UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

TELEFONIA DIGITAL Y RDSI

"FUNCIONAMIENTO DE UNA RED DE AREA LOCAL"

TRABAJO DE SEMINARIO
QUE PARA OBTENER EL TITULO DE :
INGENIERA MECANICO ELECTRICISTA
P R E S E N T A :
CLAUDIA IVETTE CAMPOS GARCIA

ASESOR: ING. VICTOR HUGO ARROYO HERNANDEZ

CUAUTITLAN IZCALLI, EDO DE MEX. 2005

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

UNIDAD DE LA ADMINISTRACION ESCOLAR

DEPARTAMENTO DE EXAMENES PROFESIONALES

VERSIDAD NACIONAL
AVTÓNOMA DE
MEXICO

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES CUAUTITLAN

DEPARTAMENTO DE
EXÁMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Telefonía Digital y RDSI

"Funcionamiento de una Red de Area Local"

que presenta la pasante: Claudia Ivette Campos García

con número de cuenta: 9652118-8 para obtener el título de :

Ingeniera Mecánica Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 16 de Mayo de 2003

MODULO	PROFESOR	FIRMA
I	Ing. J. Luis Rivera López	
III	Ing. Víctor Hugo Arroyo Hernández	
IV	Ing. Vicente Maraña González	

ERNESTO:

Por tu gran valor, responsabilidad y carácter
Por no dejarte vencer cuando pareciera que todo es más difícil
Y por mostrarme que ante la adversidad, siempre has seguido adelante

GRACIAS

ESTELA:

Por tu amor constante
Por tu gran fuerza interior
Por tu entrega a la familia
Por enseñarme que la perseverancia,
es esencial para superar cualquier obstáculo en la vida

GRACIAS

A LOS DOS, MIS PADRES:

Por creer en mi
Por no dejarme sola en ningún momento
Por su apoyo incondicional
Y porque gracias a sus valores inculcados
Hoy alcanzo uno de mis mas grandes anhelos

TODO MI CARIÑO Y RECONOCIMIENTO

ANGEL Y KARINA:

A los dos, mis hermanos; por su alegría y entusiasmo
Por compartir este momento tan especial conmigo

GRACIAS

A MIS FAMILIARES Y AMIGOS:

A todos aquellos que me han apoyado de alguna manera
Sin mencionar un sólo nombre, pero sin olvidar a nadie
A los que están aquí y a los que se han ido ya

SINCERAMENTE
GRACIAS

INTRODUCCION

OBJETIVOS

Pág.

CAPITULO I INTRODUCCION A LAS REDES DE COMPUTADORAS

1.1 Definición de red o networking 1

1.2 Clasificación de las redes según su extensión 1

1.2.1 LAN (Local Area Network) 1
1.2.2 MAN (Metropolitan Area Network) 2
1.2.3 WAN (Wide Area Network) 2

1.3 Clasificación de las redes según su tecnología de transmisión 3

1.3.1 Redes de difusión o broadcast 3
1.3.2 Redes punto a punto 4

1.4 Clasificación de las redes según su transferencia de datos 4

CAPITULO II MODELO OSI

2.1 El modelo de referencia OSI 5

2.2 ¿ Por qué un modelo de red dividido en capas ? 5

2.3 Las siete capas del modelo de referencia OSI 7

2.3.1 Capa 1 – Capa física 7
2.3.2 Capa 2 – Capa de enlace 8
2.3.3 Capa 3 – Capa de red 8
2.3.4 Capa 4 – Capa de transporte 8
2.3.5 Capa 5 – Capa de sesión 8
2.3.6 Capa 6 – Capa de presentación 9
2.3.7 Capa 7 – Capa de aplicación 9

Pág.

