISDN mejorada que ofrece un rango de datos mucho mayor utilizando en medios de comunicación de fibra óptica.

Son comunmente considerados estándares WAN.

Suite del protocolo ISDN en el Modelo OSI



Suite del protocolo ISDN en el modelo OSI

IEEE/ISO 802.X/8802.X Series

En 1985 el Institute of Electrical and Electronic Engineers (IEEE) publicaron una serie de estándares para las capas física y de enlace de datos que fueron adoptados por la ANSI, los cuales han sido revisados por la ISO y se refiere a ellos como el protocolo ISO 8802. Actualmente 12 subcomités técnicos han sido asignados para desarrollar estándares específicos.

Sumario del Protocolo IEEE 802.X

- IEEE 802.2. Define el estándar de la capa de enlace de datos al ser utilizada con implementaciones IEEE 802.3, 802.4, 802.5 y 802.6. IEEE 802.2 agrega varios campos de encabezados (headers) los cuales identifican la capa superior del protocolo que está usando el frame y que proceso de capa de red es la fuente y el destino de los frames.

- IEEE802.3. Ofrece una variedad de opciones en la capa física, incluyendo diferentes modos de señalización (baseband y broadband), tipos de medios de

comunicación, topologías y RATE de datos. Esta implementación está compuesta de tres nombres; el primero representa el rango de datos en mega bits por segundo (Mbps); el segundo indica si la señal es en baseband o broadband y el tercero indica la distancia efectiva.

RIP

RIP (Routing Information Protocol) es un protocolo de vector de distancia, el cual obliga al ruteador a tomar sus decisiones de ruteo basándose únicamente en la distancia (hop counts). Esto es, RIP no considera ninguna otra característica de la red, como congestión, velocidad de la línea, costo, etc. cuando realiza sus decisiones de ruteo.

Cada 30 segundos, las tablas de ruteo son enviadas a la red para que el resto de los ruteadores se mantengan actualizados. Sin embargo, si hay modificaciones en las direcciones antes de que transcurra ese tiempo, RIP también manda las tablas de ruteo.

RIP permite un diámetro máximo de red de 16 (máximo número de "saltos"). Este límite es por los efectos que tendría en la cantidad de tiempo que le tomaría a cada ruteador aprender un nuevo cambio (convergencia).

Algunas implementaciones pueden permitir el uso de RIP extendido, el cual permitiría incrementar el número máximo de saltos hasta 128, lo cual no es recomendable debido a podría haber un importante incremento en la convergencia.

Un ambiente RIP genera cada 30 segundos un tráfico extra de 20 bytes por ruta en cada ruteador. En una topología RIP con 10 ruteadores cada uno con 10 rutas, se agregaría un tráfico extra de 2000 bytes en la red cada 30 segundos (20 bytes * 10 ruteadores * 10 rutas/ruteador).

OSPF

OSPF (Open Shortest Path First) es un protocolo de ruteo de Internet que distribuye información de ruteo entre ruteadores pertenecientes a un solo sistema autónomo. OSPF fue desarrollado por un grupo de ingeniería de Internet, y por lo tanto fue diseñado expresamente para dicho ambiente incluyendo soporte explícito para IP.

OSPF es un protocolo de estado de enlace, el cual permite a cada ruteador recoger información acerca de todas las rutas posibles hacia los destinos, y con esa construir una tabla de ruteo que muestre el mejor camino posible para cada destino dentro de su sistema autónomo. Esto se realiza construyendo una estructura, la cual además de indicar todas las posibles rutas hacia un destino, señala el costo de cada una de ellas.

Todos los ruteadores corren en paralelo el mismo algoritmo. De la base de datos topológica, cada ruteador construye un árbol de rutas cortas teniéndose a él mismo como la raíz. Dicho árbol proporciona la ruta a cada destino en el sistema autónomo. Las tablas de ruteo se construyen tomando la información del árbol de rutas cortas, y consisten de una colección de las mejores rutas hacia un destino en particular.

Para RIP, la mejor ruta es aquella con menores saltos (hops), OSPF es más sofisticado ya que reconoce que en un simple salto no se considera el ancho de banda disponible. Por ejemplo, una ruta con un salto extra por un canal T1 de 1.54 MB, puede ser más eficiente que pasar por una ruta corta pero congestionada. Para OSPF, la mejor ruta es aquella que ofrece menor retardo.

Para reducir el nivel de tráfico, OSPF permite hacer agrupaciones de redes contiguas, las cuales junto con los ruteadores con al menos una interfaz conectada a cualquiera de esas redes, es llamada una área. La topología de una área es invisible para quienes no están en ella; de igual manera los ruteadores que residen dentro de una sola área no conocen la topología externa a ella.

La segmentación de un sistema autónomo en áreas da origen a dos tipos de ruteo; el ruteo intra-área y el ruteo inter-área. En el primer caso, el ruteo de paquetes se realiza entre nodos pertenecientes a la misma área, en el segundo caso el ruteo se lleva a cabo teniendo la fuente y el destino en áreas diferentes.

En el ruteo intra-área, los paquetes se rutean basándose únicamente en la información obtenida dentro de la misma área, la información externa no se necesita y además no puede ser usada. En el ruteo inter-área, la información es ruteada en tres etapas: (1) un ruteador interno (todas las redes directamente conectadas a él se encuentran en la misma área) dirige el paquete a un ruteador de frontera de área (da servicio a más de una área); (2) el ruteador de frontera dirige los paquetes a través del área de espina dorsal (backbone) OSPF hacia la red destino, (3) un ruteador interno transmite el paquete a su destino final.

El backbone OSPF consiste de redes no contenidas dentro de ninguna área, los ruteadores directamente conectados a ella y aquellos ruteadores que pertenecen a múltiples áreas. Los ruteadores de frontera y los de backbone deben ser configurados para reflejar su conectividad del backbone OSPF.

El backbone distribuye la información de ruteo entre las demás áreas. Tiene las propiedades de cualquier área OSPF y su identificación como tal es 0.0.0.0. Los backbone OSPF deben ser contiguos. Dependiendo de la topología de la red y la definición del área es posible construir una topología OSPF en la cual el backbone no sea contiguo. En éste caso se necesitan enlaces virtuales para restaurar la continuidad.

Los enlaces virtuales son componentes del backbone configurados que unen dos ruteadores backbone que tienen una interfaz a una área no-backbone.

La siguiente tabla muestra la clasificación de algunos protocolos:

Protocolos	LAN	WAN	Orientado a Conexión	No orientado a Conexión	Ruteable	No Ruteable
X.25		X	X		X	
TCP/IP	X	X	X		X	
IPX/SPX	X	x	X		X	
Apple Talk	X			X	X	
Frame Relay		X	X		X	
LAN Bridges	X			X		X
SNA		X	X			X

CAPÍTULO 3

ADMINISTRACIÓN AVANZADA DE REDES DE COMPUTADORAS

3 ADMINISTRACIÓN AVANZADA DE REDES DE COMPUTADORAS

Como administración de sistemas se puede entender el mantenimiento y control del uso de las aplicaciones de software. Así, es posible con las herramientas apropiadas tener un reporte del número de usuarios, utilizando las diversas aplicaciones.

Es fácil imaginar las ventajas que ofrece un sistema de este tipo, cuando permite que desde una consola central de administración el operador conozca el momento exacto en que se ejecuta un determinado proceso en la red.

La información que se obtiene proporciona a los programadores y personal de soporte técnico, referencias para la optimización de sistemas de hardware y software a fin de evitar cuellos de botella en el acceso a los datos. También es efectivo como sistema de monitoreo del control de accesos y seguridad.

3.1 ADMINISTRACIÓN DE REDES

Cuando hablamos de redes locales, el concepto de administración comprende los recursos que ofrece el servidor y el acceso al mismo. Bases de datos, espacio en disco, comunicaciones, correo electrónico, control de los nodos, número de licencias de software y su versión, piratería, configuración estándar e impresión son algunos de los servicios que pueden controlarse.

Existe en el mercado un sin número de herramientas para complementar las utilerías *que proporciona el sistema operativo de redes en uso. Generalmente se atienden por* separado, el servidor y los nodos. Para el servidor se pueden controlar elementos como:

- Seguridad.
- Utilización de los recursos.
- Desempeño del hardware.
- Registro de errores.
- Respaldo de la información.

Mientras que para los nodos:

- Inventario de hardware y software.
- Control de los archivos de configuración críticos.
- Control del número de licencias de software permitidas.
- Configuración del hardware.

Cuando aumenta el número de nodos dentro de una red o se interconectan varias de ellas entre sí, las tareas de administración suelen crecer en forma considerable, al igual que la responsabilidad de mantener el sistema en un estado operativo y eficiente, solo correspondería a redes amplias (WAN).

Varias redes conectadas representan nuevos aspectos que administrar y otros ya considerados adquieren mayor relevancia. La seguridad y control de accesos son puntos de vital importancia. La adecuada distribución de los servicios permitirá mantener el tráfico entre los enlaces a un nivel aceptable.

Estos enlaces también deberán ser administrados, pues un funcionamiento intermitente o con bajo nivel de desempeño ocasionará que los usuarios en el otro extremo no tengan acceso a los servicios, con la consiguiente pérdida de productividad.

Dependiendo de la importancia de la información es posible tener enlaces redundantes o canales de comunicación de diferentes velocidades y costos. Un sistema de administración se vuelve necesario para la detección oportuna de problemas con los enlaces y la mediación del tráfico que pasa por cada uno de ellos.

En este ambiente de interconexión existen varios dispositivos susceptibles de ser administrados:

- Sistemas finales: terminales, PC, estaciones de trabajo, minis y mainframes.
- Sistemas intermedios: puentes y ruteadores, multiplexores, modems, repetidores/concentradores.

Los sistemas finales son aquellos dispositivos en donde se produce o consume la información, mientras que los intermedios sirven de enlace entre los finales y otros sistemas.

3.1.1 Esquema general de la administración

El sistema de administración de redes debe cumplir con las cinco tareas definidas por la ISO:

- **Detección de errores.** El sistema debe ser capaz de detectar fallas en el funcionamiento normal de los sistemas administrados.

- **Administración de la configuración y cambios.** El software de administración cuenta con herramientas para la detección automática de cambios en la configuración de los dispositivos.

- **Contabilidad de los recursos.** Es posible generar un reporte del costo del uso de líneas de comunicación.

- **Administración de la seguridad.** Estas herramientas permitirán conocer los intentos ilegales de acceso a los sistemas de cómputo y de comunicaciones.

- **Administración del rendimiento.** La consola de administración tiene herramientas para la graficación del rendimiento de los sistemas de cómputo y de comunicaciones, ofreciendo las facilidades para la asignación de umbrales máximos y mínimos.

Un sistema de administración global de redes se compone básicamente de los siguientes elementos:

- Consola de administración, desde donde se analiza la información recabada y se controla el estado operativo de cada uno de los elementos administrados.
- Software de administración, el cual reside en la consola o estación administradora.
- Programa agente, que se ejecuta en los programas que serán administrados.
- Protocolo de administración, que se encarga del intercambio de información entre el software de administración en la consola y el agente en el dispositivo administrado.

Para la correcta operación del sistema, es preciso evaluar el comportamiento de la

red durante un periodo de tiempo, con el fin de registrarlo en todo tipo de situaciones para tener valores de umbral más certeros.

En otro enfoque del manejo de una red se definen seis disciplinas diferentes asociadas con el manejo de los componentes de una red:

- **Determinación del problema.** La determinación del problema debe identificar que elemento falló, no necesariamente por qué sucedió y debe distinguirse de procedimientos de mantenimiento y servicio. Es el proceso de identificación de fallas de modo que se pueda llamar al distribuidor y organizaciones de servicio indicados.

- **Análisis del desempeño.** Las medidas del tiempo de respuesta y disponibilidad de la red son funciones del análisis del desempeño. Esta categoría puede incluir, en una red de área local que utiliza protocolos CSMA/CD, medidas tales como el número de colisiones y el tráfico.

- **Manejo del problema.** Consiste en el reporte, registro y resolución de impedimentos de la posibilidad del usuario de comunicarse de manera efectiva con un dispositivo destino.

- **Manejo de cambios.** Los cambios en los componentes de la red deben ser registrados, reportados y aprobados a través de este proceso.

- **Manejo de la configuración.** Requiere la creación de una base de datos que contenga un inventario de las características físicas y lógicas pasadas, presentes y futuras de los elementos de la red. La base de datos de la configuración incluirá información sobre terminales y puertos, y la configuración exacta de cada dispositivo de acceso de la red.

- **Manejo de las operaciones.** Éste tiene que ver con la manipulación distante o

remota de diversos dispositivos de la red. Incluirá, pero no estará limitado a: respaldo para el enlace de nuevos dispositivos, suministro de documentación acerca de como realizar ciertas funciones de la red (como transferencias de archivos de un nodo a otro) y aspectos relacionados.

A la lista anterior deben agregarse el respaldo de usuarios, seguridad y planificación.

3.1.2 Funcionamiento de la red

Algunas de las funciones que una red debe cumplir para ofrecer un adecuado servicio a sus usuarios son:

- Conectividad.
- Acceso a dispositivos periféricos.
- Sistema de base de datos común.
- Acceso a software común.
- Servicios con valor agregado.
- Vías de acceso, puentes de enlace y servidores de comunicaciones.

Todos estos servicios llevan implícita la necesidad de contar con respaldo del usuario. También es importante contar con personal capacitado para la solución de problemas, la provisión de documentación y capacitación para el usuario.

A fin de resolver problemas del usuario de manera efectiva, el administrador de la red debe tener a su disposición cuando menos los siguientes documentos de apoyo:

- Mensajes y códigos de todos los sistemas operativos de la red, así como también de todas las máquinas. Además debe disponerse también de los mensajes y códigos de aplicaciones importantes.

- Guías para el operador relacionadas con todo el equipo a disposición de usuario como manuales de terminales, dispositivos de la red, métodos de acceso y cualquier otra información relevante.
- Guía de determinación de problemas de todo el equipo relevante.
- Datos sobre la configuración de la red a fin de determinar si el usuario ha cambiado de alguna forma parámetros referentes a equipo de acceso a la red.

El objetivo fundamental de contar con la documentación adecuada, es poder mantener una red en funcionamiento todo el tiempo. Es función del administrador de la red asegurarse que todo el personal de soporte cuente con la información pertinente para realizar su trabajo.

Otra documentación importante que se necesita para que la red funcione en forma adecuada es la que se proporciona al usuario.

3.1.3 Mantenimiento de la red

El mantenimiento de la red consiste en reparar interrupciones cuando éstas se presentan y evitar que éstas ocurran. Para evitar interrupciones en el servicio, el mantenimiento contempla tareas como la actualización del software del sistema operativo de la red, prueba de cables y componentes activos del sistema de cableado, tarjetas de interfase de red y monitoreo de la carga de trabajo, rendimiento y tiempo de respuesta.

Cuando ocurren interrupciones en el servicio, el objetivo debe de ser devolver el sistema a su operación normal lo más pronto posible. Pero a través del uso de equipo de respaldo también podemos acelerar el tiempo de recuperación, minimizando de esta forma el impacto de la interrupción.

En general, cuando se diseña el sistema total, todo esfuerzo debe estar encaminado

a reducir el número de puntos de falla individuales. Donde éstos sean detectados, si es económicamente viable, debe contarse con equipo de respaldo.

Consideraciones de respaldo

Aunque cuando se diseña la red de área local haciendo un esfuerzo para evitar puntos de falla individuales, no sea posible evitarlos totalmente, en el caso de algunos componentes de la red, bastará con tener unidades operacionalmente redundantes o de repuesto para reemplazarlas rápidamente y lograr la recuperación instantánea del sistema en caso de alguna falla.

Quizá el problema principal con la redundancia o duplicación para minimizar la interrupción del servicio sea el costo asociado con esta estrategia. Si el costo se justifica o no, depende de cuan crítica es la interoperabilidad en la que se basa la empresa en una relación costo/tiempo

Manejo de las interrupciones en el servicio

Al enfrentarnos con interrupciones en el servicio es importante plantear expectativas adecuadas antes que algo suceda. Por lo tanto, se deben anticipar por escrito para los usuarios y fabricantes. A menudo esto se puede hacer por contrato con los fabricantes, pero los usuarios no suelen ser muy pacientes ante las interrupciones de ninguna clase, por lo que es conveniente dejarles claro el procedimiento de operación normal de manejo de problemas.

Es importante que se conserven registros de los orígenes de fallas, ya que las recurrencias de los mismos problemas u otros similares pueden traducirse en componentes fallidos o en un diseño equivocado. Debe estructurarse un documento de captura de errores que permita a las operaciones de la red capturar indicadores de error, pruebas y resultados, y datos relacionados. Los problemas intermitentes son especialmente difíciles de manejar, pero los datos conjuntados con el paso del

tiempo pueden ayudar a elaborar un expediente de éstos problemas. Hasta donde sea posible se debe capacitar a diversas personas de la organización en auxiliares y pruebas de comunicación de manera que ayuden en el diagnóstico de interrupciones.

3.1.4 Herramientas administrativas de mantenimiento y desempeño

Intimamente relacionado con las pruebas de diagnóstico está el equipo necesario para monitorear el nivel de desempeño del sistema. Los datos conjuntados para realizar el monitoreo del desempeño también están muy relacionados con la función de manejo general y también con los aspectos de planificación.

El objetivo principal del monitoreo del desempeño de la red es obtener los datos necesarios para la óptima configuración de la red, esto proporcionará el mayor rendimiento de los datos, y en una red CSMA/CD, esto significa que habrá un número relativamente bajo de colisiones entre paquetes. En un sistema CSMA/CD conmutado por paquetes, cuando menos, la carga y el tamaño de los paquetes afectan el potencial de incidencia de colisiones.

La consecuencia de la carga y el tamaño de los paquetes significa que es necesario conjuntar datos relacionados con paquetes, caracteres, sesiones y canales. Después, los datos conjuntados se pueden utilizar para anticipar el desempeño de una red en condiciones cambiantes. En una red en la que se utiliza más de un canal es posible ubicar servicios y usuarios específicos a esos servicios en el mismo canal con un puente a través de los canales. En consecuencia, es posible optimizar el rendimiento del sistema para diferentes clases de usuarios, aunque los usuarios de los canales cruzados observarán alguna degradación. Con la posibilidad de monitorear el tráfico y el desempeño no es posible tomar las decisiones de manejo necesarias de reconfigurar, expandir o modificar la red.

Existen dispositivos que pueden ayudar al administrador de la red. Algunos de ellos

son relativamente sencillos y están diseñados para probar la continuidad o la existencia de cortos en el cable. Algunos de éstos son dispositivos autónomos, mientras que otros son tarjetas que se colocan en las computadoras y cuando se combinan con el software adecuado, pueden ofrecer información concerniente a índices de colisión en una red Ethernet o bien inspección de cuadros en una red Token Ring.

3.1.5 Planificación

Es importante tener como parte intrínseca del manejo de una red, una función de planificación progresiva tal que se puedan anticipar problemas y oportunidades. Uno de los aspectos principales de la comunicación es la rapidez con la que se puede ampliar la red.

Aunque la red deba ser diseñada con la posibilidad de expansión presente, el índice de expansión dependerá del capital disponible, y de la disponibilidad de personal y productos. La demanda del usuario de servicios en la red en una organización dinámica probablemente superará cualquier expansión planificada.

La necesidad de expansión, modificación o reconfiguración dependerá del tráfico en la red, del rendimiento de la misma y de la disponibilidad del sistema en sitios organizacionales adecuados. No importa cuanta planificación realicen los administradores de redes, *los usuarios siempre tendrán demandas de último minuto* que no fueron anticipadas y quizá sea necesario atenderlas.

En un sentido estricto, la planificación de una red consiste en la anticipación del cambio y la expansión a través del uso de modelos basados en datos referentes a desempeño. La función de planificación debe hacerse una parte intrínseca del manejo de una red para obtener resultados óptimos. El planificador debe servirse de todas las herramientas a su disposición, y de datos concretos o reales, como

estadísticas de uso de terminales de sistemas de computación, nodos y transacciones totales, para representar la red a través de modelos y adquirir sentido de lo que está sucediendo.

Con el tiempo, tales datos pueden sentar las bases de la anticipación por extrapolación. Sin embargo, como sucede con la mayoría de los problemas de predicción tecnológica, gran parte de la planificación debe estar basada en datos aproximados, ya que lo que se necesita es encontrar nuevos usos y nuevos usuarios. Estos elementos pueden estar sujetos sólo a alguna técnica de anticipación objetiva; aunque si se realiza en forma sistemática, entonces puede derivarse algún *conocimiento del proceso de planificación.*

En la mayoría de las organizaciones el concepto de planificación recibe una atención informal, pero mucho de lo que sucede en torno a la planificación en grandes organizaciones es sólo eso. Para que los programas de planificación sean tomados con seriedad es necesario tener no sólo una planificación orientada a metas, sino también planificación de la instalación.

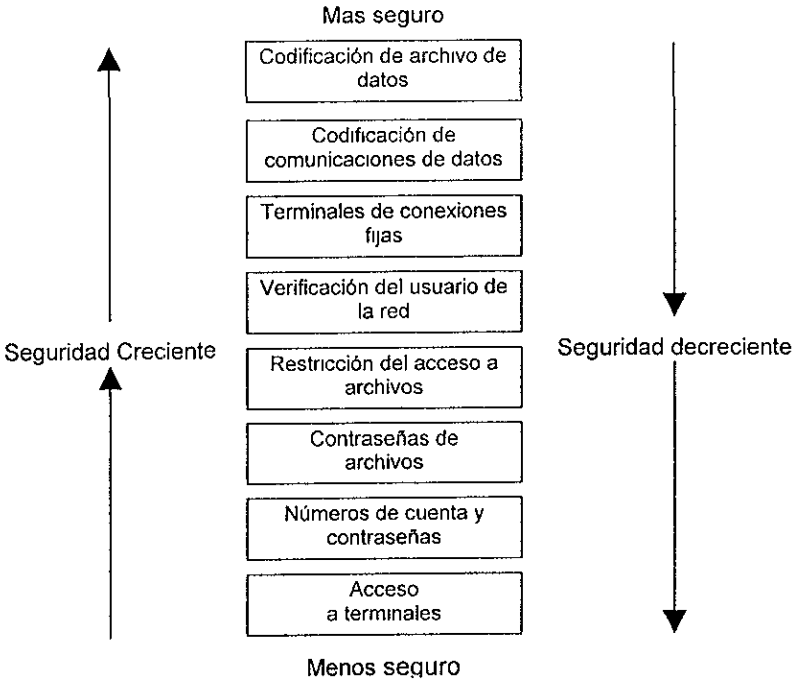
Algunas veces puede ser necesaria la alteración de planes al momento; pero la planificación por si sola, con poco esfuerzo en la instalación de planes, es un ejercicio inútil, poco placentero y excesivamente costoso.

El acierto de la planificación determinará el éxito de la red y su manejo. Cuando menos, el proceso de planificación proporcionará las bases fundamentales para los *encargados de la toma de decisiones en* cualquier punto de la cadena organizacional.

3.1.6 Seguridad en la red

Uno de los objetivos principales de las redes de computadoras, consiste en ofrecer acceso sencillo y conveniente a sistemas de computación dentro de una organización, y ese uso muy sencillo puede entrar en conflicto algunas veces con necesidades de seguridad. Por lo tanto, el sistema de seguridad de la red debe tomar medidas para identificar a usuarios legítimos con fines autorizados al mismo tiempo de negar el acceso o uso no autorizados de datos importantes.

Podríamos concebir la seguridad como una serie de estratos donde el de más arriba representa el nivel más alto de seguridad y el de más abajo el menor nivel de seguridad Esto se ilustra en la siguiente figura:



Como uno de los objetivos primarios de una red es la conectividad, la óptima instalación de un sistema altamente conectivo tiende a frustrar algunos métodos de seguridad y control. Los diversos estratos de seguridad están diseñados para impedir el acceso no autorizado y en esto está implícito un aspecto de seguridad importante: el costo de conservarla o de permitir una brecha en el sistema de seguridad.

La seguridad es importante, y los problemas de seguridad deben ser atendidos sin llegar a una preocupación excesiva por los mismos.

3.1.7 Administración de una red en perspectiva

El manejo de una red consiste en mucho más que tender cables y anexar conectores. En todas las actividades mencionadas, existe una demanda implícita de la estructura política inherente en cualquier organización, y esa estructura política impedirá o alentará la instalación de la red y su manejo.

Cuando una red opera debidamente será transparente para el usuario. Éste no debe saber que está ahí y tampoco debe preocuparse por el mecanismo de transporte que se utiliza para llevar datos de un punto a otro.

Es responsabilidad de la administración de la red anticipar necesidades, no sólo a partir de las exigencias de algunos usuarios, sino tomando en cuenta también las necesidades de los usuarios potenciales.

3.2 DISTRIBUCIÓN DE SOFTWARE

El creciente uso de las redes de computadoras ha permitido que se desarrolle una gran variedad de aplicaciones que permiten utilizar de manera más eficiente y eficaz los recursos que se tienen, esto a hecho que el Administrador de la Red deba tener presente lo referente al Software que se utiliza en ella, así como la distribución del mismo.

Muchos de los productos comerciales que existen actualmente, están configurados para una posible instalación en red, lo que facilita al Administrador de Red tener la posibilidad de un control en la distribución del Software, este tipo de software generalmente se instala en el servidor de una red mediante la opción que se conoce como **instalación administrativa**.

La instalación administrativa da la oportunidad de que el software pueda ser instalado por los usuarios de dos formas distintas, en ambas el inicio del proceso consiste en que el usuario se conecta a los recursos de la red, propiamente al servidor donde se encuentra instalado el software para su distribución, de ahí selecciona la instalación del producto que desea y durante el proceso de instalación elige una de dos opciones posibles.

- La primera opción permite que el software se instale para que pueda ser ejecutado desde el servidor, lo que implica que solamente algunos archivos de inicialización serán copiados a la estación de trabajo con el fin de que éstos puedan comenzar con la ejecución del software cuando éste se requiera. La ventaja de éste tipo de instalación radica en economizar los recursos de las estaciones de trabajo, sobre todo, en lo que se refiere al espacio de almacenamiento en disco que requieren algunas aplicaciones. Esta opción es muy útil cuando las estaciones de trabajo cuentan con pocos recursos y no es posible dotarlas de mayor capacidad de almacenamiento.

- La segunda opción, realiza una instalación completa del producto desde el servidor al disco duro de la estación de trabajo, esto significa que el usuario hace uso del servidor únicamente para instalar el software que necesita y una vez instalado éste se ejecutará en la misma estación de trabajo. La ventaja de esta opción es que no se necesita que el servidor esté activo para poder ejecutar la aplicación.

Existe software que no permite realizar una instalación administrativa en el servidor, con lo cual no se puede hacer la distribución de software como se mencionó anteriormente, por lo tanto dicha distribución se lleva a cabo colocando los discos de instalación en subdirectorios y permitiendo que los usuarios tengan acceso a ellos para que puedan copiar su contenido y realizar la instalación por si mismos. Para emplear este medio de distribución de software se debe tener cuidado en permitir el acceso únicamente a los usuarios a los que se va a distribuir el software.