2.4 Proceso de comunicación 9

2.5 Encapsulación de datos 11

CAPITULO III CAPAS DEL MODELO OSI

3.1 Capa física 14

3.1.1 Técnicas de transmisión 14

3.1.1.1 Banda base 14

3.1.1.2 Banda ancha 14

3.1.2 Medios de networking 15

3.1.2.1 Cable coaxial 15

3.1.2.2 Cable de par trenzado no blindado 16

3.1.2.3 Cable de par trenzado blindado 17

3.1.2.4 Cable de fibra óptica 18

3.1.3 Selección del medio de networking adecuado 21

3.2 Capa de enlace de datos 22

3.2.1 Tarjeta de interfaz de red (NIC) 23

3.3 Capa de red 25

3.4 Capa de transporte 29

3.4.1 Control de flujo 30

3.4.2 Establecimiento de una conexión con un sistema de iguales 30

3.4.3 Operaciones en ventana 33

3.4.4 Acuse de recibo 34

3.5 Capa de sesión 37

3.6 Capa de presentación 36

Pág.

3.7 Capa de aplicación 37

CAPITULO IV TOPOLOGIAS, DISPOSITIVOS Y TECNOLOGIAS DE RED

4.1 Topologías 40

4.1.1 Topología de bus 40
4.1.2 Topología en estrella 42
4.1.3 Topología en estrella extendida 43
4.1.4 Topología en anillo 44

4.2 Dispositivos de red 45

4.2.1 Repetidor 46
4.2.2 Hub 47
4.2.3 Switch 48
4.2.4 Puente 49
4.2.5 Router 52
4.2.6 Gateway 54

4.3 Tecnologías de red 55

4.3.1 Estándares de LAN Ethernet /802.3 56

4.3.1.1 Funcionamiento de Ethernet /802.3 58
4.3.1.2 Broadcast Ethernet/802.3 58
4.3.1.3 Medios de acceso 59

4.3.2 Fast Ethernet 61

4.3.3 Gigabit Ethernet 62

CAPITULO V SISTEMA DE CABLEADO ESTRUCTURADO

5.1 Sistema de cableado estructurado 63

Pág.

5.2 Elementos de un sistema de cableado estructurado 64

5.2.1 Area de trabajo 64
5.2.2 Cableado horizontal 64
5.2.3 Cuarto de telecomunicaciones 64
5.2.4 Cableado de backbone 65
5.2.5 Cuarto de equipos 65
5.2.6 Entrada de facilidades 66
5.2.7 Administración 66

5.3 Estándares de medios de networking 66

5.3.1 Estándar EIA/TIA-568B 67
5.3.2 Estándar EIA/TIA-569A 67
5.3.3 Estándar EIA/TIA-606A 68
5.3.4 Estándar EIA/TIA-607 69

CONCLUSIONES 70

REFERENCIAS BIBLIOGRAFICAS 71

En un principio las computadoras eran elementos aislados que constituían una estación de trabajo independiente; cada una precisaba sus propios periféricos y contenía sus propios archivos, de tal forma que cuando un usuario necesitaba imprimir un documento y su equipo no disponía de una impresora, debía desplazarse a otro equipo con impresora e imprimirlo desde allí, o bien instalar otra impresora en su equipo, lo que hacía una duplicación de dispositivos y recursos.

Era imposible implementar una administración conjunta de todos los ordenadores, por lo que la configuración y gestión de cada uno de los equipos independientes y de los periféricos, era una tarea ardua para el responsable de esta labor.

Esta forma de trabajo, no fue un sistema económico, ni eficiente para las empresas e instituciones. Fue entonces cuando se hizo necesaria la implementación de sistemas que permitieran la comunicación entre diferentes ordenadores y la correcta transferencia de datos entre ellos, surgiendo de esta forma el concepto de redes de computadoras o networking.

A mediados de los años 70, diversos fabricantes desarrollaron sus propios sistemas de redes locales. En 1980 la empresa Xerox, en cooperación con Digital Equipment Corporation e Intel, desarrolló las especificaciones del primer sistema de red, denominado Ethernet.

El principal inconveniente de estos sistemas de comunicación en red fue que cada uno de ellos era propietario de una empresa particular por lo que habían sido desarrollados con hardware y software propios, elementos protegidos y cerrados y que utilizaban protocolos y arquitecturas diferentes; como consecuencia de ello, la comunicación entre ordenadores pertenecientes a distintas redes era imposible.

Con ello, nació la necesidad de salir de los sistemas de networking propietarios, optando por una arquitectura de red con un modelo común que hiciera posible interconectar varias redes sin problemas.

Para solucionar este problema, la Organización Internacional de Estándares (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad); por lo tanto, en 1984 fue creado el Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI).

En la actualidad, una adecuada interconexión entre usuarios y procesos dentro de una empresa u organización puede constituir una clara ventaja competitiva. La reducción de costos de periféricos, la facilidad para compartir y transmitir información son los puntos clave en que se apoya la creciente utilización de las redes.

Los objetivos generales son:

- Definir el concepto de red o networking, así como su importancia en la actualidad;
- Describir la función principal de cada nivel de modelo de referencia OSI, así como el proceso de encapsulación y comunicación entre capas;
- Identificar los principales medios de networking en la capa física;
- Definir y describir el propósito de una dirección MAC y de una NIC en la capa de enlace; el direccionamiento IP en la capa de red.
- Describir la función principal de la capa de transporte, capa de sesión, capa de presentación y capa de aplicación.
- Identificar y definir los dispositivos de networking y las topologías.
- Definir la Tecnología de LAN Ethernet y sus estándares que la definen.
- Describir los elementos que forman un sistema de Cableado Estructurado

CAPITULO I

INTRODUCCION A LAS REDES DE COMPUTADORAS

1.1 DEFINICION DE RED O NETWORKING

Una *red* o *networking* es un sistema de interconexión entre estaciones de trabajo que además de permitir la transmisión de información, permite también compartir recursos tales como dispositivos periféricos, unidades de disco duro, CD-ROM, DVD, impresoras, escáneres, y otros dispositivos.

En una red es posible que distintos tipos de equipos se comuniquen entre sí; aun si éstos son un sistema macintosh, una PC o un mainframe. Lo que en verdad importa es que todos los dispositivos utilicen el mismo lenguaje o protocolo, que es una descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información. En informática el protocolo es un lenguaje común que todos los dispositivos de una red pueden entender.

1.2 CLASIFICACION DE LAS REDES SEGUN SU EXTENSION

Las redes se clasifican según su extensión en Redes de Area Local/Local Area Network (LAN), Redes de Area Metropolitana/Metropolitan Area Network (MAN) y Redes de Area Amplia/Wide Area Network (WAN).

1.2.1 LAN (Red de Area Local /Local Area Network)

Las LAN, son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Las LAN interconectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos entre sí; permiten que las empresas que utilizan tecnología informática compartan elementos tales como archivos e impresoras de manera eficiente. Como resultado, una empresa puede utilizar una LAN para unificar sus datos, sistemas de comunicaciones, equipos y servidores de archivos.

Las LAN están diseñadas para:

- Operar dentro de un área geográfica limitada.
- Permitir que varios usuarios accedan a medios de ancho de banda elevado.
- Proporcionar conectividad continua con los servicios locales.
- Conectar dispositivos adyacentes.

Las LAN tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de microsegundo) y experimentan muy pocos errores. Las LAN más nuevas operan a velocidades muy altas de hasta 1 Gbps.

1.2.2 MAN (Red de Area Metropolitana /Metopolitan Area Network)

Una MAN es básicamente una versión más grande de una LAN y se basa en una tecnología similar. La distancia que cubren está en el orden de las decenas de kilómetros, podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o publica. Una MAN puede manejar datos y voz e incluso podría estar relacionado con la red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salidas potenciales. Al no tener que conmutar se simplifica el diseño.