Con el auge creciente de la red Internet, se han desarrollado otros mecanismos para realizar la distribución del software, uno de ellos, el más comúnmente utilizado consiste en colocar en una página del web de la compañía, el software que se desea distribuir, éste generalmente se encuentra compactado en un único archivo el cual es copiado al destinatario que se encuentra consultando el web y una vez que el usuario tiene el archivo procede a ejecutarlo para poder realizar la instalación, la ventaja de utilizar las herramientas de Internet dentro de una red corporativa, es dar una presentación más amigable al usuario y hacer más agradable su trabajo, lo cual representa un incremento en la productividad y el uso creciente de nuevas tecnologías.

Por último, independientemente de la forma que se elija para distribuir el software dentro de una red, es importante no olvidar que se debe tener presente la situación de las licencias, ya que no se debe caer en la situación de otorgarle a los usuarios la oportunidad de utilizar todo el software de la red, si no se cuenta con las licencias respectivas, de lo contrario se está cometiendo una violación a los Derechos de

Autor, lo cual puede traer consecuencias graves, no sólo para el personal encargado de la administración de la red, si no para toda la organización.

La distribución de software es una de las funciones más delicadas del administrador de redes, independientemente del tipo de distribución que se haga es importante considerar que el software siempre debe estar disponible a los usuarios de la red, sobre todo cuando éste se está ejecutando desde el servidor y no se puede permitir que no esté disponible.

3.3 CONTROL DE INVENTARIOS

Cuando una organización tiene cientos o miles de nodos en una red de cómputo, los administradores deben saber el total de componentes de hardware y aplicaciones de software que se encuentran operando.

La dificultad por mantener el control del inventario, tanto del hardware como del software son tareas que deben llevarse a cabo de forma separada.

3.3.1 Software

Para crear un inventario de software existen algunos programas de computadora que buscan en los directorios del disco duro de una estación de trabajo la existencia del software instalado, tratando de emparejar los archivos ejecutables de las aplicaciones a su Base de Datos de productos conocidos, generalmente ésta base de datos puede ser ampliada para incluir aplicaciones propias, así como nuevas aplicaciones que aparezcan en el futuro.

Si la computadora se encuentra conectada a una red LAN, la información puede obtenerse aprovechando el proceso de login al sistema y almacenarla en el servidor de archivos. Al tratarse de una red empresarial (Interconexión de LANs) un servidor principal puede contener información de varios servidores de la red, por otra parte para las computadoras que se encuentran aisladas, la información en ellas se almacena en discos añadiéndose posteriormente al inventario global.

Existe también la posibilidad de que éstos programas detecten el número de instalaciones efectivas de cada aplicación y notifiquen si éste número supera las licencias disponibles, lo cual indicaría la cantidad de licencias adicionales que se requieren comprar, en lugar de adquirir una para cada usuario potencial.

En forma general ésta es la forma en que trabajan la mayoría de los programas para el control de inventarios, con el fin de determinar el software que se encuentra instalado en una organización.

Aunado a lo anterior, algunas de las aplicaciones para redes más comunes han sido dotadas de instrumentos que permiten controlar su uso, dando la posibilidad de ser instaladas en un servidor de red y tienen dos opciones para el manejo de las licencias:

- **Licencia "Por Servidor".** Consiste en que al software instalado se le indica el número de usuarios que pueden conectarse de manera concurrente para poder hacer uso del producto, esto implica que el siguiente usuario que desee conectarse al servidor será rechazado y automáticamente recibirá un mensaje indicando que se ha excedido el número máximo de usuarios permitidos.

- **Licencia "Por Seat" (Por Equipo).** Transfiere las licencias a los usuarios, lo que permite que cualquier computadora de la red que tenga una licencia del producto podrá hacer uso del software instalado, el inconveniente es que se requiere comprar una licencia para cada estación de trabajo, no importando el número máximo de usuarios que pueden estar conectados al servidor al mismo tiempo.

Ésta es una forma sencilla en la cual se puede mantener un control del uso del software y controlar el inventario, la decisión del tipo de opción que se elija dependerá de las necesidades especificas de cada organización.

Como ejemplo podemos considerar a una organización que tiene 100 empleados los cuales hacen uso de los recursos de la red, la cual consta de 2 servidores.

Si la opción que se elige es *Por Seat*, todos los empleados pueden acceder a los recursos de todos los servidores. Si la opción elegida es *Por Servidor*, el administrado debe determinar el número máximo de conexiones concurrentes para

poder distribuir las 100 licencias y poder garantizar el acceso a todos los usuarios, dependiendo de la demanda es posible que se pueda requerir la compra de más licencias.

Por el contrario, si los usuarios rara vez se conectan al servidor y cuando lo hacen es para realizar funciones de transferencia de archivos e impresión, resultaría demasiado costoso el que cada usuario tuviera una licencia, lo ideal sería adquirir solo algunas de ellas y que los usuarios pudieran conectarse concurrentemente para hacer uso de ellas.

El costo de cualquiera de las dos opciones, dependerá de la situación muy particular de cada caso, existirán algunos casos donde resulte más económica la opción *Por Seat* y en otros la opción *Por Servidor*.

3.3.2 Hardware

En cuanto al inventario de hardware la situación es más difícil, el software de inventario de hardware interroga al BIOS de la computadora y a los subsistemas para proveer informes valiosos de la memoria instalada, espacio disponible en el disco duro y otros recursos, desafortunadamente solo hay unas cuantas cosas que puede hacer en cuanto a la búsqueda de controladores especiales en memoria, para reportar lo que pueda estar pasando en el bus del sistema.

Ante esta situación, los programa para el control de inventario de hardware se verán beneficiados con el paso evolutivo de los productos Plug and Play (PnP ó conectar y usar), los cuales podrán proporcionar más y mejores informes de los recursos instalados en un sistema y de su configuración, sin embargo, no ayudaran a catalogar la gran inversión que se tenga en hardware ya instalado, y sin la ayuda de productos compatibles con PnP, es difícil que un programa de inventario de hardware identifique los adaptadores de redes, las tarjetas de video y otros

dispositivos del sistema.

A continuación se presentan las características de algunos de los productos disponibles para el control del Inventario de hardware y software:

Invent 2.0

Éste es un producto desarrollado por una empresa española denominada "Panda Software" y realiza las siguientes funciones:

- Un inventario automático de hardware y software disponible.
- Reconoce las aplicaciones instaladas en cada puesto.
- Análisis exhaustivo de la configuración hardware de cada computadora.
- Realiza automáticamente el almacenamiento de datos, sin intervención del usuario.
- Almacena información tanto de computadoras conectadas a una red como de computadoras aisladas.
- Alerta sobre las aplicaciones instaladas carentes de licencias.

Microsoft Systems Management Server 1.2

Otro producto, que presenta también grandes ventajas en el control del inventario (hardware y software), así como en la distribución del software, es el desarrollado por la empresa Microsoft y es el Systems Management Server.

El Systems Management Server es un producto que centraliza la administración y solución de problemas relacionados con el control de inventario y la distribución de software, ya sea que se trate de una organización pequeña o una red corporativa, dentro de sus principales características se encuentra:

- Identificar y mantener un inventario de PCs y Servidores.
- Instalar el agente de administración en los clientes y a todas las máquinas de una red.

- Mantener un inventario detallado del hardware y software, incluyendo la historia de los cambios que se hayan efectuado.
- Identificar el software instalado, basándose en una extensa base de datos.
- Permitir al administrador de la red distribuir software a las estaciones de trabajo.
- Instalar software en servidores específicos para ser compartido a usuarios basados en Windows.

3.4 RESPALDO Y RECUPERACIÓN

Debido a que los servidores de red almacenan datos muy importantes para las compañías, es necesario contar con sistemas de respaldo. Uno de los mayores problemas con que se encuentra el usuario es la inmensa cantidad de datos generados por programas, documentos, imágenes, copias de seguridad etc.

Los dispositivos de almacenamiento son tan importantes para un administrador que se han convertido en uno de los elementos que ha tenido mayor evolución en la historia de la informática.

Para elegir un sistema de respaldo hay que tener claro que tipo de información tenemos y que tan importante es para poder elegir el tipo de almacenamiento.

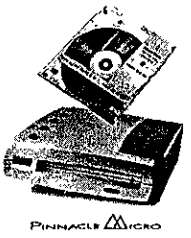
La forma de respaldo mas usada son las copias de seguridad y almacenamiento periódico de datos importantes que pueda contener nuestro servidor. Pero cuando se trabajan con datos vitales esta práctica es imprecisa y tediosa.

Cuando se maneja poca información podemos optar por soluciones como las unidades de cinta, en donde se pueden citar dos tecnologías para las unidades de cinta: *grabación por muestreo lineal* (QIC Quarter Inch Cartridge) que son unidades compatibles con el sistema de un cuarto de pulgada siendo muy comunes por su bajo costo y confiabilidad, su capacidad es de 600 Mb. Por otro lado se tienen las de *grabación por muestreo helicoidal* (DAT) que son unidades de cinta magnética digital de 4mm y 8mm, para el registro sonoro las compañías con redes más grandes que requieren una mayor capacidad de respaldo y con frecuencia prefieren utilizarlas, estas unidades pueden almacenar hasta 8Gb de datos comprimidos, se utiliza un sistema parecido al de los videos, con tambor giratorio donde se instalan las cabezas al mismo tiempo que la cinta gira en dirección contraria, con esto su velocidad es menor que las QIC pero la densidad es mayor.

Últimamente ha salido al mercado una nueva especificación denominada Travan que permite grabar hasta 1.6 Gb con el sistema QIC 3020. Gracias a este nuevo formato de cinta se prevé alcanzar los 12 Gb en unidades especiales.

A pesar de estos avances que proporcionan una considerable capacidad de almacenamiento, lo cierto es que presenta algunos inconvenientes: baja velocidad de acceso y recuperación de datos de forma secuencial. Otro problema con estas cintas magnéticas es que no son confiables a largo plazo, ya que cualquier soporte magnético podría perder datos con el tiempo. Para realizar copias de seguridad confiables durante largo tiempo es mejor tomar en cuenta las unidades Magneto-ópticas (MO) o las nuevas unidades de cambio de fase (PC Phase Change). Este tipo de dispositivos garantizan una confiabilidad en la lectura y escritura de los datos y conservan durante décadas las propiedades de la grabación gracias a sus características y a la protección del cartucho que rodea los discos. El inconveniente de las unidades de cambio de fase es que, aun siendo más rápidas que las cintas, son bastante lentas comparadas con un disco duro y más caras que las cintas. Las dos tecnologías MO y PC se dirigen a usuarios que necesitan almacenar datos durante largo tiempo y no exijan mucha velocidad de acceso. Este equipo es generalmente adquirido para servidores de red.

Discos Magneto-Opticos (MO)



Los discos Magneto Opticos utilizan una combinación entre la tecnología láser y los principios magnéticos empleados en los discos duros En los discos magneto ópticos la grabación de los datos se efectúa aplicando un campo magnético en una amplia superficie del disco. Para que las partículas magnéticas de la superficie del disco se orienten según el campo aplicado, se utiliza el láser que aumenta la temperatura en los puntos que deseamos orientar.

Para la lectura de los datos se utiliza el llamado efecto Kerr, que describe los efectos del magnetismo en el plano de polarización de la luz de un rayo láser. De esta manera podemos distinguir si un bit determinado en la superficie del disco está a cero o a uno dependiendo de la luz de láser reflejada por ese punto.

Una unidad MO (Magneto-óptica) puede tener una velocidad de transferencia de unos 2 Mb por segundo y un tiempo medio de acceso de aproximadamente 35 milisegundos.

Unidades de Cambio de Fase

Esta nueva tecnología de cambio de fase cuenta con un sistema de lectura-escritura puramente óptico, basado en las propiedades de ciertos cristales. Los discos que se utilizan en este tipo de tecnología están recubiertos por una capa de material formado por una serie de cristales de estructura regular.

Calentando rápidamente una pequeña parte de la superficie del disco mediante un rayo láser, se provoca la ruptura de la estructura de los cristales convirtiéndolos en material reflectante pero amorfo, de esta manera podemos escribir ceros y unos en la superficie del disco destruyendo o manteniendo intacta la estructura de los cristales.

Utilizando el láser a menor intensidad se pueden leer los datos contenidos en el disco mediante un rayo láser, siendo el mismo proceso que emplean los lectores de CD-ROM, ya que los cristales y el material amorfo reflejan la luz del láser de forma distinta.

La diferencia con los CD-ROM es que los discos de cambio de fase pueden volver a escribirse hasta un millón de veces.

Estas unidades permiten almacenar hasta 650 Mb en un solo disco y son capaces de

leer discos compactos, lo que permite amortizar aún más la inversión. Esta tecnología a sido desarrollada por la empresa Matsushita, que comercializa ya versiones de estos dispositivos a través de las firma Panasonic.

Dispositivos portátiles

Los dispositivos como Iomega Bernoulli, el mini-disc de Sony, las unidades Zip y EZ135 de Iomega y SysQuest resuelven los problemas de incompatibilidad en los formatos de cintas y discos con que se venían enfrentando los administradores, ya que con estos dispositivos portátiles podemos recuperar información en cualquier momento.

Este tipo de dispositivos utiliza una tecnología similar a las de los discos duros tradicionales, pero separado el disco de las cabezas de lectura y grabación. Con estas unidades es posible alcanzar características de un disco duro normal, sin olvidar las ventajas de trabajar con dispositivos removibles y transportables.

Respecto a la evolución de los discos para almacenamiento de datos se tienen los siguientes datos:

Discos de metal

Las unidades Winchester, son unidades de 14 pulgadas en envases sellados, y por su tamaño para máquinas grandes. Sus capacidades eran de 30 Mb.

Otros discos de igual capacidad estaban empacados en cartuchos removibles o paquetes de discos que contenían uno o dos discos montados en un mismo eje, con capacidades entre 30 y 300 Mb.

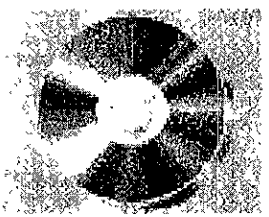
Los discos rígidos más pequeños de 5.25, 8 y 9 pulgadas se utilizaban para almacenar en máquinas más pequeñas con capacidades de 40, 80 y 120 Mb.

Ahora se tienen unidades rígidas de 5.25 y 3.5 pulgadas con capacidades entre 120 Mb y 4 Gb y en arreglos de discos se llegan a tener de 1 a 2 TB.

Discos Flexibles

El almacenamiento en estos discos flexibles era mejor, pero muy fácilmente podían dañarse con algo de polvo, si se doblaban, etc. Se realizaron mejoras y aparecieron los discos más comunes de hoy en día, cuya medida es de 3.5 pulgadas, y su funda es de plástico rígido con protección metálica para la zona de lectura/escritura. Pueden almacenar 720 Kb, 1.4 Mb y 2.8 Mb.

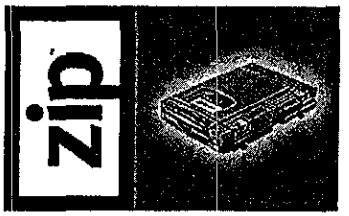
Discos Compactos



La distribución masiva de programas y datos es una de las necesidades en el almacenamiento de la información. En la actualidad la única alternativa adoptada para la distribución de datos y software en discos compactos son los CD-ROM, con capacidades de hasta 650 Mb y debido a su estructura, las unidades de CD-ROM (unidades de solo lectura) no existe problema de alterar la información, solo pueden leerse. Existen unidades para grabar información pero aún son costosas.

Este soporte se ha convertido en el vehículo ideal para la distribución de aplicaciones, y aunque resulta más lento que la mayoría de los dispositivos anteriores, actualmente es la opción más extendida por su bajo precio.

Unidades Zip Drive



Lo último en medios de respaldo son las unidades Zip Drive que almacenan en un disco de 3.5 pulgadas 100Mb (equivalente a 70 discos de 1.4 Mb), unidades para respaldar en cartucho de 3.2 Gb (parecidos a los audio casettes pero más gruesos). El drive Zip ocupa sus propios discos Zip, los cuales tienen mayor capacidad, desempeño y durabilidad que los discos flexibles. Los discos Zip son muy resistentes, estos pueden soportar un stock de 1000 Gs (una caída de 8 pies), sin ningún daño a los datos, con una vida de estante de 10 años. Tienen bajo costo y es fácil de utilizar y de transportar debido a sus pequeñas dimensiones y su peso de tan solo una libra, tiene una gran velocidad de acceso como si se utilizara el disco duro, inclusive ejecutar programas desde la unidad.

Para ser utilizado, en su versión para puerto paralelo, el drive Zip requiere de una computadora PC 386 compatible o superior, con puerto paralelo y sistemas operativos Msdos y/o Win 3.1 o posterior. En la versión SCSI, para ser utilizado en Macintoch, el drive requiere de sistema operativo 6.05 o posteriores y puerto SCSI de 25 pines

A continuación se presenta una tabla comparativa de los dispositivos de respaldo:

Tipo	Descripción	Capacidad	Ventajas	Desventajas
Disco Compacto Regrabable (CD-R)	Tecnología de un CD que utiliza un láser para leer y grabar los CD-ROMS	650Mb	Vida útil más larga; puede leer los datos directo del medio de almacenamiento	Alto costo de la unidad, no puede ser sobregrabado; baja capacidad.
Cinta de audio digital (DAT)	Cinta magnética de 4mm, mediante la tecnología que utiliza el escaneo hélico como método de grabación.	2GB a 4GB	Alta capacidad; velocidad, costos bajos, tanto del medio como de la unidad.	No tiene la velocidad ni la capacidad de las cintas de 8mm DLT.
Cinta digital lineal (DLT)	En forma simultánea, graba y lee múltiples canales.	6GB a 40GB	Alta capacidad; velocidad.	Alto costo de la unidad.
Escaneo hélico de 8mm	Tecnología que utiliza el escaneo hélico como método de grabación.	2.5GB a 7GB	No necesita software extra; costo bajo del drive; lee los datos directo del medio.	Alto costo de la unidad, baja capacidad.
Cartucho de cuarto de pulgada (QIC)	Tecnología de cinta magnética que utiliza la grabación en forma de serpentín como método.	60Mb a 5GB	Alta capacidad, bajo costo del medio.	Alto costo

Algunas compañías pueden invertir en un Sistema de Administración de Almacenamiento (SMS). Estos sistemas almacenan en medios más baratos y de manera automática los archivos que no se usan y luego los recuperan cuando son necesarios, esta técnica es llamada *Administración Jerárquica de Almacenamiento* (HSM). Todo esto es transparente al usuario.

El software de administración de respaldo programa en un calendario y monitorea todos los trabajos de respaldo a través de la red del software, permite seguir la pista de cada localidad de cinta y notificar al administrador cuando las cintas tienen que ser cambiadas. La mayoría de los programas marcan los archivos con la hora y la fecha para tener un mejor control.

Algunos de estos softwares de respaldo son:

BackupNet

Actualmente en su versión 1.5 cuenta con las siguientes características:

- Incluye filtros, respaldos, apagado y actualizaciones automáticas.
- Notificación de errores durante el respaldo a través de email o el visualizador de eventos.
- Los filtros proporcionan facilidad en los respaldos.
- Restablece directorios en forma jerárquica.

ServerStor

Cuenta con las siguientes características:

- Tareas de respaldo automáticas para ser ejecutadas cada día, semana, hora específica.
- Reduce el tiempo requerido para la creación de un respaldo.
- Automatiza totalmente la recuperación en caso de siniestro.
- Interfaz por medio de ventanas fácil de usar.
- Compatibilidad con cintas DAT 4mm, QIC.

ImageStor y FileStor

Software de imagen y respaldo.

- Captura una imagen completa del disco duro y pone el duplicado en un medio de almacenamiento secundario.
- Permite crear respaldos completos, increméntales o de archivos seleccionados y los restaura desde o hacia cintas de respaldo.

La información que se encuentra en los servidores de una red puede tener niveles de

importancia: datos vitales, datos irrecuperables, datos fácilmente recuperables, datos desechables. Dependiendo de estos niveles es el respaldo y el almacenamiento que necesitamos, y esos niveles de seguridad sólo los puede fijar el administrador de la red en conjunto con directivos de la empresa.

3.4.1 Almacenamiento en red

Para los administradores de red es de gran importancia la tolerancia a fallas. Si falla una unidad de discos de un servidor de archivos, deben estar seguros de que los datos no se perderán. Una solución que cada vez es más común se conoce como Arreglos Redundantes de Discos Baratos (RAID, Redundant Arrays of Inexpensive Disks).

Un arreglo de discos puede incrementar el rendimiento, aumentar la capacidad de almacenamiento y proporcionar mayores niveles de tolerancia de fallas. El arreglo de discos es simplemente una serie de discos duros que están direccionados lógicamente como un solo disco más grande. Las ventajas de un diseño así son:

- Velocidades de transferencia efectivas de alta velocidad.
- Capacidad para manejar múltiples requerimientos.
- Incremento en la capacidad de almacenamiento.
- Flexibilidad en la configuración.
- Alta seguridad.

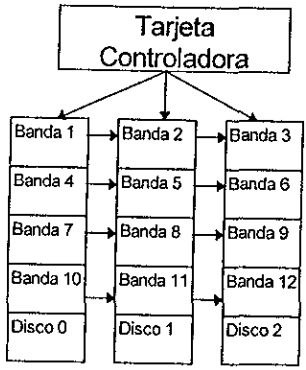
En ambiente de red, el servidor debe procesar múltiples archivos y requerimientos de datos mucho más rápido y con un más alto grado de confiabilidad.

Muchos discos físicos se agrupan para componer un volumen lógico. Este tipo de configuración lógica es realizado con la configuración del Sistema.

La tecnología de arreglo de discos distribuye los datos a lo largo de la serie de discos que han sido configurados como un solo volumen lógico. Esta distribución de los datos hace posible el acceso de datos mucho más rápido. Esto también permite que los arreglos de discos respondan a múltiples requerimientos simultáneamente.

Raid 0

- Extención de datos a través de múltiples discos
- Menor Latencia
- Menor costo
- Mejora el rendimiento.



En el RAID 0 un archivo es dividido en segmentos y escrito a través de múltiples discos. Esto mejora la latencia del disco (la cantidad de tiempo que la cabeza del disco tiene que esperar para que el sector objetivo se mueva bajo la cabeza).

Ventajas

Permite accesar más de un disco a la vez, logrando una tasa de transferencia más elevada y un rápido tiempo de acceso. Por no utilizar espacio en información redundante, el costo de Megabyte es menor.

Limitaciones

La división de datos es más rápida que las escrituras convencionales en un disco sencillo sin embargo no hay protección de fallas si un disco fallara. Si el disco 1 fallara se perdería el archivo completo y no podría escribirse información adicional en los discos.

En tanto mas drives se añaden al arreglo, el potencial de falla se incrementa. Por lo

tanto un diseño con RAID 0 no es deseable para ambientes que requieran tolerancia a fallas.

Ambientes donde se realiza:

Es una buena opción en sistemas donde sea más importante el rendimiento que la seguridad de los datos. Es decir ambientes que puedan soportar una pérdida de tiempo de operación para poder reemplazar el disco que falle y reponer toda la información.

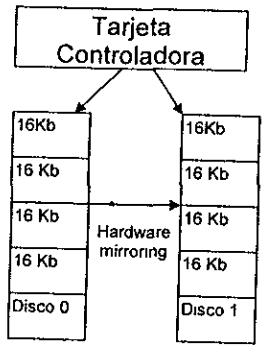
Raid 1

Espejo de Hardware

- Usa 50% de los datos
- Requiere un número par de discos
- Hace espejo del disco completo
- Divide búsquedas

Espejo de Software

- Basado en la partición
- Menos eficiente
- Puede ser más difícil la recuperación de una falla



En el espejo de hardware si un disco falla, el espejo del disco proporciona una copia de los archivos y la operación del sistema no se interrumpe.

El espejo de software a sido implementado actualmente por Ms Windows NT Server, Novell Netware 3.x,4.x y Bayan Vines 4.x 5.x. El espejo de software le da una carga adicional al procesamiento de CPU principal por lo que a veces es menos eficiente que el de hardware.

Ventajas

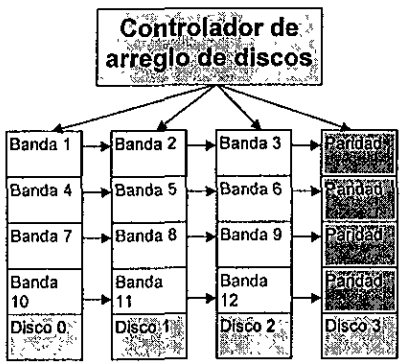
Se protege la información en caso de falla tanto del disco como del controlador (en

caso de dúplex), ya que si un disco suspende su operación el otro continua disponible. De este modo se evita la pérdida de información y las interrupciones del sistema debido a fallas de discos.

Ambientes donde se realiza

Está diseñado para sistemas donde la disponibilidad de la información es esencial y su reemplazo resultaría difícil y costoso. Típico en escrituras aleatorias pequeñas con tolerancia a fallas. El problema de este tipo de arreglos es el costo que implica duplicar los discos.

En el **RAID 2** se realiza la corrección de errores para proporcionar tolerancia a fallas. Si un disco falla puede reconstruirse a partir de los datos de corrección de errores dispersos en varios discos.



En el **RAID 3** la corrección de errores se incluye en el hardware controlador de unidades así como en una unidad de paridad. Los datos se transfieren al conjunto de unidades de disco, byte por byte; se calcula la paridad y se almacena en la unidad dedicada a la paridad. Se usa un solo controlador de unidades para leer y escribir de manera que solamente se pueda escribir en una unidad de disco del conjunto a la

vez. El RAID 3 es el más adecuado para el manejo de grandes bloques de datos.

Ventajas

Proporciona una alta disponibilidad del arreglo, asi como una tasa de transferencia elevada, mejorando de ese modo el rendimiento del sistema.

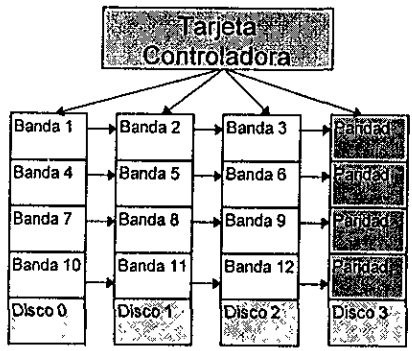
Ambientes donde se realiza

Es típico para transferencia larga de datos en forma serial, tal como aplicaciones de imágenes o vídeo.

Raid 4

Protección de Datos por Hardware

- Disco dedicado a paridad
- El disco de paridad tiende a tener cuellos de botella.
- Tolerante a fallas

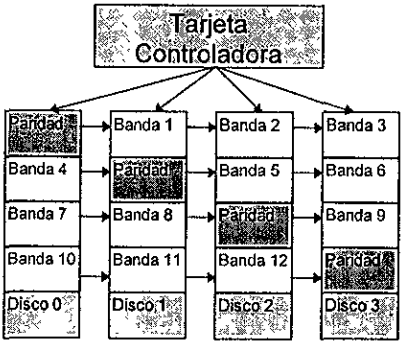


Este nivel es similar al RAID 3 salvo que ofrece mejor rendimiento con menos tolerancia a fallas. La lectura y escritura pueden llevarse a cabo en forma independiente en cualquiera de las unidades del conjunto. Una desventaja del RAID 4 es que la información de paridad debe actualizarse en cada escritura a cada unidad.