Las MAN tienen un mecanismo de arbitraje propio llamado DQDB (Distributed Queue Dual Bus /Bus Doble de Colas Distribuidas). El DQDB consiste en dos buses unidireccionales a los cuáles están conectadas todas la computadoras. Cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior. El tráfico hacia la izquierda usa el de abajo.

1.2.3 WAN (Red de Area Amplia/Wide Area Network)

A medida que incrementó la utilización de equipos en las empresas, se hizo obvio que las LAN no eran lo suficientemente eficientes; ya que en una LAN, cada departamento o empresa era independiente.

Por lo que, cada vez fue mayor la necesidad de encontrar la manera de trasladar información de modo más eficiente y veloz entre LAN's.

La solución fue la creación de las WAN. Estas interconectan a las LAN para brindar acceso a equipos o servidores de archivos que se encuentran en otros lugares.; debido a que las WAN conectan redes dentro de un área geográfica extensa, las empresas pudieron comunicarse entre sí aunque se encontraran separadas por grandes distancias.

Al realizar networking o conectar equipos, impresoras y otros dispositivos en una WAN éstos podían comunicarse entre sí y compartir información y recursos, así como también podían tener acceso a Internet.

Las WAN contienen una colección de máquinas dedicadas a ejecutar programas de usuario llamadas hosts. Los host están conectados por una subred de comunicación, el trabajo de esta subred es conducir los mensajes de un host a otro.

En muchas WAN, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión también llamadas circuitos, canales o troncales, transmiten los bits de una máquina a otra. Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea o entrada, el conmutador debe escoger una línea de salida para reenviarlos.

A estos conmutadores también se les denomina nodos conmutadores de paquetes, sistemas intermedios, centrales de conmutación de datos o enrutadores.

1.3 CLASIFICACION DE LAS REDES SEGUN SU TECNOLOGIA DE TRANSMISION

1.3.1 Redes de difusión o broadcast

Las redes de difusión tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos llamados también paquetes que envía una máquina son recibidos por las demás. Un campo de dirección dentro del paquete especifica a quien se dirige. Al recibir un

paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si esta dirigido a alguna otra máquina, lo ignora

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama difusión (broadcasting). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas llamado multidifusión. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes n-1 bits de dirección pueden contener un número de grupo. Cada máquina se puede suscribir a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las máquinas que se suscribieron a ese grupo.

1.3.2 Redes punto a punto

Consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante en este tipo de redes. Las redes pequeñas geográficamente localizadas tienden a usar difusión, mientras que las redes más grandes suelen ser punto a punto.

1.4 CLASIFICACION DE LAS REDES SEGUN EL TIPO DE TRANSFERENCIA DE DATOS

- *Redes Simplex*, la transmisión de datos sólo viaja en un sentido.
- *Redes Half-Duplex*, la transmisión de datos pueden viajar en ambos sentidos pero sólo en uno de ellos en un momento dado; es decir, solo puede haber transferencia en un sentido a la vez.
- *Redes Full-Duplex*, la transmisión de datos viaja en ambos sentidos a la vez.

CAPITULO II

MODELO DE REFERENCIA OSI

2.1 MODELO DE REFERENCIA OSI

El modelo de referencia OSI es un esquema de red descriptivo. Sus estándares aseguran una mayor compatibilidad e interoperabilidad entre distintos tipos de tecnología de red; además de describir la forma en que la información viaja a través de las redes. Es una estructura conceptual que especifica las funciones de red que se producen en cada nivel. Su aplicación a las redes no implica solución tecnológica alguna; sino que aporta procedimientos para el intercambio de información normalizada.

Describe la forma en que la información se traslada desde programas de aplicación (por ejemplo: hojas de cálculo) a través de un medio de red (por ejemplo: cables) hasta otro equipo de una red. A medida que la información que se debe enviar desciende a través de los niveles de un determinado sistema, el lenguaje utilizado se parece cada vez menos al lenguaje humano y cada vez más a los códigos de unos y ceros que son comprensibles para los equipos informáticos.

2.2 ¿ POR QUE UN MODELO DE RED DIVIDIDO EN CAPAS ?

El modelo de referencia OSI divide el complejo traslado de información entre equipos a través de un medio de red en siete problemas más simples. Estos fueron elegidos debido a que son razonablemente independientes y por lo tanto, más sencillos de resolver de modo que no tengan que ocuparse del detalle de la implementación real de los servicios.

A la división de estos siete problemas simples en funciones de red se le denomina *división en capas*. Tal como se indica en la figura 2-1, cada nivel o capa del modelo de referencia OSI resuelve cada una de las siete áreas problemáticas.

Capa 7	Aplicación	Procesos de red hacia las aplicaciones
Capa 6	Presentación	Representación de datos
Capa 5	Sesión	Comunicación entre hosts
Capa 4	Transporte	Conexiones de extremo a extremo
Capa 3	Red	Direcciones y mejor ruta
Capa 2	Enlace de Datos	Acceso a los medios
Capa 1	Física	Transmisión binaria

Figura 2-1 Capas del modelo de referencia OSI

Debido a que las capas inferiores (de la 1 a la 3) del modelo de referencia OSI controlan la transmisión física de mensajes a través de la red, a menudo se les denomina *capas de medios.* Por otro lado, las capas superiores (de la 4 a la 7) del modelo de referencia OSI, se encargan de la transmisión precisa de datos entre equipos de la red, por lo cual se denominan *capas host* (figura 2-2).

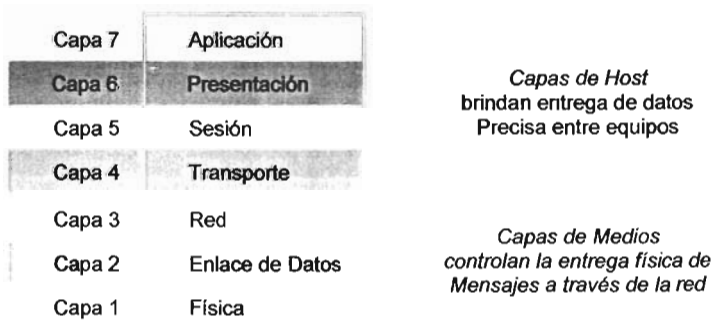


Figura 2-2 Capas host y capas de medios del modelo de referencia OSI

La mayoría de los dispositivos de red implementan las siete capas. Sin embargo, para organizar las operaciones, algunas implementaciones de red incorporan funciones de varias capas a la vez.

Al dividir el modelo de referencia OSI en estas siete capas, se obtienen las siguientes ventajas:

- Se dividen los aspectos interrelacionados del funcionamiento de la red en elementos menos complejos.
- Se definen las interfases estándar para la compatibilidad plug and play y la integración de varios fabricantes.
- Permite que los ingenieros especialicen el diseño y promuevan la simetría en las distintas funciones modulares de interconexión de redes, de modo que interoperen entre sí.
- Impide que los cambios que se producen en un área afecten a las demás para que cada área pueda evolucionar más rápidamente.
- Divide la complejidad de la interconexión en subconjuntos de operación separados, de aprendizaje más sencillo.

2.3 LAS SIETE CAPAS DEL MODELO DE REFERENCIA OSI

Cada capa posee un conjunto predeterminado de funciones que debe ejecutar para que se produzca la comunicación. Las funciones se describen en las siguientes secciones:

2.3.1 Capa 1 - Capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de tensión, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física.

2.3.2 Capa 2 - Capa de enlace de datos

La capa de enlace de datos ofrece un tránsito confiable de datos a través de un enlace físico. Para hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (que es diferente al de red, o lógico), la topología de la red, la disciplina de línea (la forma en que los sistemas finales utilizan el enlace de red), la notificación de errores, la entrega ordenada de tramas y el control de flujo.