Raid 5

Protección de Datos Distribuidos

- Paridad Dividida
- Tolerancia a fallas



En este nivel de RAID dispersa datos e información de paridad por todas las unidades del conjunto. No existe un sólo disco dedicado a la paridad que realice la revisión de errores. El rendimiento se mejora porque es posible tener lecturas y escrituras de datos simultáneamente

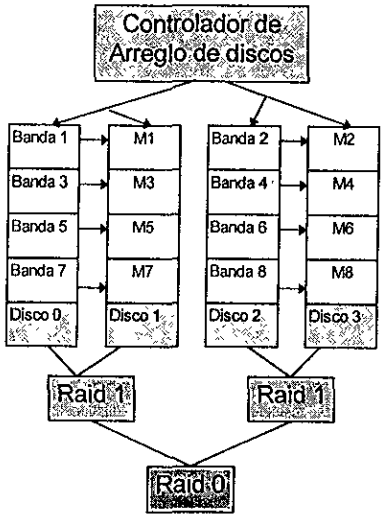
Ventajas

Es el esquema de protección de información más usado comúnmente, ya que proporciona un buen rendimiento general con una mínima pérdida de capacidad. Además el sistema tiene suficiente redundancia para ser tolerante a fallas.

Ambientes donde se realiza

Es recomendable para aplicaciones intensas de entrada/salida y de lectura/escritura, tal como procesamiento de transacciones.

RAID 10



Es un nivel de arreglo de discos, donde la información se distribuye en bloques como en RAID-0 y adicionalmente, cada disco se duplica como RAID-1, creando un segundo nivel de arreglo. Se conoce como "striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utiliza el 50% de la capacidad para información de control.

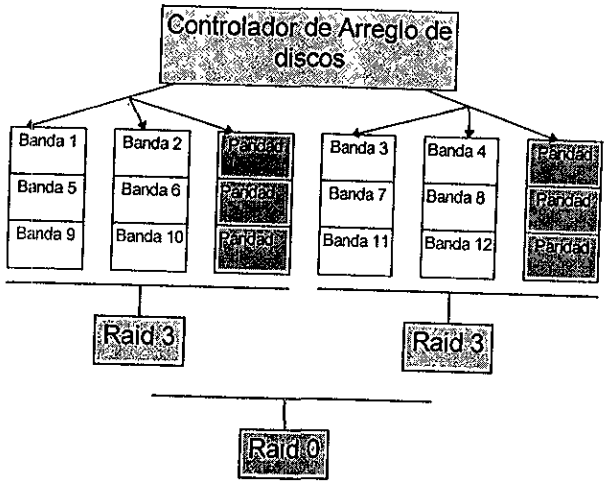
Ventajas

Este nivel ofrece un 100% de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante.

Ambientes donde se realiza

Ideal para sistemas de misión crítica donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escrituras aleatorias pequeñas.

RAID 30



Se conoce también como "striping de arreglos de paridad dedicada". La información es distribuida a través de los discos, como en RAID-0, y utiliza paridad dedicada, como RAID-3 en un segundo canal. Requiere mínimo seis discos.

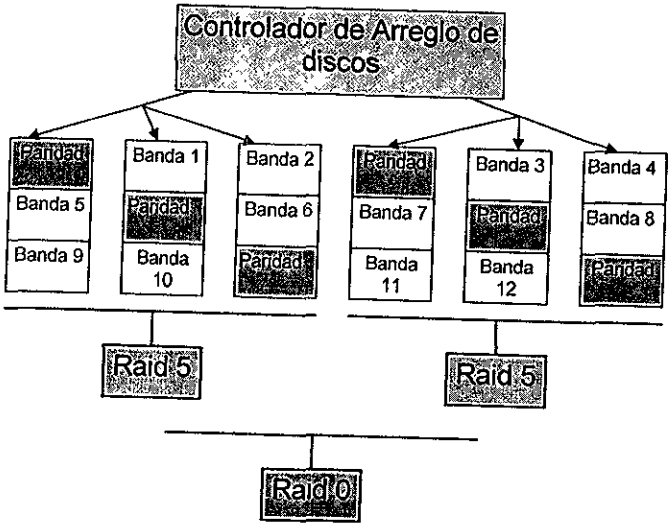
Ventajas

Proporciona una alta confiabilidad, igual que el RAID-10, ya que también es capaz de tolerar dos fallas físicas de discos en canales diferentes, manteniendo la información disponible.

Ambientes donde se realiza

RAID-30 es el mejor para aplicaciones no interactivas, tal como señales de vídeo, gráficos e imágenes que procesan secuencialmente grandes archivos y requieren alta velocidad y disponibilidad.

RAID 50



Con un nivel de RAID-50, la información se reparte en los discos y se usa paridad distribuida, por eso se conoce como "striping de arreglos de paridad distribuida". Se requieren mínimo seis discos.

Ventajas

Se logra confiabilidad de la información, un buen rendimiento en general y además soporta grandes volúmenes de datos. Igualmente, si dos discos sufren fallas físicas en diferentes canales, la información no se pierde.

Ambientes donde se realiza

Es ideal para aplicaciones que requieran un almacenamiento altamente confiable, una elevada tasa de lectura y un buen rendimiento en la transferencia de datos. A este nivel se encuentran aplicaciones de oficina con muchos usuarios accesando pequeños archivos, al igual que procesamiento de transacciones.

Actualmente los servidores soportan mas de un nivel de RAID, con los adaptadores

adecuados, a continuación se mencionan algunos:

Adaptador HP NetRAID para HP NetServer

Diseñado para garantizar la más alta disponibilidad en ambientes de red, es flexible y fácil de administrar.

Características:

- Alto rendimiento y máximo tiempo de operación.
- Adaptador central PCI Ultra SCSI de tres canales con capacidad de control **RAID.**
- Utiliza un ASIC para mejorar el rendimiento del sistema y permite el almacenamiento interno y externo para máxima capacidad.
- Un soporte para siete niveles **RAID (0, 1, 3, 5, 10, 30, 50)** le brinda la flexibilidad necesaria para encontrar el mejor equilibrio en cuanto a costos, rendimiento y disponibilidad.
- Resultados flexibles y confiables.
- Fácil de configurar y administrar.

Sistema Alpha Server 1000 4/266

Características de Disponibilidad:

- Reinicialización automática.
- Manejo térmico.
- Administración remota del sistema.
- **RAID (0, 1, 3, 5, 10, 30, 50).**
- Cambio instantáneo de disco.
- Doble backplane SCSI.
- Memoria de respaldo.
- Memoria ECC.
- Caché ECC.
- Registro de errores.
- Sistema de fuente de poder redundante opcional.
- Fuente de suministro ininterrumpido de poder (UPS) opcional.

3.5 SEGURIDAD

El gran desarrollo que han tenido las redes en los últimos años, ha permitido a muchas personas utilizar recursos que antes no se tenían disponibles, hoy en día una persona puede consultar información en la pantalla de su computadora sin tener que desplazarse grandes distancias, esto gracias a la ayuda de las redes de computadoras, sin embargo, lo mismo que ha hecho que las redes adquieran la importancia que tienen actualmente, como el compartir información y recursos, es una de sus desventajas, debido a que se pueden registrar accesos no autorizados, los cuales pueden ocasionar que la información que se tiene pueda ser alterada o robada, en algunos casos.

La seguridad tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta, por lo tanto es de esperar que con el uso de redes de computadoras y la cada vez mayor integración de los equipos de cómputo a las redes de comunicaciones, se tengan la necesidad de mantener en secreto la información, evitando los accesos y modificaciones no autorizados.

Cuando se habla de seguridad en redes de cómputo, es posible distinguir dos campos de acción:

- Seguridad en redes pequeñas (LAN's).
- Seguridad en redes amplias (WAN).

Para redes pequeñas quizás la seguridad no sea muy importante, esto debido a que generalmente se trata de grupos de trabajo pequeños, donde el objetivo es compartir algún dispositivo, ya sea éste una impresora, una unidad de CD-ROM, un Scanner, o en su caso información que únicamente afecta a dicho grupo. Por lo tanto podemos decir que en éste caso el nivel de seguridad puede no ser muy alto.

En la medida que la red empieza a crecer, se hace necesario establecer ciertos

niveles de seguridad, con el fin de evitar que personas no autorizadas puedan hacer uso indebido de los recursos.

El nivel de seguridad dependerá en gran medida del tamaño de la red, ya que los recursos humanos y técnicos necesarios para establecer los diferentes niveles de seguridad serán mucho mayores en redes grandes que los requeridos en redes pequeñas.

Para poder implementar mecanismos de seguridad en una red es indispensable conocer:

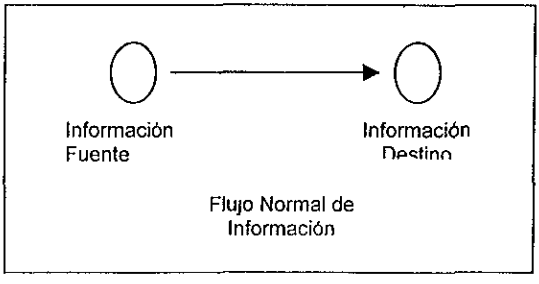
¿Que se quiere proteger?

Es difícil proteger algo cuando no se sabe qué es, es aquí donde se debe determinar si se requiere o no proteger la información o los servicios que ofrece una red, sobre todo definir claramente los puntos vulnerables y de mayor importancia que puedan ser de interés para los intrusos.

¿Contra qué se quiere proteger?

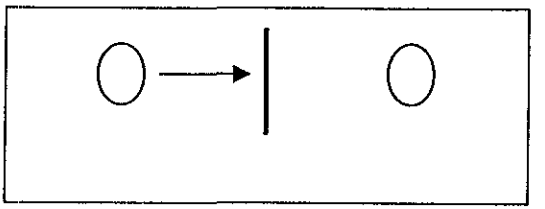
La importancia de ésta pregunta, radica en que si la red no se comunica con otras que se encuentran fuera de las instalaciones, entonces se pueden limitar los posibles ataques a la información.

Existe una pequeña clasificación a los posibles ataques de la información:



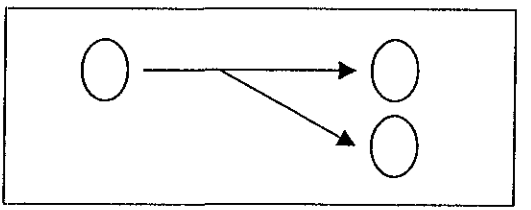
Interrupción

La información del sistema es destruida o llega a ser inutilizable, en este ataque se puede incluir la destrucción de una pieza de hardware, como un disco duro o el corte de una línea de comunicaciones.



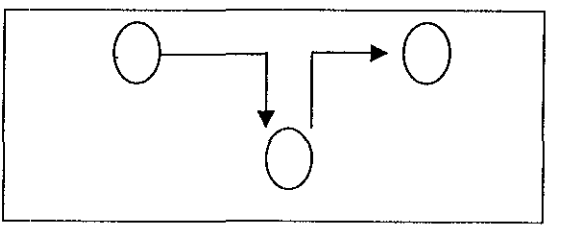
Intercepción

Ocurre cuando alguien realiza una copia de la información que se está transmitiendo.



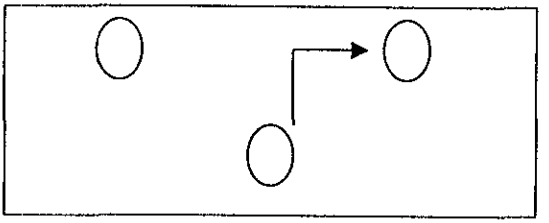
Modificación

Este tipo de ataque consiste modificar la información transmitida, de tal manera que los datos no son confiables.



Fabricación

El ataque de fabricación consiste en introducir paquetes de datos falsificados en una red.



Por último

¿ Que inversión se tiene que realizar y el tiempo que se va a requerir para lograrlo?

Éste es un punto que generalmente afecta de manera significativa la instalación de los sistemas de seguridad en una red, ya que en la medida que se dediquen recursos a esta actividad se tendrán diferentes niveles de protección.

En muchas ocasiones es imposible lograr una seguridad total de los recursos de una red, ya que siempre existirán elementos que puedan afectar de forma interna y externa la operación de la misma, además se debe considerar que la mayoría de los ataques que se sufren, son ocasionados por gente de las mismas instalaciones.

3.5.1 Tipos de Seguridad

Existen diferentes clasificaciones a los diversos tipos de seguridad, sin embargo, los más generales y que en cierta medida engloban a todos los demás son:

Confiabilidad y Control de acceso

Un sistema de cómputo no debe permitir que la información contendida en él sea accesible por alguien que no tenga autorización. Para ello, ésta es la parte de la

seguridad más conocida por la mayoría de la gente, ya que es la más fácil de entender y la que se puede apreciar más rápidamente.

En la mayor parte de los sistemas de cómputo, para poder hacer uso de los recursos es necesario contar con un nombre de usuario y una clave de acceso, esto con el fin de llevar un registro de las personas que están haciendo uso de los recursos, además de comprobar que se trata de usuarios que efectivamente tienen derecho a usar la información.

El problema de la seguridad comienza cuando se tiene acceso a un sistema, las contraseñas y los nombres de usuarios forman una parte importante para prevenir el acceso a personas no autorizadas; la importancia de elegir adecuadamente el nombre de los usuarios y sus contraseñas, radica en evitar que éstas sean fácilmente adivinadas por otros personas.

De estos dos puntos "Nombre de usuario" y "Clave o Contraseña", la clave es el elemento más importante en la seguridad, ya que si la protección con contraseñas es adecuada, se puede eliminar el 80% o 90% de los ataques que se puedan tener en un sistema.

En general se recomienda utilizar nombres de contraseñas que puedan ser recordadas por los usuarios, pero a su vez que no puedan ser adivinas por intrusos, en general no es recomendable que la contraseña conste de: nombre o apellido del usuario, el nombre de algún amigo o familiar, dirección o teléfono del usuario, el cumpleaños del usuario y en términos generales, cualquier elemento de información acerca del usuario, ya que cuando un intruso trata de entrar al sistema, éstos son los elementos que comúnmente utiliza para poder ingresar.

Por otro parte existen diversos tipos de cuentas donde se debe de tener especial cuidado, ya que éstas pueden ser un medio para que un intruso tenga acceso a un sistema.

Cuentas sin contraseña

Las cuentas sin contraseña son elementos que no deben de existir dentro de la administración de una red, en cualquier caso éstas deben ser borradas o en su defecto se debe asignar una contraseña.

Cuentas preinstaladas

La mayoría de las veces al adquirir un sistema de cómputo o de comunicaciones, estos equipos traen consigo un conjunto de cuentas preinstaladas, es recomendable que éstas sean eliminadas o en su caso se proceda a realizar un cambio de contraseña, lo anterior en prejuicio de que una persona que tenga el mismo equipo, ya sea éste un servidor o algún equipo de comunicaciones, y conociendo la existencia de las cuentas preinstaladas, pueda introducirse a la red sin que alguien se percate de su acceso.

Cuentas abiertas

En algunos sistemas es común contar con este tipo de cuentas, lo ideal es eliminarlas, ya que representan una posible fuente de ataques. En los casos donde dicha cuenta sea requerida, es conveniente asignarle una contraseña que no sea tan predecible y dársela a aquellas personas que lo requieran.

Cuentas grupales

En realidad no es muy conveniente crear este tipo de cuentas, debido a que se pierde la posibilidad de rastrear las acciones de forma individual, lo cual ocasionaría que existiera un problema de seguridad grave pues sería muy difícil determinar en caso de una falla, quien fue el responsable.

Cuentas dormidas

La importancia de realizar una adecuada administración de las cuentas de usuario, es debido a que se puedan detectar cuentas que no son utilizadas por su dueño,

esto ocasiona que alguien pueda usar la cuenta sin que puedan notarlo, lo mejor en estos casos es monitorearlas constantemente y en un momento dado cancelarlas.

Integridad y autenticidad

Cualquier sistema de cómputo seguro, no debe permitir que los datos contenidos en él puedan ser modificados sin autorización, esto comprende la posibilidad de que ningún usuario pueda modificar los datos de otros.

Una primera línea para evitar que un usuario pueda modificar archivos que no son suyos, es el permiso a los archivos, generalmente un usuario que es propietario de un archivo, tiene todos lo privilegios sobre su archivo, leer y escribir en él, pero no los de las otras cuentas.

Por lo tanto, es importante saber asignar los permisos a los archivos, sobre todo cuando se trata de los archivos de configuración de un sistema de cómputo, como puede ser el caso de un servidor en la red, ya que puede ser una fuente de ataque por parte de intrusos.

En algunos casos, se puede contar con la posibilidad de verificar quién está enviando la información y si está no a sido modificada, a esto se le llama autenticidad y es un punto de la seguridad que va relacionado con la integridad.

Disponibilidad

Es la capacidad de un sistema de que los datos contenidos en él estén disponibles al momento que son requeridos. Este tipo de seguridad tiene mucha importancia, sobretodo cuando los usuarios hacen uso de la red para accesar sus datos, si la red funciona bien y los datos están disponibles cuando se necesitan nadie notara nada, pero si por alguna causa, los datos no pudieran consultarse, los usuarios dirían que la red no sirve o que en su caso no está bien administrada, éste es un punto clave para cualquier administrador de red.

3.5.2 Mecanismos de seguridad

Para poder instalar diversos servicios de seguridad, es necesario contar con mecanismos y técnicas que garanticen una correcta y efectiva aplicación de la seguridad, como:

Criptología

La criptología se divide en dos áreas importantes: la Criptografía y el Criptoanálisis. La Criptografía toma su denominación del griego y se puede traducir como "La manera de escribir raro" (Criptos, extraño; Graphos, escritura). La Criptología se preocupa por conseguir que nuestros mensajes sean comprensibles únicamente para aquellos que nosotros deseamos e inteligibles para el resto de la humanidad, con el fin de proteger la información que viaja a través de una red. El Criptoanálisis es la parte encargada de quebrantar el cifrado obtenido de la Criptografía.

Pared de fuego (Firewall)

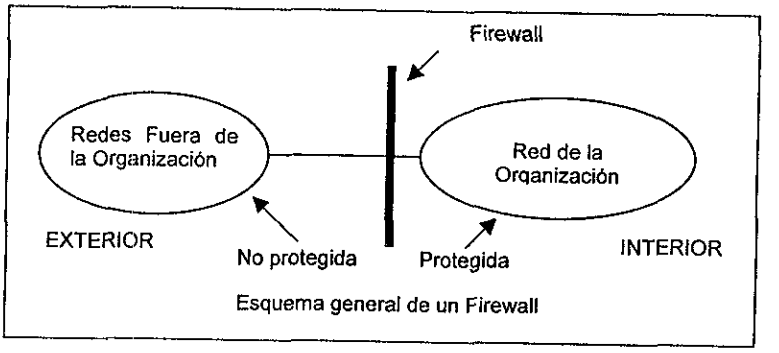
Un firewall es un conjunto de Hardware y Software destinado a establecer mecanismos de seguridad en el punto o puntos de entrada a una red.

El objetivo de un firewall, es aislar dos redes que se encuentra comunicadas, permitiendo que exista una división entre ambas, con esto se puede distinguir dos partes importantes, aquello que se encuentra dentro de la red y lo que se encuentra en el exterior.

La forma más común de implementar un firewall, es mediante un dispositivo conocido como ruteador (router), cuyo objetivo es filtrar paquetes de información y dejar pasar solo aquellos cuyo destino sea un elemento de la red, aunque podría utilizarse cualquier máquina con dos tarjetas de red y un software adecuado para filtrar los paquetes.

Otra característica importante de estos sistemas, es que permite llegar hasta donde

los sistemas operativos de red a veces no pueden, actualmente es uno de los medios más utilizados, ya que con el creciente incremento en el uso de Internet, muchas compañías han tenido que implementar mecanismos de este tipo.



Esquema general de un Firewall

Firmas Digitales

En situaciones donde no hay confianza entre el emisor y el receptor se requiere contar con elementos que garanticen esa confianza, la solución a ese problema es la firma digital. La cual es semejante a la firma escrita de un documento, ésta debe ser posible de verificar y de autentificar su contenido, además de ser verificada por un tercero. Por tanto las propiedades más importantes de una firma digital son:

- Ha de ser posible verificar el autor, la fecha y el tiempo de la firma.
- Ha de ser posible autentificar los contenidos durante el proceso de firma.
- La firma ha de ser verificada por tres partes, para resolver conflictos o disputas.

Como resultado de lo anterior podemos formular los requerimientos para una firma digital:

- La firma ha de ser una parte extraída del mensaje que se requiere firmar.
- La firma ha de utilizar información exclusiva del emisor, para prevenir la creación de un mensaje por parte de un intruso.

- Debe ser relativamente fácil producir una firma digital.
- Debe ser relativamente fácil reconocer y verificar la firma digital.
- Debe ser difícil crear una firma digital engañosa.

La forma en que opera una firma digital consiste en generar un mensaje de un emisor X a un receptor Y, éste se dirige primeramente a un árbitro A, que somete el mensaje y su firma a un examen para comprobar su originalidad y contenido. El mensaje es entonces fechado y enviado a Y con una indicación que demuestra que el mensaje ha sido verificado satisfactoriamente por el árbitro.

3.5.3 Seguridad en los Servicios

Además de todo lo que se ha comentado sobre la seguridad en sus diferentes aspectos, existe un elemento más a considerar por el Administrador de una Red, y es el que se refiere a la seguridad de los servicios de red.

World Wide Web (www)

Éste es uno de los servicios de redes más difundido actualmente y cuyo crecimiento ha sido tan explosivo que no podría haber sido previsto hace algunos años.

La gran mayoría de los documentos www están escritos en HTML (HyperText Markup Language), y son enviados a través de la red utilizando un protocolo conocido como HTTP (HyperText Transfer Protocol). Por lo tanto todo servidor www debe estar corriendo algún HTTP. Es en las distintas formas de implantar estos servidores donde puede haber problemas de accesos no autorizados a los recursos.

Los principales problemas que puede ocasionar un servidor www son:

- Divulgación de información o documentos a individuos no autorizados.

- Información confidencial enviada por el cliente al servidor y que sea interceptada por alguien no autorizado.
- Divulgación de datos acerca de la máquina que funciona como servidor, dando la posibilidad de que algún intruso pueda usarla para efectuar un ataque a la información.

Las principales medidas que se deben tomar para controlar la seguridad en una maquina que funciona como servidor de www, son:

- Evitar usar un servidor con problemas conocidos. Muchos de los servidores de HTTP ampliamente utilizados han tenido problemas de seguridad. En la mayoría de los casos estos problemas ha sido resueltos y colocados en las versiones posteriores, sin embargo existen todavía lugares donde se usan las versiones anteriores.
- Establecer de manera correcta el permiso a los archivos, para evitar que a través de ellos puedan hacer modificaciones a los archivos de configuración.
- Monitorear constantemente las bitácoras del servidor para detectar comportamientos extraños.
- Limitar el acceso a los archivos que contiene la información que se está publicando en el www.
- Desactivar la ejecución de programas CGI (Common Gateway Interface) salvo en casos necesarios y cuidadosamente controlados.

También es importante tener cuidado del lado del cliente. Si el visualizador que se está utilizando está configurado para cualquier documento de tipo aplicación que se encuentre, es posible ejecutar comandos arbitrarios en la máquina que está ejecutando dicho visualizador.

FTP Anónimo

Éste es el servicio más utilizado para transferir archivos entre dos computadoras de la red, sobre todo en aquellas organizaciones donde se comparte información de uso común.

Los principales problemas que puede causar un servidor de FTP con errores o mal configurado son:

- Posibilidad de modificar archivos del área de acceso anónimo, con esto se abre la posibilidad de acceso interactivo al sistema.
- Distribución de programas o material ilegal.
- Posibilidad de ejecutar comandos arbitrarios en el servidor.

Para evitar que sucedan algunos de los problemas que se mencionaron anteriormente, es recomendable configurar correctamente los permisos de los archivos en el directorio de FTP Anónimo. En particular asegurarse de que la cuenta ftp no pueda modificar nada.

Telnet

El protocolo de telnet, por el hecho de permitir a un usuario tener acceso a otras computadoras en la red, es fuente de problemas de seguridad. Los dos principales que existen son:

- Normalmente, para establecer una sesión, el usuario tiene que proporcionar una contraseña, el problema es que como la contraseña viaja por la red ésta puede ser capturada, y utilizada para posteriormente para iniciar sesiones.

- Recientemente en algunas aplicaciones telnet, fue descubierto que un usuario podía tener privilegios de administrador (root) en la máquina a que se conectaba, este descubrimiento está documentado en el CERT Advisory 95:14 y es

recomendable leer dicho documento para corregir el problema, en caso de que exista.

NFS (Network File System) y NIS (Network Information System)

NFS y NIS permiten a un conjunto de maquinas compartir dos recursos fundamentales: espacio en disco y bases de datos de usuario.

Ambos son muy convenientes sobre todo si se tiene muchas máquinas con configuraciones similares, algunos puntos que se deben de tomar en cuenta son:

- NFS y NIS fueron desarrollados para un ambiente donde la cooperación era la regla, donde tanto usuarios como administrador sabían lo que hacían y lo hacían de buena fe, hoy eso ya no es cierto, sobre todo si la red se interconecta con otras.

- Usar NFS y NIS solamente cuando sea necesario, generalmente si se trata de una red local, ya que se evitara que la información viaje por ruteadores y redes desconocidas.

- Nunca otorgar acceso irrestricto a ningún recurso. Cada uno de los recursos proporcionados por NFS y NIS deben ser estrictamente configurados para que sean accesibles sólo a los clientes autorizados.

Otro elemento a considerar en la seguridad de una red, y que actualmente es una cuestión que preocupa no solo a un administrador de red, sino también a cualquiera que tenga una computadora ya sea que ésta se encuentre o no conectada a una red, es el problema de los virus.

Los virus de computadora, son programas que se reproducen y propagan por sí mismos, su objetivo fundamental es causar daño a los datos y en ocasiones dañar

algún dispositivo de hardware; su importancia radica en que para la seguridad de una red sería muy peligroso que un de ellos pudiera entrar al sistema de archivos o a los archivos de configuración de un servidor.

La detección y prevención de virus se puede realizar en tres niveles diferentes:

1. A nivel de estación cliente o computadora personal en donde se instala y ejecuta el software antivirus, la intensión es poder detectar si algún archivo se encuentra contaminado antes de que éste pueda ser introducido a la red, esto representa un primer paso que todo administrador de red debe contemplar para la seguridad de todos los sistemas.

2. El segundo nivel de detección es la instalación del software antivirus en los servidores, la desventaja de esta técnica consiste en que muchos de los accesos al exterior de una red, no necesariamente pasan por el servidor, como sucede en el caso de internet, donde un usuario puede bajar un archivo mediante FTP, sin que éste haya sido analizado por el servidor por lo que el virus no puede ser detectado.

3. El tercer nivel de detección se basa en la instalación de software antivirus en las interfaces de acceso a la red, de tal manera que se aíslen todos los virus antes de que lleguen a la red.

Si se toma en cuenta la cantidad de virus de computadoras que se encuentran en el mundo, cualquier computadora trabajando en forma aislada o conectada a una red, es susceptible de poder ser contaminada, para lo cual en el caso del administrador de una red, debe tener mecanismos de protección basados en los tres niveles.

La utilización actual de las redes de computadoras y la gran ayuda que brindan en el adecuado uso de los recursos informáticos en una organización, ha hecho que existan un sin número de aplicaciones que actualmente operan en un entorno de red,

por tal motivo, lo mencionado anteriormente representa sólo algunas de las consideraciones que deben tenerse respecto a su seguridad. Sin mencionar el hecho de que aún cuando se tomen todas las consideraciones necesarias existirá siempre la posibilidad de sufrir un ataque.

3.6 MONITOREO DE LA RED

Existe dentro de la administración de una red el monitoreo distribuido y dedicado, que nos permiten atacar las tareas reactivas, que son aquellas que suceden una vez que se presentó el problema y las proactivas enfocadas en atacar las causas y no los efectos de los problemas.

Una de las maneras de implantar un monitoreo distribuido consiste en instalar en cada uno de los segmentos de la red una pieza de hardware, como un nodo más de la red, el cual se encarga de recolectar todos los datos que pasen a través del segmento al cual está conectado.

Pero es necesario recuperar de alguna manera los datos almacenados en esa pieza de hardware y es precisamente un software especializado es el encargado de accesar la información almacenada y, entre otras cosas, desplegarla en forma de gráficas o almacenarla en archivos.

El software nos permite obtener algunas estadísticas como: porcentaje de utilización de la red, colisiones y errores, entre otros, además de proporcionar una lista de todos los usuarios que están utilizando la red. Otra característica es la capacidad de fijar alarmas que se disparen en el momento en que ocurra algún evento, por ejemplo, el hecho de que la utilización de la red sea mayor a un porcentaje específico durante un tiempo mayor de un minuto.

La idea del monitoreo distribuido es tener acceso desde una sola consola a todos los dispositivos que estén conectados en nuestra red y resolver la mayor cantidad de problemas generados en toda la red desde un solo punto.

Aunque el fin del monitoreo distribuido es analizar toda la red desde un solo punto, hay ocasiones en que se detecta una falla y no es posible solucionarla de manera remota, entonces es necesario enviar a un ingeniero de soporte con una herramienta

que le permita encontrar y aislar el problema de la manera más rápida posible, a esto es a lo que se le llama el monitoreo dedicado.

Como herramienta para el monitoreo dedicado se encuentran analizadores de protocolos que permiten identificar problemas dentro de la red.

Una de las características que distinguen a los analizadores de protocolos, son las pruebas inteligentes que posee, es decir, poder llevar a cabo una auditoria de la red y finalmente dar un comentario acerca del comportamiento de la misma, y si encuentra alguna falla, plantear varias causas por las cuales se pueden estar presentando los problemas.

El Analizador de Protocolos permite obtener datos como el porcentaje de utilización de la red, errores o colisiones, también genera una lista de los nodos que más errores generan dentro de la red y cuenta con algunos servicios como el PING y ARP. Además, es capaz de generar tráfico en la red con el fin de recrear el ambiente bajo el cual se pueden presentar fallas.

Los probadores de medios son utilizados para analizar el medio a través del cual transmitimos la información, ya sean cables o microondas, por ejemplo, y verificar que la información viaje adecuadamente.

El monitoreo distribuido y el dedicado no son excluyentes, sino que al contrario se complementan con el fin de obtener mejores resultados.

3.6.1 Monitoreo de dispositivos y conexiones

La evaluación del rendimiento de la red asegura que la red esté funcionando correctamente y que los usuarios puedan trabajar en forma eficiente. Por esto se debe realizar el monitoreo de los dispositivos y conexiones asociadas a la red para

determinar su utilización y tolerancia, dicho monitoreo se compone básicamente de:

Colección de datos

Tales como dispositivos que se están utilizando y ligas que se realizan en cada momento.

Para medir el nivel de servicio, se deben tomar en cuenta los siguientes datos:

- **Tiempo de respuesta total.** Es el tiempo desde que el usuario pide información hasta que ésta se despliega en el monitor.

- **Rango de rechazo.** Es el porcentaje del tiempo en que la red no puede transferir información debido al rendimiento de la red o los recursos no están disponibles.

- **Disponibilidad.** Es el porcentaje del tiempo en que la red es accesible y operacional para los usuarios.

Se debe usar un protocolo administrador de la red para la colección de los datos desde la red. Entre estos se encuentra SNMP (Simple Network Management Protocol), este protocolo no está relacionado con los servicios de usuario sino con la administración de los protocolos de comunicación dentro de cada estación y los diferentes miembros de interconexión de redes que proporcionan dichos servicios, es decir administra todo el ambiente de interconexión de redes.

El protocolo SNMP ha sido definido para ayudar al manejador de la red a realizar sus funciones de administración de desempeño y fallas.

SNMP es un protocolo de aplicación, por lo que una plataforma de comunicación estándar debe ser usada para permitir que los mensajes asociados sean transferidos concurrentemente con el mensaje relacionado con el servicio de usuario.

El papel de SNMP es proporcionar un camino para el administrador de procesos (en el administrador de estación), para intercambiar mensajes relacionados con la administración, ejecutando procesos administrativos en los diferentes elementos que se utilizan: gateways, estaciones, etc.

SNMP opera bajo UDP (User Datagram Protocol), este protocolo es usado ya sea cuando no se requiere corrección de error o para un simple intercambio de un mensaje solicitud/respuesta corto entre dos protocolos de aplicación.

El protocolo RMON (Remote Monitoring protocol) también es un protocolo que nos permite recopilar información de la red, fue creado para aumentar las posibilidades del SNMP en redes segmentadas por switches o que tenían muchos enlaces remotos. RMON utiliza agentes inteligentes (pruebas de medición), que permiten el filtrado de datos e información sólo cuando es requerido por la estación de monitoreo SNMP. Esto reduce la carga en la red que introducía el SNMP en redes de gran tamaño, causa principal del uso restringido del monitoreo de la red.

Con el fin de permitir al administrador de red la introducción de condiciones de análisis, RMON facilita pruebas de medición de las prestaciones de la red. Cuando las condiciones programadas se superan, la prueba RMON alerta a la estación de monitoreo SNMP del problema. El protocolo RMON facilita estadísticas de la capa 2 de la norma OSI (capa de enlace) así como nuevas extensiones facilitan también información de la capa 3 de la norma OSI (nivel de red).

Entre los dispositivos inteligentes o pruebas de medición que dan a RMON mayor capacidad se encuentran:

- **Alarmas.** Informa de cambios en las características de la red, basado en valores umbrales para cualquier variable MIB de interés. Permite que los usuarios configuren una alarma para cualquier Objeto monitoreado.

- **Estadísticas.** Mantiene utilización de bajo nivel y estadísticas de error.
- **Historias.** Analizan la tendencia, según instrucciones de los usuarios, basándose en la información que mantiene el grupo de estadísticas.
- **Filtros.** Incluye una memoria para paquetes entrantes y un número cualquiera de filtros definidos por el usuario, para la captura selectiva de información; incluye las operaciones lógicas AND, OR y NOT.
- **Ordenadores.** Una tabla estadística basada en las direcciones MAC, que incluye información sobre los datos transmitidos y recibidos en cada ordenador.
- **Los N principales.** Contiene solamente estadísticas ordenadas de los "N" ordenadores definidos por el usuario, con lo que se evita recibir información que no es de utilidad.
- **Matriz de tráfico.** Proporciona información de errores y utilización de la red, en forma de una matriz basada en pares de direcciones, para correlacionar las conversaciones en los nodos más activos.
- **Captura de paquetes.** Permite definir buffers para la captura de paquetes que cumplen las condiciones de filtrado.
- **Sucesos.** Registra tres tipos de sucesos basados en los umbrales definidos por el usuario: ascendente, descendente y acoplamiento de paquetes, pudiendo generar interrupciones para cada uno de ellos.

Análisis de los datos y conexión entre ellos

El resultado del análisis de los datos debe ser una gráfica representativa sobre la utilización de los dispositivos o ligas en tiempo real para tener una perspectiva histórica.

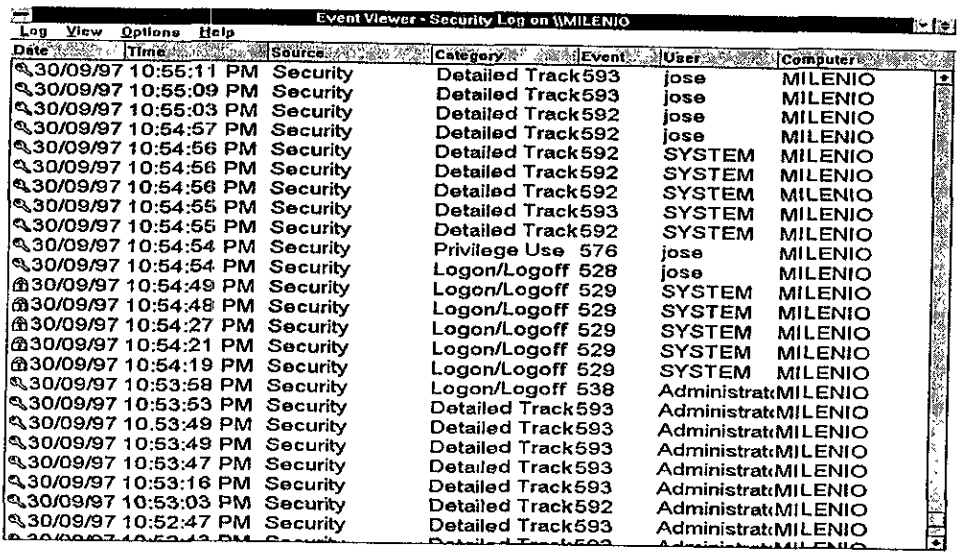
Por ejemplo una gráfica de líneas o barras que demuestre el análisis del rendimiento de la red.

Una gráfica en tiempo real es un buen instrumento para la solución de problemas que puede mostrar el uso o los errores en la red.

Utilización de un simulador

Esto es para saber como se puede alterar la red y maximizar el rendimiento.

3.6.2 Monitoreo de eventos



Date	Time	Source	Category	Event	User	Computer
30/09/97	10:55:11 PM	Security	Detailed Track	593	jose	MILENIO
30/09/97	10:55:09 PM	Security	Detailed Track	593	jose	MILENIO
30/09/97	10:55:03 PM	Security	Detailed Track	592	jose	MILENIO
30/09/97	10:54:57 PM	Security	Detailed Track	592	jose	MILENIO
30/09/97	10:54:56 PM	Security	Detailed Track	592	SYSTEM	MILENIO
30/09/97	10:54:56 PM	Security	Detailed Track	592	SYSTEM	MILENIO
30/09/97	10:54:56 PM	Security	Detailed Track	592	SYSTEM	MILENIO
30/09/97	10:54:55 PM	Security	Detailed Track	593	SYSTEM	MILENIO
30/09/97	10:54:55 PM	Security	Detailed Track	592	SYSTEM	MILENIO
30/09/97	10:54:54 PM	Security	Privilege Use	576	jose	MILENIO
30/09/97	10:54:54 PM	Security	Logon/Logoff	528	jose	MILENIO
30/09/97	10:54:49 PM	Security	Logon/Logoff	529	SYSTEM	MILENIO
30/09/97	10:54:48 PM	Security	Logon/Logoff	529	SYSTEM	MILENIO
30/09/97	10:54:27 PM	Security	Logon/Logoff	529	SYSTEM	MILENIO
30/09/97	10:54:21 PM	Security	Logon/Logoff	529	SYSTEM	MILENIO
30/09/97	10:54:19 PM	Security	Logon/Logoff	529	SYSTEM	MILENIO
30/09/97	10:53:58 PM	Security	Logon/Logoff	538	Administrat	MILENIO
30/09/97	10:53:53 PM	Security	Detailed Track	593	Administrat	MILENIO
30/09/97	10:53:49 PM	Security	Detailed Track	593	Administrat	MILENIO
30/09/97	10:53:49 PM	Security	Detailed Track	593	Administrat	MILENIO
30/09/97	10:53:47 PM	Security	Detailed Track	593	Administrat	MILENIO
30/09/97	10:53:16 PM	Security	Detailed Track	593	Administrat	MILENIO
30/09/97	10:53:03 PM	Security	Detailed Track	592	Administrat	MILENIO
30/09/97	10:52:47 PM	Security	Detailed Track	593	Administrat	MILENIO

El monitoreo de eventos de la red es la capacidad de rastrear y grabar lo ocurrido en la red. El Administrador de la red debe tener la habilidad de buscar en los eventos ocurridos, es decir, en la base de datos por tipos de eventos específicos tales como entradas de usuario, ruteo de paquetes, y errores de hardware, para poder tomar decisiones en cuanto a la administración de la red, para poder resolver problemas tales como:

- ¿Porqué no está recibiendo correo electrónico una ciudad?
- ¿Quién está accesando a la base de datos?
- ¿Dónde está una estación de trabajo, y porqué está transmitiendo corruptamente los datos?

3.6.3 Detección de fallas

El monitoreo puede detectar fallas, elaborar reportes y previene crisis en la administración de la red. Un programa de detección de fallas registra cada dispositivo de la red y compara su estado de operación con unas bases de datos. Si hay diferencias entre la realidad y la base de datos -un puente no responde- el detector de fallas manda una alarma, un mensaje al Monitor de eventos o una alarma audible o visible al administrado de la red.

3.6.4 Línea de monitoreo de la red

En otro nivel de problemáticas, debe ser necesariamente monitoreado el nivel técnico del medio en que se comunica la red. Con esta información el administrador puede determinar cuáles estaciones tienen un rendimiento correcto y cuáles tienen problemas.

Las herramientas usadas para el monitoreo de tráfico en la red solo están disponibles en algunas plataformas para un tipo de red y protocolos. Este monitoreo es llamado comúnmente analizador de protocolos, analizador de tráfico, ó monitor de línea de red. Estas herramientas tienen varios alcances. Algunas solo capturan los paquetes de información, otras capturan y descifran y otras tienen la capacidad de generar tráfico para probar la capacidad de la red.

La captura de los datos puede ser descifrada en muchas formas. Algunas líneas de monitoreo, por ejemplo, pueden desplegar los datos completos en forma de paquete que incluye encabezado, dirección, corrección de errores, y los datos mismos. Esta habilidad puede ser muy útil para la seguridad de la información. No todas las técnicas deben tener acceso a leer todos los mensajes como lo son los correos electrónicos. Estas herramientas deben tener diferentes niveles de descodificación de paquetes donde sólo el personal apropiado pueda ver toda la información.

Requerimientos del software

Requerimientos	Cabletron Spectrum	Hp OpenView	IBM NetView	Sun SunNet
Distribución de Servidor a servidor	*	*		
Maneja mas de 5000 nodos en un dominio	*	*		
Soporta más de 30 operadores	*	*	*	*
Filtros Sofisticados	*	*	*	*
Correlación automática de Eventos	*			
Conectividad al sistema administrativo local	*	*	*	*
Disponible en NT y Unix	*	*		
Sistema de memoria y resonancia	*			

Se muestran a continuación algunas características del software de monitoreo:

Hewlett-Packard cuenta con herramientas que abarcan cada una de las áreas de monitoreo y administración, la equivalencia es:

- Plataformas de administración — **HP Open View** (DOS y UNIX)
- Monitoreo Distribuido — **HP LanProbe II Ethernet/Token-Ring**
- Analizadores de Protocolos — **HP Network Advisor** (Eth, T-R, FDDI)
- Probadores del Medio — **HP Cable Test Set**

HP NetServer Assistant

Tiene las siguientes características:

- Incluye HP Open View 7.2.5 (versión de 100 nodos).
- Controlador SCSI y notificador de falla del dispositivo.
- Control de la consola de Administración desde un PC remoto, permitiendo que sean usadas las mismas propiedades en una consola de administración local o un PC remoto no conectado a la Red.
- Pueden ser añadidos extensiones del HP NetServer Assistant para administradores avanzados de Red.

Spectrum Rmote Monitoring

Tiene la siguientes características:

- Módulo basado en RMON.
- Contiene un analizador de protocolos RMON.
- Provee de reportes estadísticos.
- Monitoreo de la red todo el tiempo.
- Tiene un decodificador de 100 tipos diferentes de protocolos.
- Tiene un filtro sofisticado.

CAPÍTULO 4

INFRAESTRUCTURA DE ADMINISTRACIÓN AVANZADA

4.1 ORGANIZACIÓN

Las necesidades de Redes actuales y futuras determinan lo extenso que puede ser el proceso de planear y organizar una red. Las redes pequeñas de unos cuantos nodos, ubicadas en la misma área física, requieren una planeación mínima. En cambio una planeación más amplia es obligada para aquellas redes de muchos nodos a situarse en diferentes espacios y en distintos pisos de un mismo edificio, e incluso entre diferentes edificios que pueden estar ubicados en lugares muy distantes.

La ventaja de lograr una adecuada organización permitirá simplificar los procesos de detección y corrección de fallas. Para lograrlo es necesario contar con los elementos que permitan identificar tanto las estaciones de trabajo y su ubicación, así como la distribución de los cables que conforman la red.

Algunos de estos elementos tienen cierto grado de complejidad, dependiendo del tipo de red que se esté organizando. Las necesidades actuales de comunicación serán diferentes en cada caso, así como las perspectivas de crecimiento a futuro.

Para tener un panorama general de cómo se organiza una red es importante reconocer las diferentes partes que la conforman, el caso más general puede ser la conexión de un pequeño grupo de computadoras las cuales necesitan compartir recursos, sea el caso de una impresora o una base de datos. El siguiente caso se presenta cuando otro grupo de computadoras necesita conectarse a la misma base de datos, entonces lo que se hace es una interconexión de redes lo cual ya implica la organización de una red más compleja.

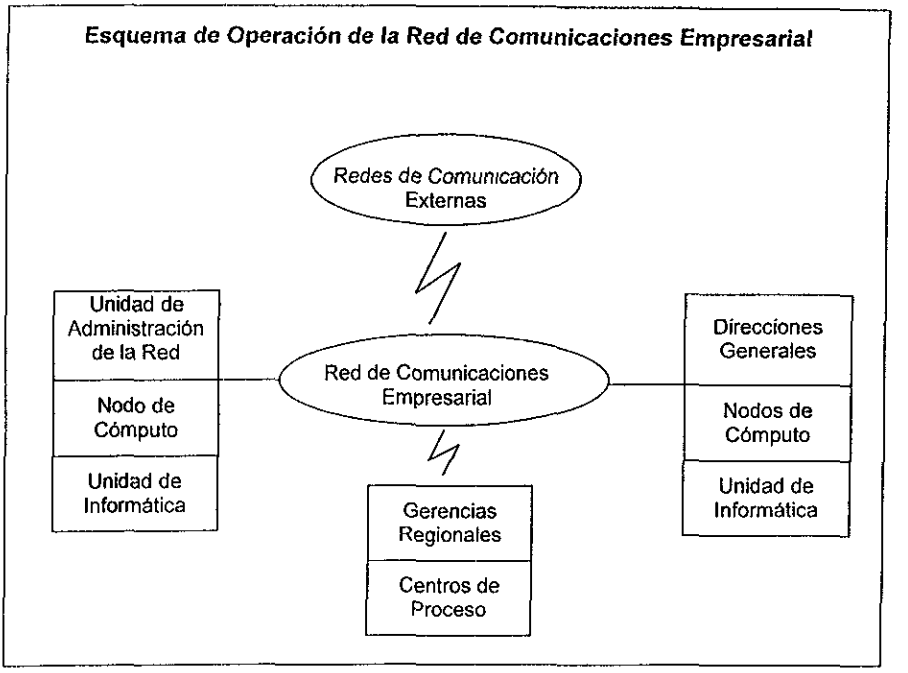
Para apreciar mejor lo expuesto anteriormente se describe la organización actual de una red Empresarial típica, donde será factible distinguir los diversos esquemas de operación de la red, comenzando por conformar lo que es una red Empresarial,

pasando por la distribución de las diversas redes locales, y terminando en el nivel de estación de trabajo.

4.1.1 Nivel Empresarial

La red constituye el componente básico para establecer la comunicación entre las diversas áreas centrales y regionales de una organización, además de permitir la interconexión con redes de otras organizaciones dentro y fuera de un país.

En general este tipo de redes trabaja a través de los equipos de comunicaciones de tipo empresarial ubicados en los nodos de cómputo de las diversas direcciones generales, así como de los equipos instalados en los centros de cómputo de las regiones que se dispongan, como se muestra en la siguiente figura:



La forma en que se encuentra constituida la red que es nuestro caso de estudio es:

- Red de comunicaciones.
- Nodo de cómputo del área encargada de administrar la red central.
- Nodos de comunicaciones de las direcciones generales.
- Nodos de comunicaciones de las gerencias regionales.

Red de Comunicaciones

La red de comunicaciones tiene como objetivo el interconectar los nodos de cómputo de las direcciones generales bajo el concepto de proceso distribuido, además de permitir la conexión con redes de comunicación externas.

Funciones básicas

- Establecer comunicación entre los nodos de cómputo de las direcciones generales.
- Acceder datos y transferir información entre nodos de cómputo.
- Compartir recursos de cómputo a nivel empresarial.
- Permitir el apoyo en procesamiento de datos entre nodos de cómputo.
- Establecer comunicación con las gerencias regionales.
- Permitir el enlace con otros equipos de cómputo de redes externas.
- Permitir la operación de servicios de red empresarial, como correo electrónico consulta a bases de datos, etc.

Características técnicas

Un hilo de fibra óptica de tres pares de 62.5/125 micras que cumple con las normas ANSI, correspondientes al sistema de distribución de fibra óptica. Este hilo conecta actualmente a todos los edificios que forman parte de la organización.

El protocolo de transporte utilizado es el basado en la norma X.25 para red de área amplia y el protocolo de transporte utilizado para la conexión con otras redes externas es el basado en la norma X.75.

Nodo de cómputo del área de administración

El área de administración de la red es la responsable de la función informática Empresarial, requiere administrar un nodo de cómputo enlazado a la red de comunicaciones, que le permita efectuar sus funciones normativas y operativas, operar los sistemas corporativos y soportar a las direcciones generales en sus requerimientos de apoyo informático y de conexión a redes de comunicación externa.

Actividades básicas

- Establecer, administrar y soportar la operación de la red de comunicaciones.
- Establecer los enlaces para conectarse con redes de comunicación externas.
- Apoyar a las direcciones generales en el proceso de datos de los sistemas que sean compatibles con sus herramientas de cómputo.
- El desarrollo, mantenimiento y operación de sus propios sistemas.

Nodos de las Unidades de Cómputo de las Direcciones Generales

Las unidades o departamentos de cómputo de las direcciones generales son responsables de la actividad informática de la dirección, sea ésta hardware o software, por lo tanto requieren administrar un nodo de cómputo que les permita efectuar las funciones de enlace con la red de comunicaciones, así como las de tipo operativo para el interior de la dirección.

Funciones básicas

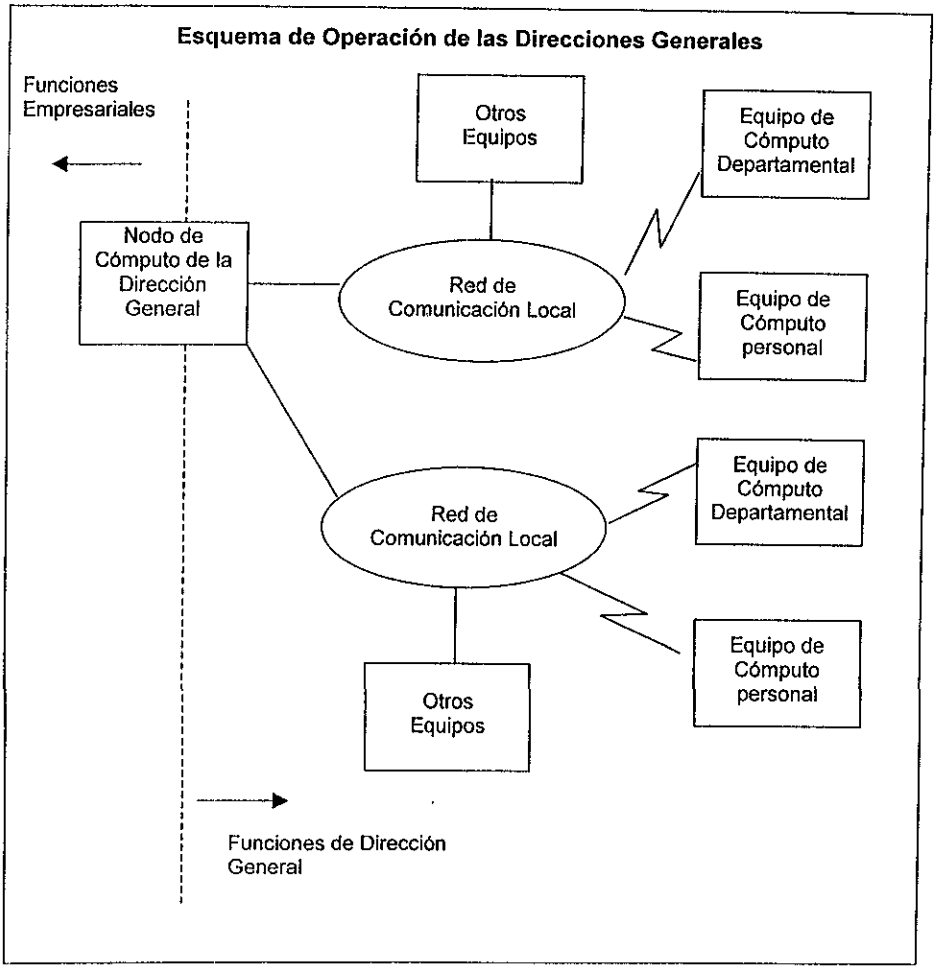
- Garantizar la estandarización del equipo de cómputo y del software empresarial.
- Establecer la conexión con la red de comunicaciones empresarial.
- Procesar y generar información para los sistemas corporativos.
- Definir los requerimientos para conectarse a redes de comunicación externas.
- Soportar el proceso de datos de equipos de cómputo departamentales y personales de la propia dirección.
- Capacitar a usuarios y personal técnico.

Nodos de cómputo de las gerencias regionales

Los centros de proceso son grupos de apoyo informático para la operación de las gerencias regionales, que les permiten respaldar sus funciones de promoción de servicios, mediante la utilización de la infraestructura informática central, por medio del enlace con la red de comunicaciones empresarial.

4.1.2 Nivel de las Direcciones Generales

El esquema de operación de las Unidades de Cómputo se integra de manera particular para cada dirección general, con base en los componentes mostrados en la siguiente figura:



Redes de comunicación local

Las redes de comunicación locales integran el componente básico para intercomunicar los equipos de cómputo departamentales y personales de las áreas internas de cada una de las direcciones generales, enlazarlos a su nodo de cómputo y en su caso, a otras redes externas.

El diseño y topología de las redes locales depende de los requerimientos particulares de cada dirección general.

La integración de los equipos de cómputo especializado de las direcciones generales a las redes locales depende de sus propios requerimientos de operación.

La recomendación general para las redes locales es: redes LAN Ethernet. La topología de la red (estrella, bus, anillo) dependerá de los requerimientos de cada dirección general.

Nodo de cómputo de la dirección general

Este nodo tiene como responsabilidad básica el cumplir con las funciones de carácter empresarial y con las funciones operativas propias de su dirección, como se establece en el nivel empresarial.

Equipos de cómputo departamentales de las direcciones generales

En este nivel de equipos de cómputo se operan los sistemas de rama comunes de aplicación económica y de apoyo administrativo, de acuerdo a las características propias de cada dirección.

Los equipos de cómputo de tipo departamental pueden ser de propósito general o especializado, sin importar su tamaño (macrocomputadoras, minicomputadoras y supercomputadoras).

El equipamiento depende de los recursos de cómputo disponibles en cada dirección general, de su compatibilidad, de la eficiencia en el diseño y manejo de la red de comunicación local y empresarial.