2.3.3 Capa 3 - Capa de red

La capa de red proporciona conectividad y selección de ruta entre dos sistemas finales que pueden estar ubicados en redes geográficamente distintas. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas.

2.3.4 Capa 4 - Capa de transporte

La capa de transporte segmenta y reensambla los datos en un flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicación, las cuatro capas inferiores se encargan del transporte de datos.

Suministra un servicio de transporte de datos que proteja las capas superiores de los detalles de implementación de transporte. Específicamente, ésta capa se ocupa de temas tales como la confiabilidad del transporte a través de las redes. Al suministrar un servicio confiable, la capa de transporte proporciona mecanismos para el establecimiento, mantenimiento y finalización ordenada de los circuitos virtuales, la detección y recuperación de errores de transporte y el control del flujo de información (para evitar que un sistema desborde a otro con datos)

2.3.5 Capa 5 - Capa de sesión

La capa de sesión establece, administra y pone fin a las sesiones entre aplicaciones, las sesiones son diálogos entre dos o más entidades de presentación. La capa de sesión brinda sus servicios a la capa de presentación, sincroniza el dialogo entre las entidades de la capa de presentación y administra el intercambio de datos. También se encarga de la regulación básica de las

conversiones (sesiones), la capa de sesión proporciona los recursos para la sincronización de unidades de dialogo, clase de servicio e informes de excepciones relacionados con problemas de la capa de sesión, de presentación y de aplicación.

2.3.6 Capa 6 - Capa de presentación

La capa de presentación asegura que la capa de aplicación de un sistema pueda leer la información enviada por la capa de aplicación de otro sistema. De ser necesario, la capa de presentación realiza una traducción entre varios formatos de representación de datos utilizando un formato de representación de datos más común.

2.3.7 Capa 7 - Capa de aplicación

La capa de aplicación es la más cercana al usuario; esta capa brinda servicios de red a las aplicaciones del usuario y es distinta de las demás en el sentido de que no brinda servicios a ninguna otra capa, sino a procesos de aplicación que se ejecutan fuera del alcance del modelo de referencia OSI. Algunos ejemplos de dichos procesos de aplicación son los programas de hojas de cálculo, los procesadores de texto y los de las terminales bancarias.

Identifica y establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece los procedimientos para la recuperación de errores y el control de la integridad de los datos. También determina si existen suficientes recursos para lo comunicación planificada.

2.4 PROCESO DE COMUNICACION

Cada capa del modelo de referencia OSI tiene funciones bien definidas, realiza tareas únicas y específicas. Cada capa se sirve de los servicios de la capa inferior y ésta a su vez presta sus servicios a la capa superior. Todas las peticiones pasan de un nivel al siguiente a través de la interfaz. La interfaz es el conjunto de elementos lógicos o físicos que comunican ambos niveles.

Cada capa del modelo de referencia OSI proporciona servicios al nivel superior siguiente y protege al nivel superior de los detalles de cómo se implementan en realidad los servicios. Las capas se configuran de tal forma que cada nivel actúa como si se estuviera comunicando con su nivel asociado del otro equipo.

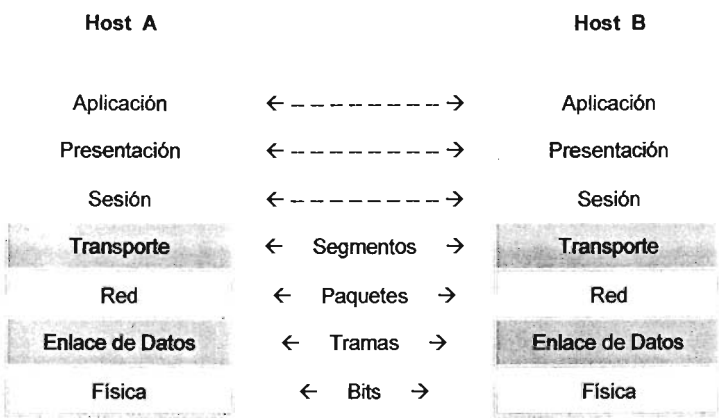


Figura 2-3 División en capas del mdelo de referencia OSI

Tal como se muestra en la figura 2-3, cada capa se comunica con su capa semejante del otro sistema por medio de un protocolo. Se denomina protocolo a un conjunto de reglas y convenciones que se siguen para intercambiar información de un equipo a otro. La información que se intercambia entre capas iguales se realiza mediante un formato específico del protocolo que recibe el nombre de Unidades de Datos del Protocolo/Protocol Data Units (PDU).

Una determinada capa puede utilizar un nombre más específico para su PDU. Por ejemplo las unidades de datos que se intercambian en el nivel de enlace, de red y de transporte suelen recibir los nombres de tramas, paquetes o datagramas y segmentos respectivamente.

2.5 ENCAPSULACION DE DATOS

Para comprender la estructura de las redes y su funcionamiento, se debe tener en cuenta que todas las comunicaciones en una red se originan en una fuente y se envían a un destino, como se muestra en la figura 2-4, la información que se envía a través de una red se denomina datos o paquete de datos.

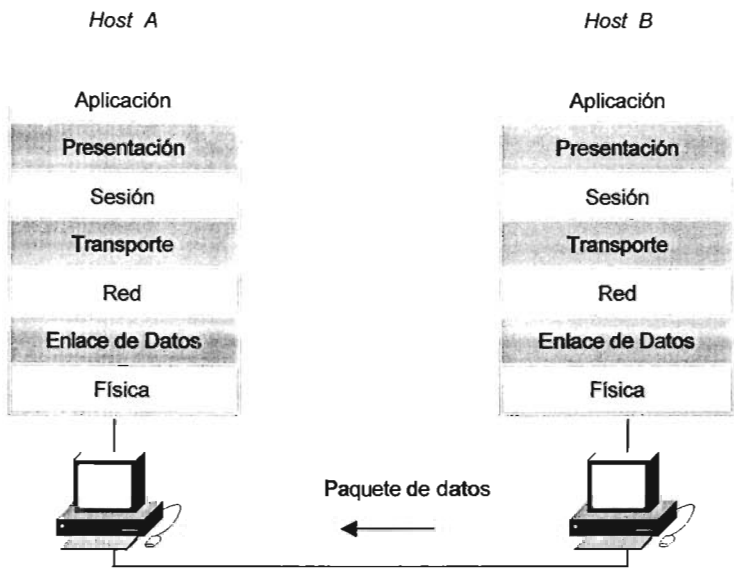


Figura 2-4 Capas del modelo de referencia OSI (origen y destino)

Para que un equipo (fuente) pueda enviar datos a otro equipo (destino), primero debe colocar los datos en paquetes mediante un proceso denominado *encapsulación*, que envuelve los datos en un encabezado de protocolo particular antes del tránsito en la red. Este proceso se puede comparar al proceso de preparación de un paquete para su envío: envolverlo, colocarlo en una caja, escribir las direcciones de origen y de destino, pegar las estampillas y colocar el paquete en un buzón.

Cada capa depende de la función de servicio de la capa inferior. Para brindar este servicio, la capa inferior utiliza la encapsulación para colocar la PDU de la capa superior en su campo de datos,

luego le puede agregar cualquier encabezado e información final que utiliza la capa para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo de referencia OSI, se agregan los encabezados y la información final.

En la figura 2.5 se puede ver cómo se forman las PDU de acuerdo con el protocolo de cada capa y cómo estas unidades de datos permiten intercambiar la información entre los extremos de la comunicación; supongamos que el host A envía una unidad de datos, mensaje o información, al host B. Los datos se entregan primero a la capa de aplicación, en donde se les añade información de control necesaria para posteriormente enviarlos a la capa de presentación, donde de igual forma, se les añade información de control, para así enviarlos a la siguiente capa, que en este caso es la de sesión y así sucesivamente.