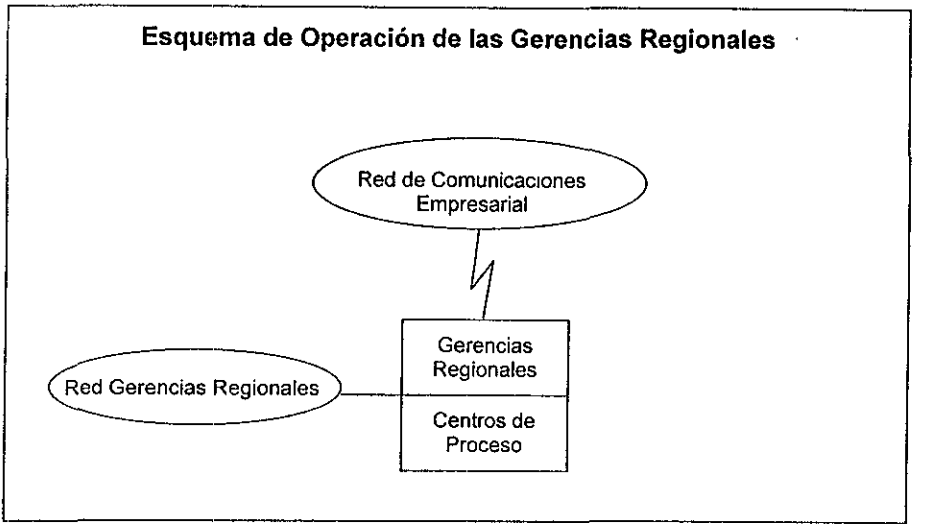
Equipo de cómputo personal

Este nivel de equipo se constituye fundamentalmente por computadoras personales con procesadores con capacidad de multitareas, en los cuales se procesan aplicaciones económicas, administrativas, de tipo secretarial y de automatización de oficinas.

La operación de estos equipos está orientada hacia el usuario final: técnicos, personal administrativo, etc., según sea el tipo de aplicación que se esté trabajando.

4.1.3 Nivel de las Gerencias Regionales

Los componentes básicos de la operación informática a nivel regional son:



Centros de procesos

Constituyen grupos de apoyo informático para la operación de las gerencias regionales, que integran recursos de cómputo de acuerdo con las características y necesidades propias de cada gerencia.

Actividades principales

- Operar equipo de cómputo asignado.
- Procesar las aplicaciones propias de la gerencia.
- Respaldar la información operativa.

Enlace con los nodos de cómputo centrales

Con el fin de aprovechar la infraestructura informática central, se establecen políticas para poder tener acceso a los nodos de cómputo centrales, conectados a la red de comunicaciones empresarial.

Como hemos podido apreciar hasta este punto, una gran parte de las redes empresariales existentes, operan teniendo un anillo de fibra óptica que enlace sus diferentes edificios tomando estos enlaces como punto central de sus comunicaciones y hacia dentro de sus diferentes áreas lo común es encontrar redes más pequeñas del tipo Ethernet basadas en cable coaxial como medio de transmisión.

4.1.4 Cableado Estructurado

El panorama descrito anteriormente, muestra la organización de una red empresarial típica, la cual enlaza sus diferentes áreas de trabajo a través de un anillo de fibra óptica, y a su vez cada área puede estar constituida de una o más redes locales que se interconectan con el anillo de fibra óptica.

Por otra parte en la mayoría de los casos estas redes empresariales están constituidas básicamente por redes tipo LAN Ethernet con cable coaxial, lo cual implica que la velocidad máxima que se puede alcanzar es de 10 Mbps con un ancho de banda de 10 MHz, si consideramos que el futuro tecnológico está basado en el incremento de la comunicación de información de tipo multimedia, es necesario entonces que las redes actuales así como su tecnología cambien para poder dar servicio a las necesidades crecientes de velocidad y ancho de banda.

Ante tal situación se plantea la necesidad de crear una infraestructura adecuada de comunicaciones que pueda tener la capacidad de manejar los anchos de banda y las

velocidades que actualmente requieren las aplicaciones modernas.

Para lograr cumplir con los requerimientos de ancho de banda de las aplicaciones de cómputo actuales, se ha desarrollado el sistema de cableado estructurado, cuyo fin primordial es distribuir el cable para que éste tenga un crecimiento firme y con posibilidades de migrar a nuevas tecnologías. El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se están apoyando las necesidades actuales sino también anticipándose a las necesidades futuras. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin tener que recurrir a costosas actualizaciones del sistema de cableado.

Existen varios tipos de cables y de diferentes categorías. Sin embargo para la instalación de un sistema de cableado estructurado los más recomendados son:

UTP. Unshielded Twisted Pair; Par torcido no blindado.
STP. Shielded Twisted Pair; Par torcido blindado.
FTP. Foiled Twisted Pair; Par torcido blindado general.

Todos estos tipos pertenecen a la categoría 5, que de acuerdo con estándares internacionales (ISO/IEC 11801) y la estadounidense (EIA/TIA 568 A) puede trabajar a 100 megahertz (MHz) y están diseñados para soportar tráfico de voz, video y datos, además de la fibra óptica que basa su principal característica en estas habilidades.

El UTP es sin duda el que hasta ahora ha sido mejor aceptado por su costo accesible y fácil instalación. Sus dos alambres torcidos aislados con plástico PVC, han demostrado un buen desempeño en las aplicaciones actuales, sin embargo a altas velocidades pueden resultar vulnerables a las interferencias electromagnéticas del medio ambiente.

El STP se define como un blindaje individual por cada par, más un blindaje que

envuelve a todos los pares. Es utilizado preferentemente en las instalaciones de proceso de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, aunque con el inconveniente de que es un cable robusto, caro y difícil de instalar.

El FTP cuenta con un blindaje de aluminio que envuelve a los pares para dar una mayor protección contra las emisiones electromagnéticas del exterior. Tiene un precio intermedio entre el UTP y STP y requiere ser instalado por personal calificado.

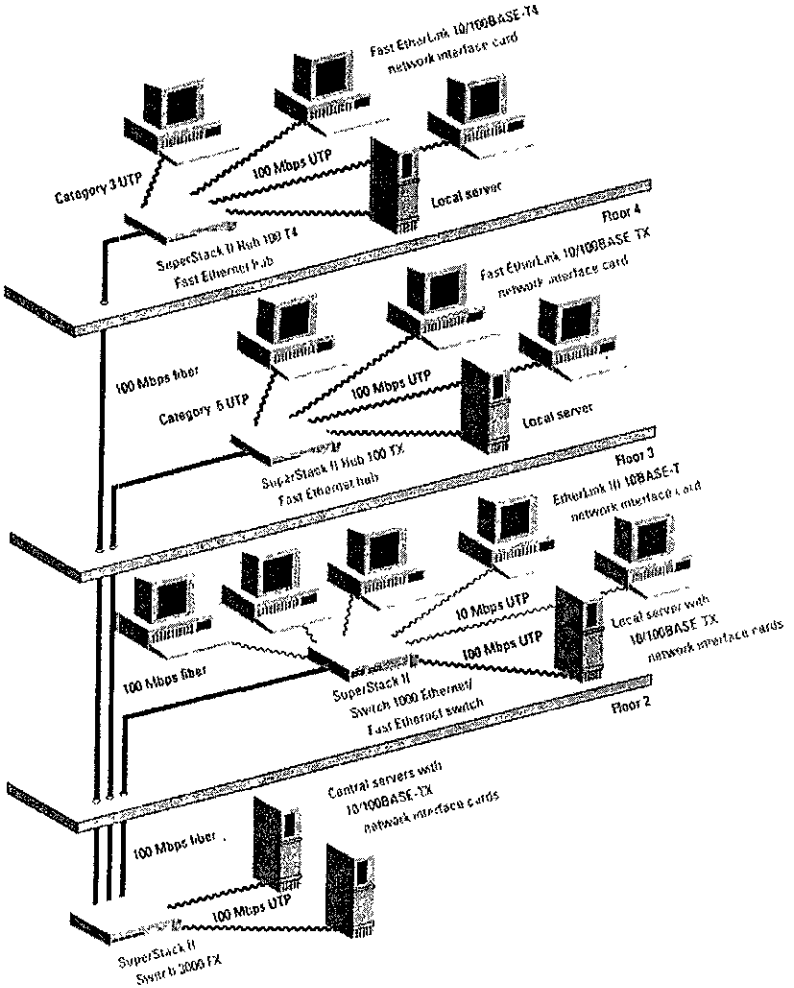
Por último, la fibra óptica tiene una capacidad mayor a los anteriores y una total inmunidad a las interferencias electromagnéticas. Sus únicas desventajas radican en su alto costo y que requiere equipo con terminales especiales. Su instalación es recomendada para aquellos lugares que se encuentran sometidos a grandes variaciones electromagnéticas y donde el medio ambiente en ocasiones juega un papel importante, se necesita equipo complejo y personal altamente calificado para poder llevar a cabo la instalación.

Como resultado de lo anterior podemos decir que el proceso normal de evolución de las grandes redes empresariales, es migrar a un sistema de cableado estructurado, el cual independientemente del tipo de cable que se use presenta mayores ventajas ante el actual cable coaxial.

Las siguientes son una serie de consideraciones que se deben tomar en cuenta para diseñar un cableado estructurado:

- Evaluar las necesidades de comunicación de los usuarios.
- Evaluar el ambiente físico de comunicaciones instalado.
- Determinar en cada caso (Edificio) el diseño apropiado de la red de comunicaciones y los medios de transmisión.
- Completar los planos finales de ubicación y registro de detalle acerca de la configuración del sistema.

A continuación vemos un ejemplo sencillo de la forma en que se interconectan diferentes equipos utilizando el cableado estructurado, como medio de comunicación. Habría que decir que la estructura de diseño y los componentes de sistema del cableado estructurado admiten cualquier topología de LAN.



Esquema de Interconexión de equipos en un Edifico con cableado estructurado

Como podemos ver en la figura, existe un sistema de "Backbone" o columna vertebral ascendente, que es la ruta principal de cable alimentador en el edificio. El Backbone ascendente lleva todas las señales desde los armarios (instalados en cada piso) de telecomunicaciones hasta la sala de equipos situada generalmente en la parte inferior del edificio el cual tiene la interfaz con la red de fibras ópticas.

En algunos casos se suele hablar de backbone horizontal cuando existen dos o más cuartos de comunicaciones en un mismo piso, en este caso el backbone horizontal interconecta los armarios de comunicaciones que existan en el piso.

El conjunto total de cables incluye:

- Tendidos horizontales o verticales de cable entre armarios de telecomunicaciones o de cableado ascendente y la sala de equipos.
- Cables entre salas de equipos y la interfaz de red de fibras ópticas.
- Cables de enlace entre armarios de comunicaciones.
- Cables de "Backbone" de enlace entre cuartos principales de equipo y salas de computadoras.

Por último, podemos decir que el sistema de cableado estructurado representa un enfoque sofisticado de integración de medios para el diseño de una red empresarial, que pueda contar con elementos que le permitan ofrecer una alta calidad en sus servicios, así como un adecuado funcionamiento y sobre todo que sea rápida, eficiente y segura.

Red ATM

Como se puede apreciar, lo expresado anteriormente demuestra que la organización de una red tiene sus diversos grados de complejidad. Dependiendo del tamaño de la red que se esté organizando se requerirá ubicar los diferentes niveles que la

componen, el cableado estructurado representa el primer nivel de una red empresarial, ya que ayuda a organizar la red hacia el interior de los edificios permitiendo controlar el tráfico de información de la red, aumentando con esto la velocidad y el ancho de banda.

El siguiente nivel de una red empresarial consiste en los enlaces que se tendrán entre los diferentes edificios que conforman una organización, este segundo nivel está compuesto por los enlaces de más alta velocidad y generalmente son hechos con fibra óptica, este segundo nivel es el que comúnmente se conoce como Backbone o espina dorsal dentro de una organización.

El lograr un adecuado funcionamiento y una operación confiable de esté segundo nivel, determinará lo eficiente que pueda resultar el trabajo de la red en su conjunto, de tal manera que así como el cableado estructurado representa la evolución de las redes LAN tradicionales, la evolución en este nivel está asociada a la aparición de tecnologías que permiten lograr el incremento sustancial de velocidad y ancho de banda que exigen las aplicaciones de hoy.

ATM es para muchos un concepto que se relaciona con velocidad y alta tecnología. ATM posee ciertas características de tiempo y velocidad que lo hacen atractivo para la transferencia de voz, datos y video bajo una misma plataforma.

La idea de ATM fue propuesta inicialmente por compañías telefónicas, que al empezar a emplear técnicas digitales para la transmisión de voz vieron la posibilidad de utilizar su infraestructura para la transmisión de video y datos. Sin embargo, también observaron que los requerimientos de ancho de banda y retardo eran completamente distintos a los existentes para voz. Por lo anterior se hizo necesario la creación de una nueva tecnología que permitiera la coexistencia, bajo una misma plataforma, de distintos tipos de información.

La diferencia básica entre estos dos tipos de información radica sobre todo en su

tolerancia a retardos y su forma de generación. La voz y el video son poco tolerantes a retardos, es decir, los paquetes de información deben llegar de manera continua y con muy poca demora.

En los datos sucede todo lo contrario. El retardo es importante, sin embargo no presenta restricciones tan estrictas como la voz. En lo referente a su naturaleza de generación la voz y el video presentan tasas continuas de transmisión en tanto que los datos presentan momentos de inactividad (no hay transferencia de información), mezclada con momentos de muy intensa actividad (transferencia de un archivo o consulta). Esta característica provoca que en ciertos momentos el ancho de banda disponible no sea suficiente para satisfacer la tasa de transmisión de datos requerida por la red.

Tomando en cuenta lo antes mencionado se decidió que el tamaño de la celda a fijar (término para paquete ATM), debía de garantizar estos requerimientos. Después de una serie de estudios, concesiones y mucha negociación política entre las empresas telefónicas vs. fabricantes, y Estados Unidos vs. Europa se decidió tener una celda de tamaño fijo de 53 bytes, 5 serían usados por el propio equipo ATM para la conmutación de celdas y el resto por protocolos superiores para transmisión de la información. Es importante recalcar que de los 48 bytes libres no todos ellos son utilizados para transportar nuestra información. Los 48 bytes libres son los que se conocen como carga útil.

Por lo tanto, ATM presenta de manera natural un 10% de sobrecarga en la red. Para poder absorber esta sobre carga, ATM requiere de enlaces de mayor velocidad de transmisión. Hoy en día muchos de los equipos existentes en ATM manejan como estándar la velocidad de 155 Mbps. Sin embargo esta velocidad no es restrictiva, de hecho ya se tienen equipos operando a 622 Mbps y potencialmente podrá ser transportada a velocidades de Gbps. Las velocidades de ATM en la actualidad presentan mucha relación con las encontradas en SONET (Synchronous Optical Networks), las cuales son conocidas como OC-XX/STS-3 (Optical

Carrier/Synchronous Transport Signal). OC-3/STS-3 se refiere a 155.52 Mbps y OC-12/STS-12 a 622.080 Mbps.

El hacer que las celdas ATM tengan un tamaño fijo permite que la conmutación pueda ser implementada en hardware, lo cual implica una conmutación bastante rápida. La red ATM transporta las celdas sin tener en cuenta la información que éstas contienen. La red simplemente las conmuta hasta que éstas llegan a su destino.

El aumento del volumen de información en las comunicaciones internas de las compañías está provocando que éstas se planteen traspasar sus redes al modo de transferencia asíncrona (ATM), el problema básico consiste en que las redes LAN tradicionales transportan datos en forma de paquetes de software que no operan de forma nativa sobre ATM.

En respuesta a esta necesidad de convivencia, se han creado especificaciones para la coexistencia de LAN normalizadas y redes LAN ATM, conocida como emulación de redes LAN ATM (LANE). El objetivo en emulación de redes LAN ATM es permitir la existencia de nodos LAN de medio compartido para interoperar a través de una red ATM y con dispositivos que conectan directamente con conmutadores ATM.

La LANE define cómo pueden ejecutarse sin modificación sobre una red ATM las aplicaciones y sistemas operativos de red con base Ethernet o Token Ring. LANE funciona permitiendo que el Sistema Operativo y todos los protocolos de las capas 2 y superiores operen de forma transparente con ATM. Un adaptador ATM que emplee controladores LANE - basados en la Network Driver Interface Specification (NDIS) o la Open Data-Link Interface (ODI)- aparece ante el sistema operativo de red y la pila de protocolos del servidor como si fuera un adaptador Ethernet o Token Ring. La clave de esto es el uso de un puente conocido como conversor ATM-LAN.

El puente lógico debe ser capaz de convertir las tramas de la LAN en celdas ATM y viceversa. Ésta es una de las funciones clave de la emulación de redes LAN ATM. La

especificación del foro sobre ATM hace uso del protocolo AAL5 para segmentar tramas LAN en celdas ATM, y agrupar celdas ATM entrantes en tramas LAN. Para celdas ATM de salida, los convertidores ATM-LAN se conectan de la forma usual a un conmutador ATM como parte de una red ATM.

Lo anterior demuestra que una de las tecnologías usadas actualmente para implantar redes WAN, está siendo ampliamente utilizada en el desarrollo de LAN´s corporativas, como solución a los requerimientos de velocidad y ancho de banda, proporcionando las siguientes ventajas:

- Proporciona enlaces de alta velocidad.
- Baja latencia.
- Switcheo de red.
- Soporte de voz, datos y tráfico de video.

Algunas de las consideraciones que se deben tomar en cuenta al adquirir equipo ATM, para configurar una red ATM son:

Cumplir con los estándares:

- Especificación IISP (The Interim Interswitch Signaling Protocol) lo que establece interoperabilidad.
- Interfaces UNI (User to Network Interface) y NNI (Network to Network Interface) que cubren:
  Conexión física.
  Señalización.
  Administración de tráfico / Control de flujo.
  Consideraciones de direccionamiento.
  Administración de red.
- Manejo de servicios ATM:
  CBR(constant bit rate).
  VBR(variable bit rate).

ABR(*available bit rate*).

- Manejo de Mecanismos de control de congestión EFCI.
- Cumplen con el Proceso estándar de señalización basado en CCITT Q.93B que establece conexión:
  Punto a punto (Point to Point).
  Punto a multipuntos (Point to Multipoint).
- Control de tráfico.
- Soporta estándares MIB.
- Este equipo cuenta con Fault Tolerance (al menos una fuente redundante).

Respecto a la Administración de los equipos se debe cumplir con lo siguiente:

- El servicio de administración cumple con dos niveles:
  Monitoreo de rendimiento, Alarmas (Layer Manager Capabilities, Lookback.)
  Aspectos de servicios, Cambio de parámetros, Reconfiguración de Vps/Vcs (Manager Plane Capabilities).
- Soporta administración y monitoreo local o remoto por medio de SNMP, ATM RMON y TELNET.
- Soporta MIB's.
- Soporta administración por ILMI (Interim Local Management Interface) que son soportadas por OSI NM o SNMP.

En cuanto a los concentradores para los diversos grupos de trabajo:

- Este equipo debe ser compatible con los estándares para Redes Ethernet y protocolos TCP/IP, IPX.
- Cumplen con la norma IEEE802.3.

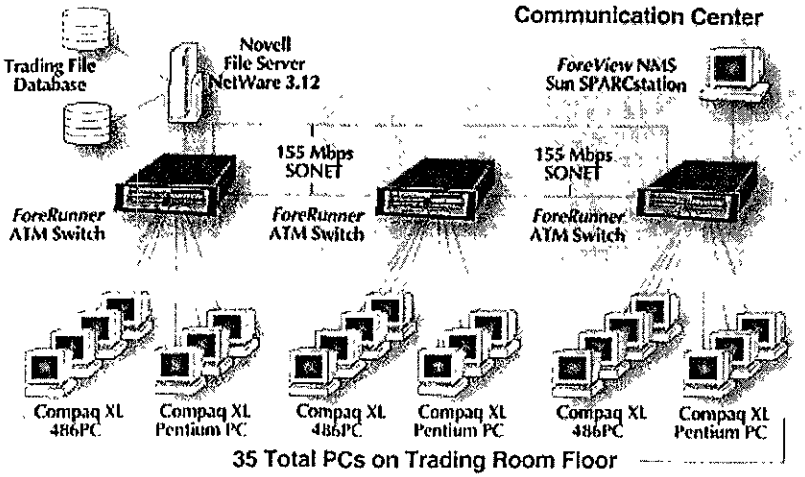
Sistema de administración, monitoreo y seguridad de la red

El software de administración debe contar con las siguientes características:

- Mapeo automático de la red.
- Monitoreo y configuración de dispositivos.

- Inventario de hardware y software de la red.
- Soporte a Virtual LAN´s y Virtual routers configuration.
- Auditoría y recursos.
- Herramientas para verificación de errores de enlace, utilización del concentrador, estadísticas de conexión, rutas, nivel de canales.
- Soporte a SNMP.
- Unidades de respaldo.
- TCP/IP para la red local y servicios ARPA.

Como ejemplo de cómo se puede configurar una red LAN con tecnología ATM, en la siguiente figura se muestra la conexión de tres Switch ATM del tipo ASX-200 de Fore Systems, los cuales se conectan con enlaces de fibra óptica a 155 Mbps y que en su conjunto forma el backbone.

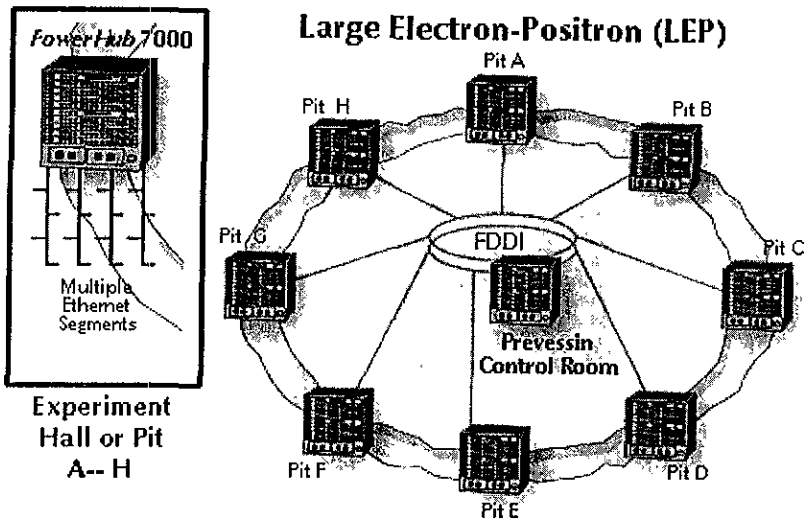


Las PC´s basadas en 486 se encuentran conectadas con enlaces de 100 Mbps y para las Pentium se utilizaron tarjetas ESA-200PC ATM de Fore System las cuales brindan un enlace a 155 Mbps.

Directamente a uno de los Switch se ha conectado un servidor de Base de Datos con lo cual se espera que el procesamiento de transacciones sea más eficiente y rápido.

Se cuenta con una Sun SPARCstation para funciones de administración y en ella se ejecuta el software ForeView Network Management, con lo cual se puede monitorear todos los eventos que ocurren en la red.

En el siguiente ejemplo se puede apreciar como se interconectan varios LAN Switch del tipo PowerHub 7000 de Fore, con la finalidad de formar una LAN corporativa donde cada Switch representa un nodo al Backbone corporativo.



De cada LAN Switch es posible conectar diversos segmentos Ethernet con lo cual se pueden formar subredes que están interconectadas al anillo de fibra óptica; con el desarrollo de ELAN (Ethernet LAN) es posible organizar diferentes grupos de trabajo y controlar el tráfico de información dentro de la red, permitiendo que la información fluya a través del anillo solamente cuando el destino de la información se encuentra

en otro segmento de red conectado a otro Switch.

Con este tipo de organización es factible conservar gran parte de la infraestructura actual, ya que únicamente se requiere conectar los concentradores a cada uno de los puertos del Switch, manteniendo los segmentos Ethernet operando sin ningún cambio.

Cabe aclarar que el tipo de configuración de una red ATM, dependerá en gran medida de los requerimientos específicos de cada organización y del tipo de servicios que se quieran brindar, así como las necesidades propias de los usuarios.

4.2 METODOLOGÍA DE TRABAJO

La necesidad de conectar computadoras, el compartir recursos y el poder establecer contacto con redes nacionales e internacionales, originó la creación de una metodología de redes y convenciones para llevar a cabo una buena administración de la red.

Como consecuencia de esto, las diferentes áreas dentro de la empresa adquieren y configuran sus diferentes redes (locales) y sistemas de comunicación de acuerdo a sus requerimientos y necesidades. El área responsable de administrar la red, es la que se encarga de establecer la metodología para implantar normas y estándares para la compatibilidad de las diferentes redes, con fundamento en el marco normativo nacional e internacional, empleando la tecnología mas avanzada.

El contar con una metodología es garantizar la correcta información de los recursos de cómputo, con eficiencia y seguridad. Su alcance es la transmisión de datos a través de la red con las diferentes redes locales que puedan existir, optimizando el enlace entre ellas y apegándolas a los estándares establecidos por los organismos encargados de la normatividad de comunicaciones (ISO, CCITT, IEE, etc.).

A continuación se describen algunos pasos que se deben de seguir para tener una metodología de trabajo en las diferentes etapas de la administración de la red:

En cuanto a su instalación:

- Realizar un inventario del Hardware y Software de la Red, así como un diagrama lógico de ésta.

- Asignar y controlar las claves de acceso para el establecimiento de comunicación con las diferentes redes.

- Hacer una relación del personal encargado de los diferentes componentes de la red.

- Realizar a conexión de equipos externos, por medio del área encargada de administrar la red, para evitar daños a los componentes que conforman dicha red. Esto se hará presentando al área un diagrama conteniendo las especificaciones técnicas de la red y sus diferentes requerimientos de transmisión.

- Actualizar, en caso de ser necesario, el inventario de comunicaciones cuando exista algún cambio en su equipamiento.

En cuanto a su operación:

- Operar en forma correcta y autorizar el acceso de otros equipos conectados a la red, por parte del área encargada de administrarla, con base en un control de acceso que se utiliza como mecanismo de seguridad.

- Contar con una biblioteca técnica con los diferentes manuales de operación de los diversos componentes que conforman la red.

- Asignar personal responsable y capaz para operar en forma correcta la red.

- Mantener una bitácora de la operación y monitoreo de la red, en la cual se registrará la problemática de la operación, los diferentes accesos que se realizen a la red por parte del área usuaria y el registro del uso de los diferentes servicios.

- Asignar claves a los diferentes usuarios de la red, para el control y seguridad en la operación de la misma.

- Mantener en forma activa las conexiones para minimizar las interrupciones que se

puedan presentar en el servicio que ofrece la red.

- Proporcionar diferentes servicios como interconexión entre diferentes edificios, diferentes redes que puedan estar localizadas dentro de estos, etc.

En cuanto a su mantenimiento:

- Establecer procedimientos del mantenimiento preventivo y correctivo de la red.
- Contar con contratos de mantenimiento preventivo y correctivo necesario para el buen servicio de los diversos componentes que conforman la red.
- Supervisar al proveedor de la red, garantizando así las reparaciones que se lleven a cabo por medio de componentes originales y personal calificado.
- Solicitar por medio del área encargada de administrar la red, el mantenimiento correspondiente de ésta por medio del proveedor que se haya contratado.
- Notificar a los diferentes usuarios y con tiempo necesario acerca del mantenimiento que requiere la red, evitando así cualquier contratiempo.

En cuanto a su seguridad:

- Establecer un control de acceso a la red, por medio de los métodos de seguridad más actuales.
- Revisar en forma periódica, la bitácora de operación de la red y aplicar medidas necesarias para la corrección de fallas que sean detectadas.

- Evitar el flujo de software sin licenciamiento a través de la red, con la aplicación de sanciones para todo el personal que incurra en esto.

- Incluir en el plan de seguridad, todo el equipo que esté conectado a la red, para evitar las interrupciones que pueda tener la red.

4.3 RECURSOS HUMANOS

El administrador de redes debe tener un conocimiento técnico y experiencia, así como una visión clara de lo que pasa en la red, por lo tanto, ya no tiene, como ocurría en el pasado, que estar corriendo detrás del cableado, viendo dónde estaban los ruteadores, ó por qué determinado segmento no funcionaba. La administración de red era una actividad un tanto física, ahora, el administrador cuenta con herramientas para monitorear tráfico, para hacer cambios a través del software y no tiene que estar corriendo detrás de los cables. Asimismo, será una persona con una visión global, capacitada para analizar con exactitud la forma en que ésta se utiliza, y por lo tanto, con el poder de decisión para determinar cómo se debe manejar.

Antes, el administrador llegaba al extremo de tener que ir hasta el panel de conmutación a cambiar servicios porque uno de los usuarios se cambiaba de piso. Actualmente, todo se hace a través de software de administración, y lo interesante es que la filosofía va cambiando un poco. El administrador no sólo es la persona que conoce a fondo la tecnología, ahora es un individuo totalmente involucrado en el negocio, lo conoce mejor y, en ese sentido, está capacitado para proponer los cambios. El control que tiene de la red le permite mejorar eficiencia, dar más servicios en la empresa.

Al ampliarse la participación de los administradores en la empresa, su papel dentro de la dinámica empresarial es una combinación de habilidades técnicas y propuestas de negocio.

En un mercado basado en la red y que constantemente recibe los beneficios del avance tecnológico, el potencial del administrador actual radica en su capacidad para explotar las oportunidades de negocio de la red.

La limitante principal para toda la industria, a nivel mundial, es la falta de suficiente personal que cuente con el nivel apropiado para manejar redes grandes. Aún hay

falta de experiencia en cuanto a la forma de cómo se manejan o administran este tipo de redes.

La solución que ofrecen los sistemas "inteligentes" como analizadores de la red, monitores y programas de administración, no es total, de hecho la aparición de este tipo de software está determinada por un mercado en que tanto hombre y sistema deben colaborar necesariamente. Nunca se pensó sustituir al administrador de red con un equipo. La complejidad de la administración se queda en el software y el hardware, no para facilitar el trabajo, sino para ofrecer más opciones de decisión. Los programas de administración se vuelven cada vez más completos y más complejos, porque tienen que manejar un gran volumen de información y brindar herramientas adicionales para que el administrador pueda tomar decisiones de mayor complejidad. Por otro lado, menos personas son necesarias para controlar la red. En lugar de tener a muchos administradores distribuidos a lo largo de la red para resolver pequeños problemas; es mejor tener a uno o dos con un grado mayor de experiencia, pero que estén capacitados para administrar todo gracias a las herramientas inteligentes colocadas en los equipos.

Sin embargo, el óptimo desarrollo del administrador de redes contemporáneo, no estará determinado por la aparición de programas "inteligentes" que en apariencia, le facilitan todo el trabajo; la realidad es otra; sin limitaciones tecnológicas para administrar una red grande, a los administradores de red se les exigirá mayor participación y compromiso con las funciones críticas de la empresa. Al mismo tiempo, los programas "inteligentes" exigen una formación técnica de alto nivel, necesitan de un interlocutor en el mismo nivel.

El perfil del administrador de red, en ese sentido, debe cubrir tanto las áreas técnicas como las empresariales.

Las herramientas "inteligentes" podrán facilitarle el control, pero este tipo de software exige más capacidad profesional.

La red se ha consolidado como el corazón de los negocios contemporáneos, y en ese sentido, el papel del administrador se vuelve vital. Los mandos técnicos de la industria están inmersos en la planeación empresarial y en el desarrollo de oportunidades de negocio. Si en la empresa el trabajo de red representa un alto porcentaje en términos de rendimiento comercial, las propuestas más objetivas podrían venir de la persona que mejor conoce la esencia (potencial y limitantes) de ese trabajo, es decir, del administrador de la red.

Pero ¿qué sucedería si por cualquier causa el administrador no estuviera presente cuando ocurren problemas o cambios en la red?

Es aquí cuando el administrador debe tener una serie de documentos que nos puedan ayudar a corregir los problemas dentro de la red, así como documentos que nos permitan saber como está constituida. Pero tal vez esto no sea suficiente, por esto mas de una persona debe estar a cargo de la ella, no con esto se pretende desmentir lo antes dicho, pero cuando está en juego la seguridad de nuestra red y los datos de nuestra empresa no se puede confiar en una sola persona, por esto es recomendable que todo lo referente a la red como son: planos de cableado y ubicación de máquinas, protocolos y sistemas utilizados, software que se comparte y como se comparte; en fin todo lo que involucra las actividades del administrador esté debidamente documentado.

4.3.1 Recursos humanos en la red

Dependiendo del tamaño de la red o la complejidad del ambiente, el nivel de conocimientos requerido por el personal responsable será variable. También es frecuente que este grupo sea el encargado del desarrollo de estrategias, diseño y planeación del crecimiento tecnológico de la empresa.

Llegar a un grado de estabilización en el funcionamiento e integración de todos los

servicios que las redes ofrecen, implica tener muchas horas de trabajo, experiencia y afinación de varios parámetros, claro que se debe de contemplar la capacitación y actualización del personal para su mejor desempeño.

Se deben tomar en cuenta algunos puntos:

- Las necesidades del usuario, una atención oportuna a sus requerimientos y seguimiento a sus solicitudes de servicio.
- Para poder resolver en forma eficiente los problemas de la red, los empleados deben estar capacitados y actualizados.
- Para tener una capacidad de respuesta alta y con calidad de servicio es necesario tener el suficiente personal.

4.4 CAPACITACIÓN

Anteriormente la capacitación se veía como el último recurso cuando todo salía mal y se había contratado a una gran cantidad de expertos que no solucionaban los problemas. No obstante, ahora se convierte en un sinónimo de prevención y ahorro en costos de operación. Por tal motivo la capacitación actualmente adquiere una importancia trascendente en el desarrollo y evolución de una organización, el contar con personal capacitado y actualizado, garantiza una mejor posición en el mundo global que se vive.

Ante la creciente necesidad que tienen muchas compañías por lograr una mayor integración de sus recursos materiales y humanos con el aspecto tecnológico, surge la posibilidad de instalar una red de cómputo como elemento que permita lograr dicha integración, muchas veces se aventura a dejar esta responsabilidad en gente que no tiene los conocimientos para hacerlo, el problema no es tan complicado si se habla de una red pequeña, 5 o 10 usuarios, pero se puede volver muy complicado si se trata de una red de cientos de usuarios, es aquí donde surge la interrogante de ¿ que tan capacitado se encuentra la persona a la que hemos designado como Administrador de la red?.

En primera instancia al analizar la infraestructura de algunas organizaciones, se podrá apreciar que muchas veces no se cuenta con un departamento encargado de llevar a cabo el diseño e instalación de una red, sobre todo si la organización es pequeña y no tiene los recursos financieros suficientes, en éstos casos se deja dicha responsabilidad al área de sistemas ya que al ser la encargada de manejar los aspectos informáticos se espera que ellos tengan los conocimientos para poder hacer el trabajo.

Es en este punto donde toma importancia la pregunta anterior, ya que no existe un curso o cursos de administrador de redes donde se pueda inscribir a una persona sin conocimientos sobre redes de computadoras y al terminar dicho curso, esté

capacitado para desempañar el puesto de Administrador de Redes.

Generalmente, la persona designada como Administrador de una red es una persona que posee los conocimientos y habilidades que se requieren para desempeñar tal función, dichos conocimientos son adquiridos en la universidad y reforzados con la asistencia a diversos cursos, con ello el Administrador puede entender el desarrollo de las nuevas tecnologías, logrando mejorar sus habilidades para poder explotar el uso de todos los recursos que estén a su alcance con el fin de conseguir que la red funcione de forma eficaz y adecuada.

Como un punto importante, se debe agregar que el Administrador es una persona que se va formando con el transcurso del tiempo, con base en la experiencia que adquiere en la solución de problemas, tanto en el manejo de equipos como en su capacidad para administrar la red eficientemente. Dicha experiencia puede ser obtenida de diferentes formas: mediante experiencia vividas día a día, mediante cursos de actualización, y tal vez uno de los más importantes, la autocapacitación.

Es gracias a la autocapacitación, que muchas personas actualmente ocupan el cargo de administrador de redes en una organización, ellas han tenido la capacidad y los conocimientos para asimilar y entender el complejo mundo de las redes y poder lograr su adecuado funcionamiento.

Por otra parte, son los administradores de redes los que más sufren por la falta o insuficiencia en la capacitación del personal en una organización, se estima que el 20% de las llamadas telefónicas de los usuarios al administrador, tienen que ver con la red, entre el 45 y 50% están relacionadas con el manejo de la paquetería instalada, y el resto tiene que ver con el funcionamiento del hardware y sobre todo aquellos relacionados con la impresión.

En muchas organizaciones, la Red de cómputo se ha convertido en el corazón de las actividades de negocio que se desarrollan, como ejemplo se puede considerar a las

Instituciones Bancarias, donde al ocurrir un problema en el flujo de información entre sus diversas sucursales y la oficina central, éste puede representar grandes perdidas financieras.

Por lo tanto, todo departamento encargado de administrar una red corporativa, debe tener los mecanismos que permitan mantener actualizado al personal que labora en la organización, tanto en el aspecto teórico que es la parte fundamental de una buena formación como en el aspecto práctico que da experiencia en la solución de problemas; lo anterior, debiendo realizarlo de manera constante y periódica, ya que en muchas ocasiones se cae en el error de pensar que las habilidades adquiridas en un curso de actualización, seguirán siendo vigentes durante mucho tiempo.

Tradicionalmente, la capacitación se imparte dentro de un aula y con los elementos que permitan realizar las practicas, en el caso especial de las redes, muchas instituciones dedicadas a la capacitación y actualización de personal en el área de cómputo, ofrecen cursos a los departamentos encargados de la administración y operación de la red empresarial, proporcionando todo el material necesario, así como un laboratorio para poder realizar las prácticas que se requieran. En este punto hay dos modalidades, debido a que algunas organizaciones sugieren que dichas prácticas se lleven a cabo en sus instalaciones y con su equipo, lo cual permite una mayor integración de los operadores de la red, con el equipo que están manejando, logrando con esto un conocimiento más profundo de cada uno de ellos.

Es importante considerar que la gente que esté a cargo de mantener una red, debe tener los conocimientos necesarios que le permitan llevar a cabo un adecuado manejo de los equipos, sobre todo para que en caso de una falla, pueda ser resuelta y no tener que acudir con el proveedor del equipo, lo cual en algunos casos representa costos adicionales.

No hay que olvidar que existe un gran número de aplicaciones que funcionan en una red, y que dependiendo de los servicios que preste, el administrador debe contar con

el suficiente conocimiento de cada uno de ellos, con el fin atender a los usuarios en los posibles problemas que se puedan presentar, lo cual implica una actualización constante en todas las áreas en las que como administrador de la red se encuentra involucrado.

Por último, siempre que se realice la compra de algún equipo de comunicaciones, es necesario que éste sea a proveedores serios que tengan la capacidad de brindar soporte técnico a los productos que vendan, ya que en caso de una falla, ésta pueda ser resuelta a través de una llamada telefónica o teniendo la posibilidad de que un experto de la compañía se traslade a las instalaciones donde se encuentra el equipo, a fin de ayudar en la solución del problema.

Un punto importante para el administrador de redes es que no sólo es la persona que conoce a fondo la tecnología, ahora es un individuo totalmente involucrado en el negocio de la empresa, lo conoce mejor y en ese sentido, está capacitado para proponer los cambios que beneficien el desempeño de la organización, aumentando la eficiencia y proponiendo nuevos servicios de valor agregado.

4.5 HARDWARE Y SOFTWARE

Las redes locales son muy flexibles en su instalación, tienen una gran capacidad de expansión, se controlan de manera local y su mantenimiento es relativamente sencillo. Dada su gran capacidad de transmisión se pueden organizar en distintos grupos de trabajo sobre un mismo segmento de red. Si consideramos que el origen de las redes fue impulsado por la necesidad de compartir recursos como impresoras y archivos, resultaría imposible por ejemplo, poder dotar a todo un grupo de computadoras con una impresora para cada máquina, por lo tanto, podemos decir que el costo de adquisición / mantenimiento / funcionalidad de una red LAN está en un punto medio bajo comparado con el costo que se tendría de dotar a cada computadora con una impresora.

El problema viene cuando distintos grupos de trabajo, distintas redes locales con objetivos independientes, desean interactuar. Si a esto le añadimos un problema generalmente bastante común, la distancia geográfica, hace que nuestra red local se quede en un pequeño punto aislado de nuestra oficina, edificio, ciudad o país.

Pero ¿por qué la mayoría de las empresas crean pequeñas redes locales, en lugar de una red global?.

Como respuesta a esta interrogante, una de las ventajas de segmentar una red en varias LAN's es distribuir el tráfico de la red, de esta manera la información se transmitirá de una forma más clara (sin colisiones) y por lo tanto más rápidamente, también se debe actuar de esta forma debido a la distancia entre los ordenadores, ya que habría un retardo considerable entre máquinas muy distantes.

Además, si por lo que fuese (un fallo de tensión, conflictos de configuración,...) una máquina dejase de trabajar, haría que la red dejase de funcionar, en cambio segmentando la red en pequeñas redes evitaríamos que el sistema cayese por completo.

Otro punto a considerar es la seguridad, ya que podemos limitar el acceso entre dos segmentos de la red, estableciendo una LAN de acceso restringido a una LAN de acceso general.

Si a todo esto le añadimos que actualmente hay un gran impacto tecnológico en los estándares, que la competencia entre fabricantes es cada vez mayor, que en el mercado hay muchas redes heterogéneas y que la necesidad de comunicación está alcanzando cuotas insospechadas, nos encontramos con la necesidad de Interconectar redes.

La interconexión de redes puede entenderse como la posibilidad de compartir recursos globales a la vez que se mantiene y reserva la independencia y la autonomía de los elementos que se conectan.

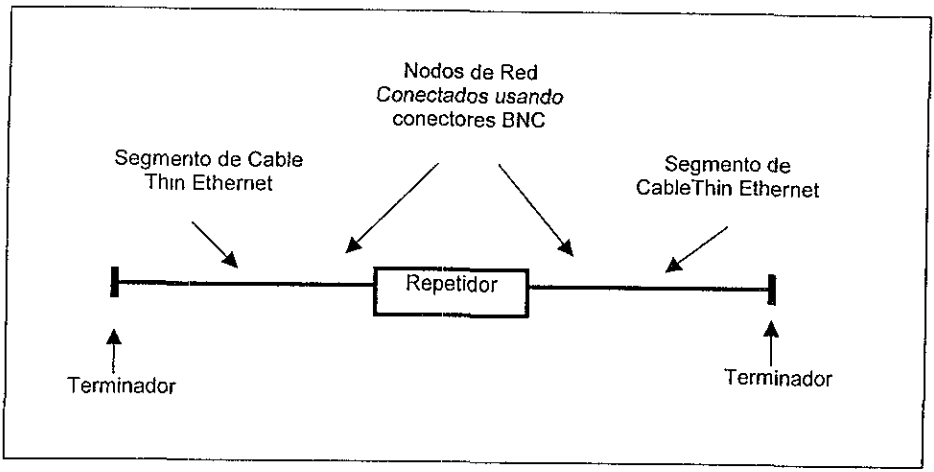
Las situaciones más típicas pueden ser, la ampliación física de una LAN más allá de su capacidad de base, la interconexión de distintas LAN's en una red pública, la integración de una LAN con una red de hosts o la interconexión de dos redes de hosts.

Por lo tanto, nos interesa saber qué son y cómo funcionan los dispositivos de interconexión de redes.

4.5.1 Repetidores

Estos operan en la capa física del modelo OSI, ya que interconectan redes iguales (del mismo tipo). Su utilización sirve para extender la distancia máxima de la LAN o para unir o interconectar distintos soportes de comunicación, aunque también puede servir para unir varios segmentos o varios anillos constituyendo una LAN física y lógica única

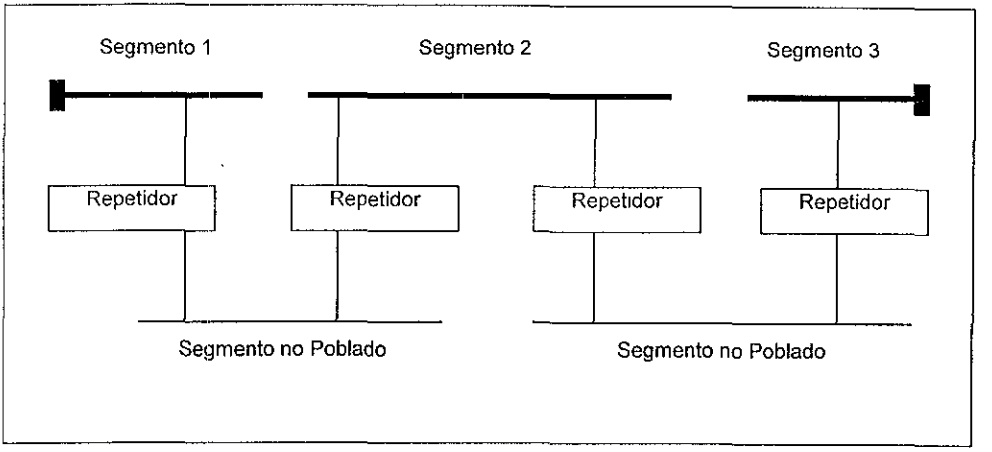
Hay que tener claro que un repetidor no analiza la información que le llega, hace una transmisión transparente de todas las tramas de un segmento de LAN a otro (en *ambos sentidos*), *regenera las señales* y *no realiza* ningún filtrado de trama. Lo que sí hace es restaurar el preámbulo (parte que activa los sincronismos) dado que no varía nunca; el resto lo amplifica. También corrige la frecuencia y la amplitud.



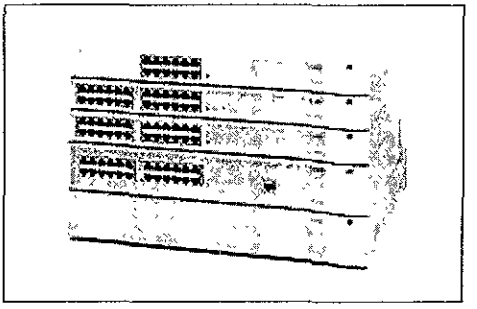
Por último, una consideración importante que se debe tomar en cuenta cuando se instalan repetidores, es la llamada regla Ethernet 5-4-3.

Las especificaciones 10Base5 y 10Base2 (coaxial) para repetidores son representadas por la Regla 5-4-3 que establece "Un paquete de datos cruzará no más de 5 segmentos físicos y es retransmitido por no más de 4 repetidores y sólo 3 de los cinco segmentos pueden ser poblados con dispositivos.

Dicha Regla se muestra representada en la siguiente figura:



4.5.2 Concentradores



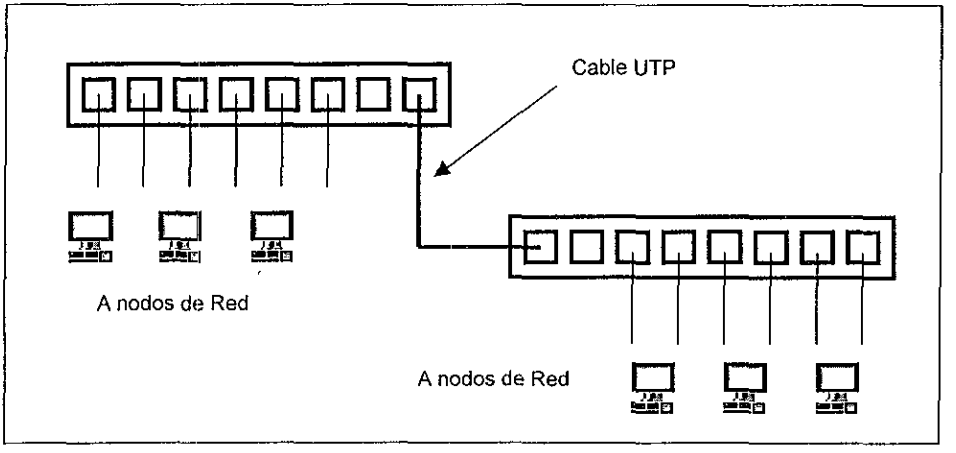
SuperStack® II PS Hub

Comúnmente conocidos como hubs, estos elementos se basan en el principio de interconexión más básico. Podemos considerarlos como un armario de conexiones donde se centralizan todas las conexiones de una red, o sea un dispositivo con

entradas y salidas, que no hace nada más que centralizar conexiones.

Suelen utilizarse para instalar topologías físicas en estrella, pero funcionando como un anillo o un bus lógico.

Los concentradores son dispositivos que se encuentran físicamente separados de cualquier nodo de la red. Aunque algunos se conectan a un puerto de expansión en un nodo de la red, también pueden llegar a conectarse varios concentradores entre sí, con la finalidad de permitir nodos adicionales, como se muestra en la siguiente figura:



El cable que se usa para conectar a los concentradores es el mismo que usa entre el concentrador y los nodos de red, ambos usan cable UTP (10BASE-T) y clavijas RJ45 para la conexión.

El primer concentrador para red surgió como una respuesta a los problemas de cableado existentes en las redes Ethernet con cable coaxial, en 1985 Xerox Corporation comenzó el desarrollo de lo que sería el primer concentrador para Ethernet; *posteriormente en 1988 sale el primer concentrador comercial para*

Ethernet desarrollado por SynOptics Comunications, poco tiempo después se fabricaron concentradores para soportar los protocolos Token Ring, FDDI, y recientemente ATM.

Un concentrador inteligente es el punto central del cableado de una red, ya que aquí, es desde y hacia donde fluyen todas las comunicaciones de una red. Además posee la inteligencia para ser administrado vía software.

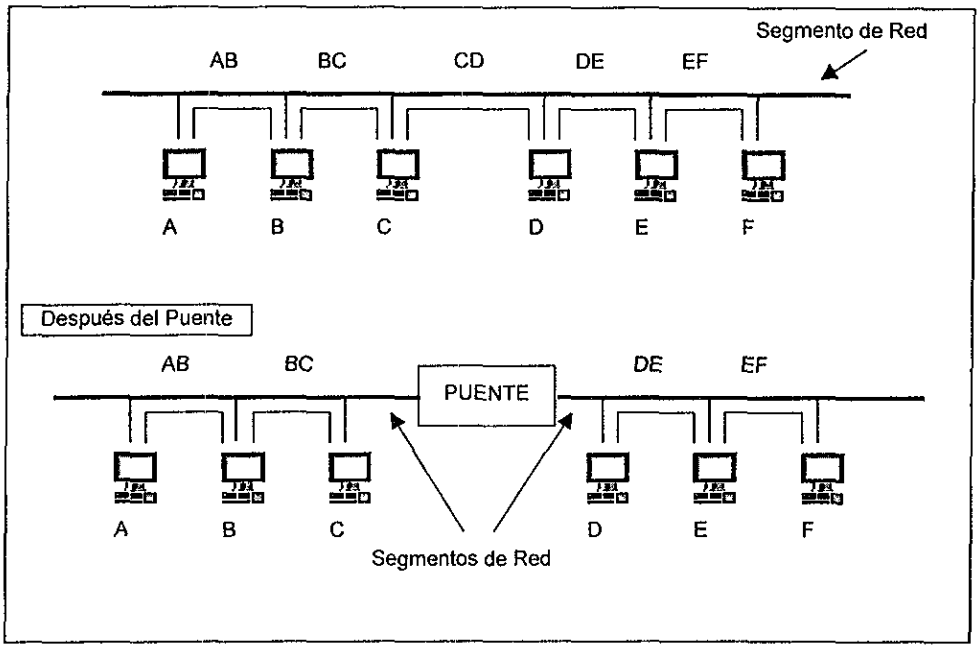
Cuando la base instalada de una red empieza a crecer, instalar un concentrador inteligente es la mejor opción que tienen los administradores para mantener un control adecuado. Una de las razones para elegir un concentrador inteligente es su capacidad de administración, ya que da control absoluto sobre los diferentes recursos y sistemas que se encuentran en la red.

Este tipo de concentradores puede encontrarse en dos modalidades: Modulares y No Modulares. Los modulares son utilizados para pequeños grupos de trabajo que pueden ser interconectados entre sí y que soportan un solo protocolo como Ethernet, Token Ring, FDDI o ATM. Los no modulares permiten integrar en un solo chasis varios métodos de acceso y múltiples protocolos como Ethernet, Token Ring, y FDDI; y que además permiten integrar dispositivos adicionales para dar a la red servicios adicionales como puentes, ruteadores, switches conexiones a host, servidores en el mismo chasis, etc.

4.5.3 Puentes

Los puentes o "bridges" son dispositivos que operan en la capa de enlace de datos del modelo OSI. No analizan los campos de datos. Los puentes, delimitan el tráfico entre redes a las redes que tienen acceso directo y deben preservar las características de las LAN's que interconectan (retardo de transmisión, capacidad de transmisión, probabilidad de pérdida, etc.). Estos elementos filtran el tráfico en

función de una tabla de direcciones. La decisión si son transmitidos hacia delante o no, se toma en función de la dirección destino que halla en cada paquete. Los puentes revisan la dirección asociada con cada paquete de información, si la dirección es la correspondiente al otro segmento de la red, el puente pasará el paquete al siguiente segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del mismo segmento de red actual, no pasará el paquete al otro lado, como se muestra en la siguiente figura:



Los puentes suelen emplearse para reducir la cantidad de tráfico en un segmento de la red. Mediante la división de un solo segmento de red en dos segmentos y conectándolos por medio de un puente, se reduce el tráfico general en la red.

Hay tres tipos de puentes, simple, transparente y de encaminamiento de fuente.

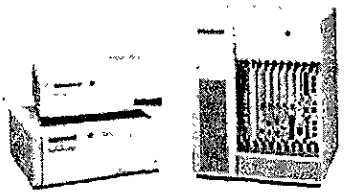
En el puente simple, la tabla de direcciones está basada en un conocimiento previo. Las ventajas que tiene son la velocidad y la simplicidad pero peca de falta de flexibilidad y de que el número de estaciones depende del tamaño de la tabla.

Los puentes transparentes, operan en el nivel MAC, es decir utilizando las direcciones físicas de las interfaces de red. Su inicialización es automática y realiza funciones de reenvío de tramas, de autoaprendizaje de las estaciones de la red, y de resolución de los posibles bucles que existan en la topología de la red.

Los puentes de encaminamiento de fuente se desarrollaron por el comité IEEE 802.5. La estación origen, determina la ruta que seguirá la trama e incluye esta información en la misma en forma de identificadores de puentes y de LAN's. De manera que un puente retransmite la trama si su identificador está en la ruta designada, sino, la desecha. En este tipo de puentes no se requieren tablas de encaminamiento en los puentes ya que éste únicamente debe conocer sus identificadores. La ruta que escoge la estación origen hasta cualquier destino viene dada por unos modos de direccionamiento y unas directrices de enrutado.

Ejemplos de puentes pueden ser los de la familia 3Com NETBuilder:

- IB/2000 Puente local Ethernet (10 Base 2, 10 Base 5).
- IB/3000 Puente remoto (interfaces RS-232, V-35 a líneas serie de 9.6 Kbps a 2048 Mbps).



NETBuilder II Intelligent Bridge/Router

4.5.4 Ruteadores

También conocidos como "routers", *actúan en la capa* de red del modelo OSI, ofrecen un servicio más sofisticado que un puente ya que puede seleccionar uno de entre varios caminos según parámetros de los equipos como retardo de transmisión, congestión, etc.

Estos dispositivos, dependen del protocolo usado. En la capa de red se controla el tiempo de vida de un paquete, el tiempo requerido para que un paquete vaya de un punto a otro de la Internet (interconexión de redes) hará que el tamaño máximo de ésta sea mayor o menor.

Los ruteadores requieren por lo general que cada red tenga el mismo Sistema Operativo de Red (NOS). *Con un NOS común*, el ruteador puede ejecutar funciones más avanzadas de las que podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring

Por ejemplo, para la interconexión de una LAN con una WAN, podemos usar el ruteador Proteon p4100 ya que soporta: Interfaces LAN (IEEE 802.5 4/16 y IEEE 802.3), Interfaces WAN (DDS – 64 Kbps, T1 – 1544 Kbps, X.25), múltiples protocolos de alto nivel (TCP/IP, Netware IPX, XNS, DECNet, AppleTalk), protocolos de intercambio de información entre ruteadores (IGP, EGP, OSPF).

El Proteon p4200 FDDI tiene unas características semejantes pero con FDDI backbone.

Para una interconexión LAN – LAN a través de una WAN podemos usar el ACS 4100 *Puente/Ruteador, que conecta* una red Ethernet (10 Base5, 10 Base2 ó 10 BaseT) a uno o dos enlaces WAN, para líneas punto a punto o X.25.

El ACS 4400 Puente/Ruteador, conecta 4 redes Ethernet (10 Base5, 10 Base2 ó 10

BaseT) a como máximo 8 enlaces WAN, soportando 802.1 Spanning Tree, TCP/IP, XNS, DECNet.

El Cisco TRouter es un ruteador multiprotocolo, puede actuar de servidor de terminales: hasta 16 dispositivos asíncronos de velocidad hasta 34.4 Kbps, proporcionando acceso remoto para conexión de múltiples dispositivos asíncronos. Cisco Trouter proporciona interfaces a: Ethernet / IEEE 802.3 y enlaces serie (HDLC, LAPB, X.25). Soporta los protocolos de enrutado (TCP/IP, DECNet, XNS, IPX, AppleTalk).

Puentes Vs. Routers

La diferencia entre puentes y ruteadores es realmente la diferencia entre la capa de enlace del modelo OSI y los servicios de la capa de red del mismo modelo OSI. Los puentes fueron hechos para puentear segmentos LAN; los routers fueron creados para conectar LAN's o redes en inter-redes.

Principales diferencias entre los Puentes y los Ruteadores

Puentes	Ruteadores
Rápidos	Mayor procesamiento
Menor filtraje	Sólo el tráfico necesario
Basados en direcciones MAC	Basados en direcciones lógicas
Conversión Ethernet-Token Ring	Transparencia a la topologia

4.5.5 Brouter

Son Dispositivos que combinan las funciones de un puente y de un ruteador. Tiene la capacidad de encaminamiento de un ruteador y la velocidad de procesado de un puente. Un brouter, es independiente del protocolo, pero puede dirigir el tráfico de

una LAN a otras redes dependiendo del protocolo.

Un ejemplo de brouter sería el Halley ConnectLAN 202, que es un dispositivo de interconexión de Token Ring, usando una tabla de encaminamiento y participando en el descubrimiento real de las rutas.

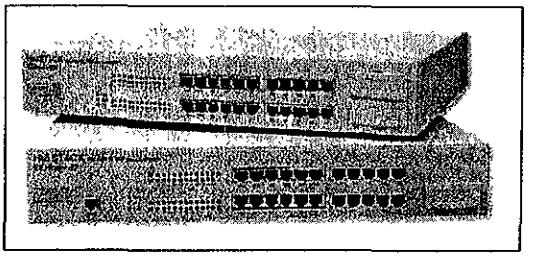
Otro brouter podría ser la familia 3Com NETBuilder con sus dispositivos BR/2000 y BR/3000, que además filtran el tráfico en función de la dirección de trama, del protocolo (XNS, IP, ...), de la longitud de trama. También autorizan retransmisiones de tramas especificas y soportan XNS (IDP, RIP), TCP/IP (IP, EGP, RIP, ICMP, AP), OSI (CLNP), actuando de puente para los otros protocolos.

4.5.6 Compuertas

Las compuertas o "Gateway", actúan como un traductor entre protocolos incompatibles; trabajan en todas las capas del modelo OSI, sin embargo la utilización más típica es en niveles superiores, a partir de la capa 4. Este dispositivo tiene como función interconectar redes totalmente distintas. Aunque cuando hablamos de gateways en el ámbito de LAN estamos haciendo referencia a los ruteadores. Podría tenerse por ejemplo, una LAN que consiste en computadoras compatibles con IBM y otra LAN que consiste en computadoras Macintosh. En este caso, un gateway permitiría que las computadoras IBM compartieran archivos con las Macintosh. Algunos tipos de gateways también permiten que se compartan impresoras entre las dos redes.

El gateway es un CPU y aplicaciones de memoria intensiva y sólo debe ser utilizado si no existe otra opción. Cuando es usado para traducir protocolos de transporte (IPX/SPX a TCP/IP por ejemplo) se crean cuellos de botella en las inter-redes.

4.5.7 Interruptor

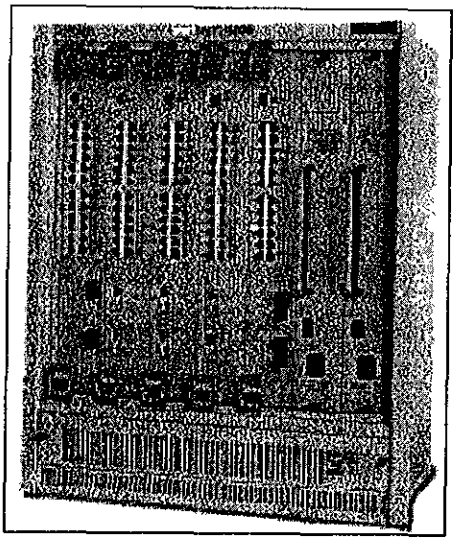


Fast Ethernet Stackable Hubs - Cabletron

En una red estándar, cada nodo sigue un esquema de Control de Acceso a Medios (MAC), como Ethernet o Token Ring, que permite compartir los tiempos de acceso en el cable. Entre más nodos hay en una red, será menor la cantidad de tiempo que cada uno de ellos va a necesitar para las transmisiones. Un interruptor aísla y canaliza los datos, de modo que cada nodo tiene acceso ilimitado al cable y una mejora radical en el desempeño.

Una subcategoría de interruptores, denominada "Interruptores Inter-redes", está diseñada para encadenar una red de interruptores. Tiene más puertos, más poder de procesamiento y, ciertamente, conexiones para crear redes de área amplia (WAN).

Actualmente este tipo de equipo está adquiriendo gran importancia, debido a la gran aceptación que está teniendo la tecnología ATM, la cual permite transmitir datos voz y video a través de un mismo medio de transmisión además de lograr que ésta sea a grandes velocidades mejorando considerablemente el desempeño de la red.



SmartSwitch 6000 - Cabletron

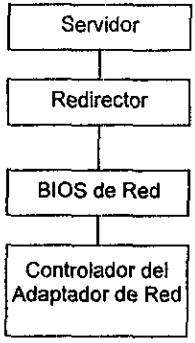
4.5.8 Sistema Operativo de Red

El Sistema Operativo de Red, es el software que contiene todos los elementos básicos para compartir recursos. Algunos productos separan en forma muy clara al cliente y al servidor, en cuanto a software y funciones.

El Sistema Operativo de Red perfecto afina el servidor, al administrar su memoria, y aloja las tareas a través de múltiples procesadores (en caso de tenerlos), con lo cual proporciona capacidad para crecer. El Sistema Operativo de Red incluye funciones administrativas que permiten mejorar su confiabilidad, y utilizar formatos de disco y técnicas de caché, que le dan un mayor acceso. La mayoría de los Sistemas Operativos de Red incluyen programas de utileria que establecen conexiones de red, administran las cuentas, las contraseñas de los usuarios y los recursos compartidos en los servidores.

Dado que cada Sistema Operativo de Red es diferente; los comandos requeridos para iniciar la red también son diferentes.

La siguiente figura muestra las diferentes capas que componen el software de red. El software de cada capa (a excepción del controlador de red) se considera como parte del Sistema Operativo de Red.



El software controlador del adaptador de red se comunica directamente con la tarjeta de red. El sistema básico de entrada /salida (BIOS) de red incluye las funciones incluye las funciones con las que el Sistema Operativo de Red envía y recibe información. En la parte medular del Sistema Operativo de Red está un programa llamado redirector, el cual intercepta las peticiones de lectura y escritura y las redirecciona hacia el dispositivo adecuado, ya sea una unidad de disco en la computadora local o una unidad de disco en alguno de los servidores de red. Por último, si la computadora es un servidor, el programa servidor proporcionará la capacidad para que el nodo comparta sus recursos con los demás.

Cada capa del software de red pasa información a la siguiente capa en un formato específico esperado por la siguiente capa. En caso contrario, la comunicación dentro del software de red falla y la red llega a ser inoperable.

CAPÍTULO 5

CONCLUSIONES

5 CONCLUSIONES

Como resultado de la elaboración del presente trabajo de tesis, concluimos que la investigación cumple con el objetivo original de mostrar los elementos requeridos para establecer un nuevo concepto, el de "Infraestructura de Administración Avanzada de Redes de Computadoras"; que incluye temas como: Distribución de Software, Control de Inventarios, Metodología de Trabajo, Recursos Humanos y Capacitación, entre otros, que si bien se tiene conocimiento de ellos, generalmente no se les da la debida importancia y en muchos casos no son considerados por el administrador de una red. Consideramos que todo administrador de redes debe tener presente los parámetros que conforman una Infraestructura de Administración Avanzada para poder brindar un valor agregado a sus redes, logrando con esto ofrecer un mejor servicio a los usuarios.

Por otra parte, estamos convencidos de que este trabajo cumple también con el objetivo de ser una valiosa herramienta de introducción para todos aquellos interesados en conocer el fascinante mundo de las redes de computadoras, ya que la forma en que está escrito el trabajo, permite una buena comprensión y entendimiento de los temas, facilitando al lector su lectura.

Como un elemento adicional, este trabajo de tesis es una guía en la cual se consideran diferentes aspectos, ya que aún cuando existe mucha información sobre redes de computadoras, ésta se encuentra dispersa a través de una gran cantidad de obras y no existe una literatura que contemple en forma general y conjunta todos los aspectos de la Administración Avanzada de Redes, siendo de gran utilidad para los administradores de red que esperan contar con una obra de este tipo.

Durante el desarrollo de esta investigación nos dimos cuenta de la importancia que tiene la administración de una red y todo lo que ello implica. Sin una administración adecuada, el control y detección de fallas no pueden ser atendidos en forma oportuna ocasionando que los recursos de la misma no sean utilizados adecuada y

eficientemente sin brindar un buen servicio al usuario. Para llevar a cabo esta tarea en forma óptima, es necesario tomar en cuenta todas las características y parámetros de la red y de la organización en la que opera, con la finalidad de seleccionar la mejor opción para cada una de las necesidades que se requieren, de lo contrario no se aprovecharían todos los servicios que ofrece la red.

Finalmente, estamos convencidos de que este trabajo de tesis sirve como apoyo a aquellos administradores de redes tanto pequeñas como grandes que desean documentar, organizar, proyectar su red y no tienen un enfoque claro. Creemos que los conceptos y elementos que se incluyen serán vigentes en un mediano plazo, en tanto no exista un cambio sustancial dentro del extenso campo de las redes de computadoras.

ANEXOS

SERVICIOS DE RED

La finalidad de una red es que los usuarios de una empresa puedan hacer un mejor uso de los recursos e información mejorando de este modo el rendimiento global de ésta. Así obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- Facilidad de comunicación.
- Mejora de la dinámica de grupo.
- Reducción del presupuesto para proceso de datos.
- Reducción de los costos de proceso por usuario.
- Administración de los programas.
- Integridad de los datos.
- Mejora en los tiempos de respuesta.
- Facilidad de uso.
- Seguridad.

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son:

Acceso

Los servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario para determinar cuales son los recursos de la misma que puede utilizar, como servicios para permitir la conexión de usuarios de la red desde lugares remotos.

Control de acceso

Para el control de acceso, el usuario debe identificarse conectando con un servidor en el cual se autentifica por medio de un nombre de usuario y una clave de acceso.

Si ambos son correctos, el usuario puede conectarse a la red y utilizar los recursos que le corresponden.

Acceso remoto

En este caso, la red de la organización está conectada con redes públicas que permiten la conexión de estaciones de trabajo situadas en lugares distantes. Dependiendo del método utilizado para establecer la conexión el usuario podrá acceder a unos u otros recursos.

Servidor de Archivos

El servidor de archivos consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones.

El servidor de archivos debe desempeñar las siguientes funciones:

- Controla el acceso actual.
- Convenio de licencias.
- Optimización de acceso.
- Rentabilidad.
- Acceso Transparente.
- Interfaces.
- Transferencias de archivos.
- Seguridad.
- Comunicaciones nodo a nodo.

Impresión

Permite compartir impresoras de alta calidad, capacidad y coste entre múltiples usuarios, reduciendo así el gasto. Existen equipos servidores con capacidad de almacenamiento propio donde se almacenan los trabajos en espera de impresión, lo cual permite que los clientes se descarguen de esta información con más rapidez.

Para estos casos es conveniente un servidor de impresión, que es un sistema de software llamado "spooler". Un spooler es una interface entre usuarios que requieren el servicio de impresión. El spooler maneja los trabajos por la posición que tengan en la cola de impresión, establece prioridades de impresión de trabajos, imprime trabajos desde la cola sobre la impresora disponible y proporciona una administración de impresión de trabajos.

Una variedad de servicio de impresión es la disponibilidad de servidores de fax, los cuales ponen al servicio de la red sistemas de fax para que se puedan enviar éstos desde cualquier estación. En ciertos casos, es incluso posible enviar los faxes recibidos por correo electrónico al destinatario.

Correo

El correo electrónico es la aplicación de red más utilizada. Permite claras mejoras en la comunicación frente a otros sistemas. Además tiene un costo mucho menor para transmitir iguales cantidades de información. Frente al correo convencional tiene la clara ventaja de la rapidez.

Usando el correo electrónico es posible enviar archivos completos además de mensajes a otro usuario según la necesidad. Es posible recibir correo sin estar presente para recibirlo. El sistema guarda el mensaje en forma automática, hasta que uno está listo para recibirlo.

Cada mensaje de correo electrónico tiene una forma similar a los mensajes utilizados en un memorándum, la persona a quien está dirigido, la fecha y la hora en que se envió y el propósito del mismo.

Otros

Las redes más actuales, con grandes capacidades de transmisión, permiten transferir contenidos diferentes de los datos, como pueden ser imágenes o sonidos. Esto permite aplicaciones como:

- Estaciones integradas (voz y datos).
- Telefonía integrada.
- Servidores de imágenes.
- Videoconferencia de sobremesa.

MATRIZ DE COSTOS

Uno de los elementos importantes que se deben considerar en la instalación de una red, es sin duda, el costo relacionado con la implantación de la misma, ya que en la mayoría de las ocasiones es el costo el que determina las características propias de la red, así como los servicios que ésta puede ofrecer

Hablar de una matriz de costos implica determinar en primera instancia el tipo de red que se desea implantar ya que no es lo mismo una red ethernet de unas cuantas PC´s, que una red con muchos nodos y que maneja enlaces a alta velocidad, como por ejemplo una red ATM, por lo tanto, es importante clarificar el alcance y dimensión de la red que se pretende armar y obtener su costo.

Como ejemplo, se presenta a continuación el caso de una pequeña empresa que desea instalar una red de tipo ethernet con 10 PC´s, 1 servidor y 1 impresora láser. La matriz de costos típica para este tipo de redes puede ser como la que se muestra a continuación:

Cantidad	Descripción	Precio unitario (Dólares)	Total (Dólares)
1	Servidor	35000.00	35000.00
10	PC´s	9000.00	90000.00
1	Impresora Láser	17000.00	17000.00
11	Tarjetas de Red	850.00	9350.00
1	Hub de 12 puertos	16500.00	16500.00
1	Sistema Operativo de Red	10500.00	10500.00
1	Cableado de la Red	8000.00	8000.00
	TOTAL		*186350.00*

Como se puede apreciar, existen elementos que pueden ser descartados como es el caso de las PC´s, si éstass ya se tienen y únicamente considerar los elementos de interconectividad necesarios, como es el caso de las tarjetas de red, el cableado y el

hub.

En este tipo de redes el objetivo es que todas la PC´s puedan compartir el servidor de impresora, ya que el costo de mantener una impresora por cada estación de trabajo resulta excesivo comparado con la instalación de una red, además de los servicios adicionales que ésta agrega, como es el poder compartir archivos e incluso servicios de correo electrónico.

Para el caso de redes pequeña, la matriz de costos representa un estudio sencillo y claro de los requerimientos de comunicación para la puesta en operación de una red, pero cuando se trata de redes de gran tamaño la cuestión no es tan sencilla, en este caso hay que determinar en primera instancia el número de usuarios que se desea conectar, ya que ello determinará las características de los equipos.

Como ejemplo de este tipo de redes, a continuación se mostrará el estudio de una organización que pretende instalar una red ATM y así conectar 4000 computadoras dentro de toda la organización. La determinación de la matriz de costos consiste en establecer las características de los equipos requeridos y solicitar cotizaciones a diversos proveedores con el fin de especificar la conveniencia de adquirir un determinado equipo.

Como nota adicional, no se dan más detalles acerca de esta red, ya que no es el caso de estudio que nos ocupa, sino el poder apreciar la utilidad que tiene el realizar un estudio comparativo de los equipos desde el punto de vista económico.

Comenzaremos entonces por analizar las características del equipo requerido:

Modulo I Switch ATM con 5 puertos a 622 Mbps y 8 puertos a 155 Mbps.
Modulo II LAN Switch con 5 puestos a 155 Mbps y 6 puertos a 100 Mbps.
Modulo III LAN Switch con 1 puerto a 100 Mbps Fibra, 10 puertos a 100 Mbps UTP y 48 puertos a 10 Mbps.

Modulo IV Concentrador de 24 puertos a 10 Mbps

Una vez determinadas las características de los equipos, el paso siguiente es realizar un comparativo de precios de diferentes fabricantes que cumplan con las opciones requeridas, por lo cual se tiene la siguiente tabla comparativa:

Precios en Dólares Americanos			
	FORE	CISCO	CABLETRON
Modulo I	101225.00	80511.62	126684.84
Modulo II	40240.00	63345.00	35888.33
Modulo III	41700.00	68340.00	34240.59
Modulo IV	2599.16	2599.16	3264.22

Con esto, ya se tienen los elementos para poder determinar el costo aproximado de la red que se ha planteado, únicamente falta por indicar las cantidades de equipo que se requieren de cada modulo, para el caso particular de esta red las cantidades requeridas son mostradas en la siguiente tabla, junto con los costos totales de cada modulo.

Precios en Dólares Americanos				
	Cantidad	FORE	CISCO	CABLETRON
Modulo I	5	506125 00	402558.10	633424.20
Modulo II	26	1046240.00	1646970.00	933096.58
Modulo III	104	4336800.00	7107360.00	3561021.36
Modulo IV	26	67578.16	67578.16	84869.72
TOTAL		**5956743.16**	**9224466.26**	**5212411.86**

Como se puede ver en la tabla anterior, el elaborar una matriz de costos permite tener entre otras cosas un panorama general del costo aproximado de la instalación de una red, lo cual para la organización representa una valiosa ayuda en la toma de decisiones.

Existen otros elementos que se deben considerar en la instalación y puesta en operación de una red, adicional al costo de los equipos de comunicaciones, también se debe agregar el costo total del cableado de la red y por su puesto el costo del software de administración de la red. En caso de que esté no venga incluido en el costo total del equipo.

La elaboración de una matriz de costos, para el caso de una red de computadoras puede ser muy variada y se pueden llegar a seguir diferentes caminos, los casos mostrados aquí representan solo una forma en la cual se pueden llevar a cabo, y en mucho dependerá de las necesidades específicas de cada red en particular y de algunos casos de la experiencia que tenga el administrador de red en la realización de su estudio de costos.

GLOSARIO

GLOSARIO

Activex: Lenguaje de programación al estilo de Java propuesto por Microsoft.

Alias: Mote que utiliza una persona o grupo de personas de la red para hacer más fácil su localización o para distinguirse de otros.

Ancho de banda (bandwidth): Capacidad máxima de transmisión de un enlace. Usualmente se mide en bits por segundo (bps). Es uno de los recursos más caros de toda red y es uno de los temas principales hoy en día pues el ancho de banda es una limitante para el desarrollo de aplicaciones que requieren transferir grandes cantidades de información a muchos puntos diferentes (multimedia, por ejemplo).

Archie: Herramienta de software utilizada para localizar archivos en servidores FTP. A partir de 1994 ha ido cayendo en desuso debido al auge del *World Wide* Web.

ARCNET (Attached Resource Computer Network; Red de computadoras con recursos asignados): Red local desarrollada por Datapoint Corporation que utiliza una tecnología de acceso Token Passing y que tiene una velocidad de transferencia de 2.5 Mbps.

ARPANet (Advanced Research Projects Agency Network; Red avanzada de agencias para proyectos de investigación): Red precursora de la actual Internet. Fue desarrollada en la década de 1960 por el departamento de defensa de Estados Unidos.

ASCII (American Standard Code for Information Interchange; Código americano estándar para intercambio de información): Estándar que define

cómo representar dígitos, letras, signos y signos de puntuación en computadoras (por ejemplo, la A mayúscula corresponde al código número 65). Aunque existen otros estándares, el ASCII es el más popular.

Autenticación: Proceso mediante el cual se comprueba la identidad de un usuario en la red.

Backbone (espina dorsal de red): Es la infraestructura de conexión principal de una red y está constituida por los enlaces de mayor velocidad dentro de dicha red.

Baud: Unidad de medida que indica el número de veces que una señal portadora cambia de valor. Su uso más común es en la industria de los modems y las comunicaciones seriales. No debe ser confundido con la velocidad en bps pues, aunque en los primeros modems el numero de bauds correspondía a los bps, actualmente los modems de alta velocidad logran transferencias de hasta 28,800 bps sin que ello signifique que trabajan a 28,800 bauds.

Beaconing: Proceso que se da dentro de una rutina de recuperación después de la perdida de una ficha (token). En este proceso se identifica un maestro del sistema.

Binhex (BINary HEXadecimal; Hexadecimal binario): Método para convertir archivos binarios en archivos ASCII. Se utiliza para poder enviar archivos binarios a través de correo en Internet pues muchos de los servidores de correo de la red sólo pueden manejar mensajes en ASCII. Normalmente se necesitan dos pasos para ello: el remitente convierte un archivo binario en ASCII y lo manda como correo, entonces el destinatario realiza el proceso inverso para reconstruir el archivo original.

BITNET (Because It's Time NETwork; Porque es tiempo de red): Red internacional de computadoras de instituciones educativas. Esta red está

conectada a Internet y algunas de las herramientas más comunes hoy en día, como los servidores de correo Listservs, se originaron en ella. Actualmente está en proceso de desaparición conforme sus miembros se integran a Internet.

Bps (Bits per second; Bits por segundo): Unidad de medida que indica los bits por segundo transmitidos por un equipo.

Browser (Navegador): Programa usado para accesar diferentes tipos de recursos en Internet. Los más famosos hoy en día son los browser de WWW (Netscape, Internet Explorer, Mosaic, etc.) y suelen trabajar con una arquitectura cliente/servidor.

BTW (By The Way; A propósito): Abreviación muy utilizada en los foros de discusiones de la red. Se podría traducir al español como "a propósito" o "por cierto".

Cableado: Columna vertebral de cualquier sistema de red, ya que lleva la información de un nodo a otro.

Cable Coaxial: Cable consistente en un conductor cilíndrico externo hueco que cubre a un alambre conductor único. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales digitales, y cable de 75 Ohms, para señales analógicas y para señales de alta velocidad.

Cable telefónico: Cable formado principalmente por dos alambres de cobre que se encuentran aislados por una cubierta plástica y torcidos uno contra el otro, por lo que también se les llama de par torcido (twisted pair). Son sumamente económicos, flexibles y permiten manipular una señal a una distancia máxima de 110 metros sin el uso de amplificadores.

CGI (Common Gateway Interface; Interfase común de acceso): Conjunto de

reglas que definen como se realiza la comunicación entre un servidor Web y cualquier otro programa (llamado por ello programa CGI) en la misma máquina. Un programa CGI se utiliza para sacar o meter datos del servidor Web.

Ciberespacio: Termino acuñado por William Gibson en la novela "Neuromancer" y utilizado frecuentemente para referirse al mundo digital creado y constituido por las redes de computadoras, en particular por Internet.

Codificador: Un programador principiante o en entrenamiento que escribe programas simples, el código para programas más extensos que ya fueron diseñados por otra persona.

Código: Un conjunto de símbolos de máquina que representa datos o más instrucciones . También puede ser, cualquier representación de un conjunto de datos por medio de otros.

Código binario: Es un sistema de codificación constituido por dígitos binarios.

Cookie: Mecanismo utilizado para que un servidor Web pueda guardar y leer información en la computadora que corre el software cliente. Se utiliza para conocer las preferencias de los usuarios, para acceso a servidores que requieren de autenticación, etc.

Correo electrónico (e-mail): Correo enviado a través de medios electrónicos. Aunque originalmente se trataba de mensajes de texto, actualmente puede cualquier otro tipo de información.

CSMA/CD (Carrier Sensing Muliple Access/Colition Detection - Acceso múltiple del sentido de transporte/Detección decolisiones): En este protocolo de acceso, que se utiliza en redes Ethernet, un mensaje se transmite por cualquier estación o nodo de la red en cualquier momento, mientras la línea de

comunicación se encuentra sin tráfico. Es decir, antes que ese nodo transmita, toma un tiempo para verificar que ningún otro lo esté haciendo. Por lo tanto, el primer mensaje que se envía es el primero en atenderse.

Cuenta dial-up (marcación directa): Cuenta de Internet que permite la conexión vía modem a la red. Normalmente requiere de la contratación con un ISP (Internet Service Provider; Proveedor de servicios de Internet) quien cuenta con una conexión dedicada a la red y revende el acceso a través de bancos de modems.

Database front end (Base de datos frontal): interfase que permite la integración de servidores Web con bases de datos.

Decodificador: Cualquier dispositivo de hardware o programa de software que convierte una señal codificada a su forma original.

Demodular: Reconvertir una señal modulada a su forma original, extrayendo los datos de la frecuencia portadora.

Digital: Tradicionalmente, el uso de números, que proviene de dígito o dedo. En la actualidad, digital se ha hecho sinónimo de computadora.

Dirección IP (Internet Protocol; Protocolo Internet): Dirección única de un dispositivo en una red TCP/IP. Consiste de cuatro números entre 0 y 255 separados por puntos (por ejemplo 200.132.5.45).

DNS (Domain Name System; Sistemas de nombres de dominio): Sistema para hacer más fácil la administración y localización de direcciones IP que funciona asignando uno o más alias a cada dirección IP. También suele llamarse así a las computadoras encargadas de administrar la base de datos del sistema de nombres de dominio. Cuando alguien pide, por ejemplo, localizar la computadora

computadora@dominio, su servidor DNS convierte ese nombre en la dirección IP correspondiente. Otra aplicación del DNS es la creación de nombres de dominio para correo. Por ejemplo, supóngase que la compañía XYZ, S.A. de C.V. requiere de direcciones de correo electrónico para sus empleados pero no quiere instalar una red propia. Entonces lo que hace es contratar los servicios de un ISP el cual tramita un nombre de dominio y crea en sus computadoras las cuentas respectivas. Así pues, podrá mandarse correo a adamian@xyz.com.mx sin ningún problema.

Download (Descargar): Nombre que recibe el proceso de transferencia de archivos desde una computadora remota hacia la computadora del usuario

Electronic mall (Centro comercial electrónico, Centro comercial virtual): Sitio donde se pueden comprar productos y servicios en línea. Normalmente se trata de un servidor Web que simula un centro comercial.

Emoticon: Símbolos utilizados en el correo electrónico para dar énfasis o para dejar claro el sentido de una frase o palabra, para verlos normalmente es necesario girar la cabeza hacia la izquierda. Algunos de los emoticones más comunes son: :=) sonrisa :=(tristeza

Encripción: Procedimientos para codificar información de manera que pueda transmitirse sin peligro de ser interceptada o alterada antes de que llegue a su destinatario.

Ethernet: Red local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation que utiliza el protocolo de contención CSMA/CD y que tiene una velocidad de transferencia de 10 Mbps.

Extensiones del sistema operativo de red: Definen lo "abierto" del sistema. Las extensiones que comúnmente se ofrecen en los sistemas operativos de red, por lo

general son manejadores de productos de alto nivel que efectúan operaciones, tales como traslado entre protocolos de acceso de archivos que requieren los diferentes sistemas operativos de usuarios o estaciones.

FAQ (Frequently Asked Questions; Preguntas más frecuentes): Un FAQ es un archivo con las respuestas a las preguntas más comunes sobre algún tema. Una de las reglas básicas de Internet es leer primero el FAQ respectivo antes de expresar cualquier duda.

FDDI (Fiber Distributed Data Interface; Interfase de datos distribuidos por fibra): Estándar para transmisión por medio de fibra óptica a velocidades de hasta 100 Mbps

Fibra óptica: Un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen capacidades de transmisión enormes, del orden de miles de millones de bits por segundo.

Finger: Software utilizado para localizar a alguien en Internet. Con finger puede averiguarse si una persona posee o no cuenta en una computadora de la red. Muchas máquinas no permiten peticiones de finger como medida de seguridad.

Filtro de correo (mail-filter): Programa que permite el filtrado de mensajes de correo electrónico de acuerdo a la información contenida en el encabezado de cada mensaje.

Firewall (pared de fuego): Mecanismo utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Una firewall puede construirse con software, con hardware o con una combinación de ambos.

Flame (Flama): Mensaje reprobatorio, de censura o violento contra alguien en la red. Muchas veces se convierte en la versión electrónica del insulto personal.

Flame War (Guerra de flamas): Estado al que llega una discusión en el ciberespacio cuando lo único que hacen sus participantes es atacarse personalmente o incluso insultarse en lugar de "hablar" civilizada y razonablemente.

Freenet: Organizaciones encargadas de buscar el acceso a Internet por parte del público en general. Pueden proporcionar sus servicios de manera gratuita o mediante el pago de cuotas muy pequeñas ya que tienen otras fuentes de financiamiento.

Freeware: Software que ha sido puesto a disposición de la comunidad por sus autores. Este tipo de programas pueden ser libremente distribuidos y utilizados sin necesidad de pago alguno.

FTP (File Transfer Protocol: Protocolo de transferencia de archivos): Como su nombre lo indica, define los mecanismos y reglas para transferir archivos entre las diversas computadoras de la red

FTP anónimo: Transferencia de archivos desde un servidor FTP que no requiere de cuenta de usuario en el mismo para poder leer información. El FTP anónimo permite la creación de áreas públicas en un servidor FTP para que cualquier persona pueda bajar los archivos hacia su computadora. En realidad si se requiere un nombre de usuario y contraseña, aunque los modernos browser hacen automáticamente este proceso: Nombre de usuario: anonymous Contraseña: nombre del usuario (por ejemplo, hjuarez@spin.com.mx)

Gateways (Puerta de acceso): Los gateways son una compuerta de intercomunicación que operan en las tres capas superiores del modelo OSI (sesión, presentación y aplicación). Ofrecen el mejor método para conectar segmentos de red y redes a mainframes. Se selecciona un gateway cuando se

tienen que interconectar sistemas que se construyeron totalmente con base en diferentes arquitecturas de comunicación.

GIF (Graphics Interchange Format; Formato de intercambio de gráficas): Formato para imágenes gráficas. Es el estándar de facto en Internet.

Gopher: Herramienta para organización de información en Internet. Puede verse como un precursor del Web y, aunque lentamente está desapareciendo, aún quedan miles de servidores Gopher en servicio. De hecho, muchos navegadores como Netscape tienen un cliente Gopher por si usted se topa con alguno.

Hardware (materia física): Conjunto de componentes físicos de una computadora.

Hiperliga: Instrucciones en un documento HTML que permiten "brincar" hacia otro lugar del documento, otro documento en el mismo servidor o incluso otro documento en otro servidor.

Hipermedia: Extensión del concepto de hipertexto para la inclusión de multimedia (sonido, gráficas y vídeo)

Hipertexto: Termino usado por Ted Nelson para referirse a un sistema no lineal de búsqueda y recuperación de información que actúa mediante hiperligas.

HTML (HyperText Markup Language; Lenguaje de marcación de hipertexto): Lenguaje utilizado para la creación de documentos de hipertexto e hipermedia. Es el estándar usado en el World Wide Web.

HTTP (HyperText Transport Protocol; Protocolo de transporte de hipertexto): Protocolo para transferir archivos o documentos hipertexto a través de la red. Se basa en una arquitectura cliente/servidor.

Home page (Página de casa): Es la página principal de un sitio web (web site).

Hotlist: Lista de URLs más utilizados por un usuario o grupo de usuarios.

IEEE (Institute of Electrical and Electronic Engineers; Instituto de ingenieros eléctricos y electrónicos): Asociación de ingenieros que definen normas para estándares de comunicación.

IETF (Internet Engineering Task Force; Fuerza de trabajo de ingeniería de Internet): Organismo encargado de proponer y establecer los estándares en Internet.

Interfases de red: Apoyan las tecnologías que son la implantación real del medio de la red. En los sistemas operativos de red más complejos, las interfases de red pueden cargarse y descargarse en forma dinámica, y se pueden instalar, simultáneamente, múltiples interfases de diferentes tipos y marcas.

Internet: La llamada "red de redes" creada de la unión de muchas redes TCP/IP a nivel internacional y cuyos antecedentes están en la ARPANet.

Internet: Conexión entre dos o más redes.

Intranet: Red de uso privado que emplea los mismos estándares y herramientas de Internet. Es uno de los segmentos del mercado de computación que más impulso está cobrando.

IMHO (In My Humble Opinion; En mi humilde opinión): Abreviación muy utilizada en los foros de discusiones de la red. Se puede traducir como "según mi humilde opinión" y se usa para hacer énfasis en que lo dicho es sólo un punto de vista muy personal.

IP (Internet Protocol; Protocolo Internet): Protocolo que provee las funciones básicas de direccionamiento en Internet y en cualquier red TCP/IP.

IPX (Internetworking Packet Exchange; Intercambio de paquetes entre redes): Protocolo de comunicaciones de NetWare de Novell utilizado para la transferencia de datos entre los nodos de una red.

IRC (Internet Relay Chat; Poner en charla en Internet): Herramienta de internet que permite a un usuario unirse a una plática en vivo con otros usuarios (en modo texto). Está siendo substituida por herramientas similares en el World Wide Web y por los nuevos sistemas multimedia que permiten el intercambio de audio y vídeo por Internet.

ISOC (Internet Society; Sociedad Internet): Organismo promotor de Internet encargado de coordinar los estándares utilizados en la red.

ISP (Internet Service Provider; Proveedor de servicios Internet): Compañía dedicada a revender el acceso a Internet. Puede proveer desde enlaces dial up hasta enlaces dedicados de muy alta velocidad. También suele ofrecer servicios adicionales como desarrollo y mantenimiento de web sites, de servidores de correo electrónico, etc.

Java: Lenguaje de programación independiente de la plataforma creado por Sun Microsystems. Está pensado expresamente para una arquitectura cliente/servidor en la que sólo es necesario intercambiar pequeñas porciones de código (llamadas Applets) que son ejecutadas por el cliente.

JPEG (Joint Photographic Experts Group; Grupo de expertos de ensamble fotográfico): Nombre del comité que diseñó el estándar de compresión de imágenes conocido precisamente como JPEG. Está pensado especialmente para

imágenes fotográficas con muchos colores y poco a poco ha ido ganando terreno sobre otros estándares.

Kbps: Kilo bits por segundo.

KBps: Kilo bytes por segundo.

Kernel: El control kernel o el núcleo de control es el corazón del sistema operativo, el cual coordina los diferentes procesos de los otros subsistemas. De una manera central, en el diseño del kernel están los procesos que optimizan el acceso a los servicios para la actividad del usuario.

LAN (Local Area Network; Red de área local): Conjunto de computadoras y otros dispositivos comunicados entre sí dentro de un área relativamente pequeña.

Línea privada o dedicada (Leased o dedicated line): Línea telefónica que conecta permanentemente dos puntos.

Lista de correo (maillist): Aplicación que envía automáticamente correo a un grupo determinado de usuarios. Es muy utilizada para mantener informado a los miembros sobre las noticias de algún área de interés para ellos. Para estar dentro de la base de datos de una lista de correos normalmente es necesario suscribirse a la misma.

Lista de correo moderada: Lista de correo en la que el moderador decide que mensajes se hacen públicos y cuáles no.

Listserv: Es el tipo más común de lista de correo en Internet. Sus orígenes están en BITNET.

Log file: Archivo que guarda información sobre los sucesos de cierto proceso. Por

ejemplo el log file de un servidor web puede almacenar información sobre quienes han entrado al servidor, que documentos usaron, que archivos transfirieron, etc.

Mailbot: Servidor de correo que responde automáticamente cuando se le solicita información.

Mainframes (Macrocomputadoras): Se refiere a un sistema computacional de grandes dimensiones.

Máquina de búsqueda (search engine): Programa que permite a los usuarios buscar información a través de Internet. En el WWW algunas de las más famosas son Lycos, Yahoo, Webcrawler, etc.

MAU (Multi-station Access Unit; Unidad de acceso de múltiples estaciones): Concentrador/repetidor de cableado con puertos múltiples para Token Ring.

Microcomputadoras: Son estaciones de trabajo por medio de las cuales se accesa la información y que ayudan al procesamiento de la misma.

MIME (Multipurpose Internet Mail Extensions; Extensiones de correo Internet multipropósito): Extensión al protocolo de coreo de Internet que permite el intercambio de archivos binarios como anexos de mensajes de correo electrónico. MIME también es usado por los servidores web para identificar el tipo de archivos que envían a los clientes (browsers).

Modem. Modulador-Demodulador: Dispositivo que convierte señales digitales a una forma adecuada para transmisión sobre medios de comunicación analógicos y viceversa.

Modulación por codificación de impulsos: Técnica para digitalizar voces tomando muestras de las ondas del sonido y convirtiendo cada muestra en un

número binario.

MOO (Mud, Object Oriented; Mud, Orientado a objeto): MUD (Multi-User Dungeon or Dimension; Encierro o dimensión multiusuario)

MUSE (Multi-User Simulated Environment; Ambiente multiusuario simulado): Ambientes que intentan ser la versión texto de una "realidad virtual". Se emplea mucho como juego en Internet en la que los participantes del habitan en cierto lugar del ciberespacio e interactuan (en tiempo real) con los demás últimamente han empezado a surgir aplicaciones más serias como la creación de campus universitarios virtuales.

Mosaic: Fue el primer cliente para servidores web.

Navegar (Navegate; Navegador): Término empleado cuando se salta entre documentos hipertexto en el World Wide Web. También se suele emplear el término surfear.

Netiquette: Reglas de etiqueta en Internet.

Netizen: Palabra derivada del vocablo inglés para ciudadano (citizen). Se utiliza para nombrar a todos aquellos miembros de Internet.

Newsgroup (Grupo de noticias): Foro de discusión de un tema en particular. Actualmente existen mas de 15 mil grupos de noticias diferentes.

Newsreader (Lector de noticias): Software empleado para leer y escribir mensajes de un grupo de noticias.

Online (En línea): Término que puede ser traducido como "conectado" o "con conexión activa". Así pues, si se hacen compras online, quiere decir que se hacen

con la conexión al centro comercial activada.

PDS (Premises Distribution System; Sistema de distribución de premisas): Estándar definido por AT&T en el que basan sus productos muchas compañías proveedoras de equipos para redes locales.

POP (Post Office Protocol; Protocolo de oficina postal): Protocolo empleado por el software cliente para extraer mensajes de los servidores de correo.

POP (Point of Presence; Punto de presencia): Sitio en el que la red de un proveedor permite interconexión con otras redes de clientes y proveedores.

Postmaster (Maestro de correo): Alias empleado por los servidores de correo para la cuenta encargada de administrar el ruteo de mensajes.

PPP (Point to Point Protocol; Protocolo punto a punto): Protocolo empleado para realizar conexiones TCP/IP a través de enlaces seriales. Su uso más común es en las cuentas dial up en las que el usuario se conecta a la red de su ISP por medio de un modem y una línea telefónica.

Protocolo de comunicación: Se refiere a la manera como los datos pasan de una estación a otra.

Protocolo por poleo: Este método de acceso su caracteriza por contar con un dispositivo controlador central, que es una computadora inteligente, como un servidor. Pasa lista a cada nodo en una secuencia predefinida solicitando a la red. Si tal solicitud se realiza, el mensaje se transmite; de lo contrario, el dispositivo central se mueve a pasar lista al siguiente nodo.

Puentes (bridges): 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).

Puentes ruteadores (brouters): Son una especie de híbrido entre los puentes y ruteadores. Frecuentemente se les denomina incorrectamente ruteadores de protocolo múltiple, los puentes ruteadores ofrecen muchas de las ventajas, tanto de los puentes como de los ruteadores para redes muy complejas. En realidad los puentes ruteadores toman la decisión de si un paquete utiliza un protocolo que pueda ser enrutable. Así, enrutan aquéllos que puede y puentean el resto.

Puerto (Port): En Internet se refiere a la parte de un URL que va inmediatamente después de un nombre de dominio y que está precedido por dos puntos (:). Se utiliza para indicar que los servicios de dicho servidor no están ejecutándose en el puerto estándar . Por ejemplo en el URL FTP://servidor.cia.com.mx:240 se indica que el servicio de FTP se ejecuta en el puerto 240.

RAM (Random Access Memory; Memoria de acceso aleatorio): Almacenamiento de información que permite al usuario mover y colocar los datos de cualquier manera posible.

RFC (Request For Comments; Petición para comentarios): Nombre dado a los documentos en los que se documenta la creación y establecimiento de estándares en Internet. Cuando se propone un nuevo estándar, la IETF publica un RFC, el cual a su vez le hereda el nombre al estándar finalmente adoptado. Por ejemplo, para correo se tiene el RFC 822.

ROM (Read Only Memory; Memoria de sólo lectura): Datos e instrucciones almacenados en la memoria que no pueden ser alterados.

Ruteadores (routers): Los ruteadores determinan 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 están limitado por protocolos de acceso o medio.

Servicios de sistemas: Los servicios de sistemas de red cubren todos los servicios que no se ajustan fácilmente a cualquiera de las otras categorías del modelo. Estos pueden ser servicios de almacenar y dirigir al nivel de sistema, tales como enfilar protocolos o subsistemas de contabilidad de recursos.

Servidor de archivos (File Server): Concepto en el que todos los usuarios pueden tener acceso a la misma información, compartir archivos y contar con niveles de seguridad.

Shareware (Programa por distribución): Software de distribución pública y gratuita pero no de uso gratuito. El autor establece un período de prueba después del cual pide una cuota de recuperación.

Shell (Redirector): Software que atrapa o captura la entrada/salida de la aplicación antes que esta entrada/salida llegue al sistema operativo local. Este software examina y envía la solicitud al servidor de archivos para su acción. Esta acción la utiliza el shell de NetWare y el MS-NET de Microsoft para soportar estaciones de trabajo bajo DOS.

Signature file (Archivo de firma): Archivo ASCII utilizado por muchos programas de correo electrónico en el que el usuario escribe un texto que será añadido automáticamente al final de cada menaje que envíe por la red.

Sistema operativo de red: Es quien rige y administra los recursos (archivos, periféricos, usuarios, etc) y lleva el control de seguridad de éstos.

Sistemas de archivo (file systems): Son los mecanismos mediante los cuales,

se organizan, almacenan y recuperan los datos, a partir de los subsistemas de almacenamiento disponibles para el sistema operativo de red.

SLIP: (Serial Line Internet Protocol: Protocolo Internet en línea serial) Protocolo antecesor de PPP que también permite el establecimiento conexiones TCP/IP a través de enlaces seriales.

SMTP (Simple Mail Transfer Protocol; Protocolo sencillo de transferencia de correo): Protocolo original para intercambio de correo en Internet. Sólo permite el intercambio de mensajes ASCII, por lo que está siendo gradualmente reemplazado por MIME.

Software (materia lógica): Conjunto de instrucciones lógicas diseñadas para el funcionamiento computacional.

STP (Shielded Twisted Pair; Cables de par torcido blindado): Clasificación de par torcidos que contienen cables de conductores más gruesos y muy bien cubiertos por un jacket.

Subsistema administrativo: Subsistema del estándar PDS que se refiere a los paneles de distribución de los cables normalmente ubicados en los closets de cableado.

Subsistema de cableado en el área de trabajo: Subsistema del estándar PDS que prácticamente es el cable que corre desde la salida de la pared a la PC.

Subsistema de cableado horizontal: Subsistema del estándar PDS que utiliza cable que corre desde la columna vertebral, hasta cada uno de los usuarios. Típicamente se utiliza cableado telefónico para este subsistema. En este caso, los cables comienzan en el closet de cableado y llegan hasta la salida de la pared a donde se va a conectar la PC

Subsistema de campo (campus): Subsistema del estándar PDS que se utiliza típicamente fibra óptica, o cable coaxial, para interconectar los diferentes edificios en donde se vayan a ubicar las redes de área local.

Subsistema de columna vertebral (backbone): Subsistema del estándar PDS que utiliza cable para la interconexión entre los diferentes pasos del edificio; típicamente también es de fibra óptica o coaxial.

Subsistema del cableado del equipo: Subsistema del estándar PDS que se refiere a los cables que intercomunican los equipos de cómputo. Es común encontrar este subsistema cuando se usan varios computadores como equipos centrales, y éstos, a su vez, están interconectados entre sí. El cable que se utiliza para interconectarlos cae dentro de este subsistema.

Sysop (System Operator; Operador del sistema): Es el responsable de la operación cotidiana de una computadora o un dispositivo de la red.

T1: Conexión dedicada de alta velocidad (1.54 Mbps).

T3: Conexión dedicada de alta velocidad (44 Mbps)

Tarjetas de interfase: Permiten empaquetar la información y transmitirla a cierta velocidad y de acuerdo con características determinadas de envío. Estas varían según la topología y el protocolo de red que pueden ser entre otras, Token Ring, Ethernet y Arcnet. Estas son las más comunes en el mercado de redes locales.

TCP/IP (Transmission Control Protocol/Internet Protocol; Protocolo de control de comunicaciones/Protocolo Internet): Conjunto de protocolos de comunicaciones desarrollado por la DARPA (Defense Advanced Research Projects Agency, Agencia de proyectos avanzados de investigación de defensa) a

finales de la década de los 1970. TCP corresponde a la capa de transporte del modelo OSI (Modelo de referencia OSI) y ofrece la transmisión de datos, e IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal función es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambientes Unix por Vinton G. Cerf y Robert E. Kahn

Telnet: Protocolo y aplicaciones que permiten una conexión como terminal remota a una computadora remota.

Terminal Server: Servidor especializado de comunicaciones que permite el establecimiento de sesiones remotas a una red.

Throughput (Transferencia Real): Cantidad de datos que son transmitidos a algún punto de la red.

Token Passing (Paso de ficha): Este protocolo, que se utiliza en redes Arcnet y Token Ring, 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 velocidades de transferencia de 4 y 16 Mbps.

Topologías de anillo: Topología en donde las estaciones de trabajo se conectan físicamente en un anillo, terminando el cable en la misma estación de donde se originó.

Topología de bus: También llamadas lineales, todas las estaciones se conectan a un cable central llamado "bus". Este tipo de topología es fácil de instalar y requiere menos cable que la topología de estrella.

Topología de estrella: Topología de red en donde cada estación se conecta con su propio cable a un dispositivo de conexión central, bien sea un servidor de archivo o un concentrador o repetidor.

Topología de red: Se refiere a cómo se establece y se cablea la red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Tres de las topologías básicas de red son la estrella, el bus y el anillo.

Under construction (Construcción subalterna): Término utilizado para indicar que un sitio web o una página web están en desarrollo y, por lo tanto, no son totalmente funcionales

URL: (Universal Resource Locator; Localizador universal de recursos): Un URL indica la localización exacta de cualquier documento o servidor en el WWW.

USENET: Otro nombre que se le da a los grupos de noticias.

UTP (Unshielded twisted pair; Par torcido sin blindar): Clasificación de cables de par torcido que contienen cables con conductores de cable delgado y menos protegidos por un jacket.

UUENCODE (Unix to Unix Encoding; Codificador Unix a Unix): Al igual que Binhex, es un método para transmitir archivos binarios en mensajes de correo electrónico ASCII.

Veronica (Very Easy Rodent Oriented Net-wide Index to Computerized Archive):; Acceso fácil a través del ratón a índices de archivos computarizados en toda la red): Herramienta desarrollada en la Universidad de Nevada para búsqueda de información en servidores Gopher. Puede verse como un precursor

del Web y prácticamente ha sido sustituido por el web.

WAIS (Wide Area Information Servers; Servidores de información de área amplia): Sistema comercial de obtención de información patrocinado por Apple, Thinking Machines and Dow Jones, Inc.

WAN (Wide Area Network; Red de área amplia): Conjunto de computadoras y otros dispositivos comunicados entre sí colocados dentro de un espacio geográfico de amplias dimensiones.

Web page (Página de red): Cualquier página en un sitio web.

Web site (Sitio de red): Conjunto de páginas web que forman una unidad única. Incluso se puede tener un sitio web de una sola página, y es entonces cuando página web y sitio web se usan indistintamente.

World Wide Web (Red mundial amplia, conocido también como: WWW, W3 ó el web): Sistema de arquitectura cliente/servidor para distribución y obtención de información en Internet basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Alta Energía del CERN (Génova) en 1991 y ha sido una de las piezas fundamentales para la comercialización y masificación de Internet.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

- ATM como solución a los requerimientos multimedia
  Luis Carlos Díaz
  Alejandra Quintero
  Universidad de los Andes, Santafé de Bogotá – Colombia
  http://hidra.uniandes.edu.co/articulos/atm/atm.html

- Sistema de Cableado Estructurado
  Mario Linares
  AT&T GIS Colombia
  http://ainsuca.uniandes.edu.co/articulos/cableado.html

- Instalando un Servidor WWW
  Daniel M. Germán
  Alejandro López Ortiz
  Universidad de Waterloo, Canadá
  http://www.fciencias.unam.mx/revista/soluciones/30s/No33/web.html

- Firmas Digitales
  Ivan Puig de la Pena
  Revista TiMagazine
  http://www.rotativo.com/timagazine/1a2b3c/0497/firmas.cfm

- Productos – Inventario de Hardware y Software
  Panda Software
  http://www.pandasoft.es/esp/doc/p4_3.htm

- Systems Management Server 1.2
  Microsoft Corporation
  http://www.microsoft.com/smsmgmt/product12.htm

- Requerimientos para la gestión de LAN´s
  Toni Arauzo Almirón
  Revista TiMagazine
  http://www.rotativo.com/timagazine/1a2b3c/0797/lans.cfm

- Protocolos para el desarrollo de Aplicaciones en Redes Locales
  Jesús Gutiérrez
  Revista Red, Marzo 1997
  http://www.red.com.mx/mar97/interconmar97.html

- ¿Cómo seleccionar personal de Redes, sin arrepentirse?
  Rafael Fernández
  Revista Red

- Controlando la Seguridad en Redes I y II
  Ricardo Cuppolo G.
  Revista Pc News, Junio 1996
  http://www.pc-news.com.ve/960625ayuda.htm

- Administradores de Red: Perfil técnico en las oportunidades de negocio
  Andrés Piedragil
  Revista Red, Octubre 1997
  http://www.red.com.mx/act97/espeoct97.html

- Capacitación: Alcances, Problemas y Oportunidades
  Jorge Arturo Piñón
  Revista Red

- ¿Está bien Capacitado?
  Personal Computing, Mayo 1997
  http://www.percom.com.mx/anteriores/mayo97/ted1.html

- El Modelo de Referencia OSI
  Manuel Capell y Batey
  Revista TiMagazine, Octubre 1997
  http://www.rotativo.com/timagazine/1a2b3c/1097/osi.cfm

- Tendencias en Cableado
  Patricia Cortes
  Revista Red, Ocubre 1996
  http://www.red.com.mx/octubre96/sooct96.html

- Introducción a ATM
  Sonia López Esquilas
  Revista TiMagazine, Noviembre 1997
  http://www.rotativo.com/timagazine/1a2b3c/1197/introatm.cfm

- ATM
  Raúl Santuyo
  Revista Soluciones Avanzadas
  http://www.fciencias.unam.mx/revista/soluciones/30s/No31/telec-31html

- Seguridad de la Información
  Ivan Puig de la Pena
  Revista TiMagazine
  http://www.rotativo.com/timagazine/1a2b3c/seguridad/seg-info.cfm

- Seguridad en Unix
  Diego Martín Zamboni
  Seguridad en Cómputo, DGSCA-UNAM
  http://www.fciencias.unam.mx/revista/soluciones/30s/No35/seg-unix.html

- Introducción a la Criptografía
  Ma. Esther Robles Blázquez
  Estudiante de 5º Ing. Informática
  Universidad de Valladolid
  Revista TiMagazine
  http://www.rotativo.com/timagazine/1a2b3b/seguridad/intro.cfm

- Firewall
  Ma. Esther Robles Blázquez
  Estudiante de 5º Ing. Informática
  Universidad de Valladolid
  Revista TiMagazine, Mayo 1997
  http://www.rotativo.com/timagazine/1a2b3b/0597/firewall.cfm

- Seguridad en los servicios de Internet
  Diego Martín Zamboni
  Seguridad en Cómputo, DGSCA-UNAM
  http://www fciencias.unam.mx/revista/soluciones/30s/No33/seg-red.html