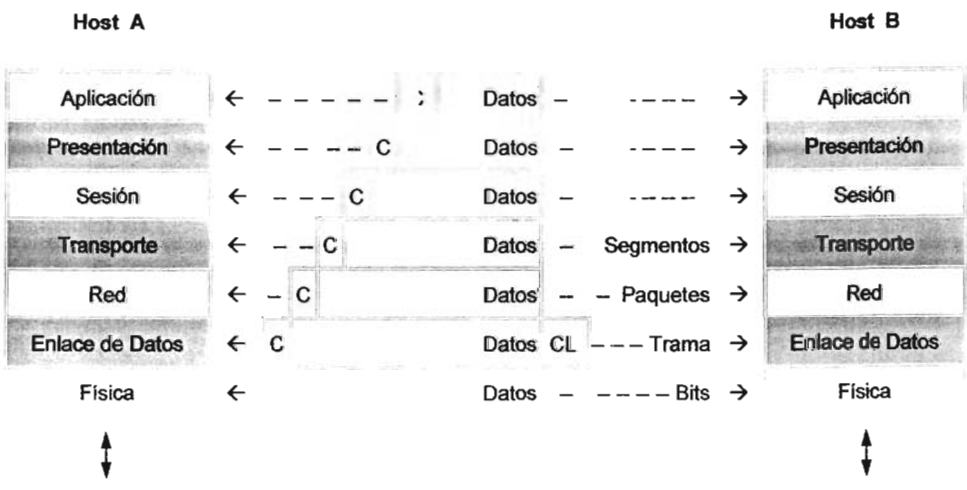


Figura 2-5 Capas del modelo de referencia OSI (origen y destino)

De esta forma, se va pasando información hacia las capas inferiores, hasta llegar a la capa física, que envía la información a través del medio físico de comunicación al que esté conectado (par trenzado, cable coaxial, fibra óptica etc.).

Cuando la información llega al otro extremo, la capa física recibe la información, la decodifica y la pasa a la capa superior, a la capa de enlace, y la traslada a la capa de red, y así sucesivamente, hasta que la información llega a la capa de aplicación tal y como fue enviada por la capa de aplicación del extremo origen.

Como se puede apreciar, no existe comunicación real entre los extremos salvo en la capa física. Sin embargo, se establece una conexión lógica entre los extremos que se encuentran al mismo nivel, de manera que dos unidades funcionales de la capa de transporte, por ejemplo, deben entenderse entre ellas cumpliendo un determinado protocolo de esa capa.

Las siete capas del modelo de referencia OSI utilizan información de control para comunicarse entre ellas. Esta información de control, como números de secuencia, es la que sirve para ordenar el dialogo en esa capa, realizar peticiones, mandar instrucciones o enviar información entre los dos extremos. La información de control se envía en forma de encabezado y/o de cola. El encabezado es información que se añade al principio de la información que reciben en la capa superior. La cola es información que se añade al final de la información recibida.

CAPITULO III

CAPAS DEL MODELO DEL OSI

3.1 CAPA FISICA

Esta capa define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Su función es la transmisión de datos; éstos pueden ser información como texto, figuras y sonidos, que son representados por la presencia de pulsos eléctricos y se denominan tensión en cables conductores de cobre o pulsos de luz en fibras ópticas. Este proceso de transmisión, denominado codificación, generalmente se logra a través del uso de elementos tales como cables y conectores, denominados medios de networking.

3.1.1 Técnicas de transmisión

Para efectuar la transmisión de la información se utilizan técnicas de transmisión; las más comunes son banda base y banda ancha.

3.1.1.1 Banda base

Transmite las señales en forma digital sin emplear técnicas de modulación, en cada transmisión se utiliza todo el ancho de banda y, por tanto, sólo puede transmitir una señal simultáneamente.

Está especialmente diseñada para la transmisión en cortas distancias, ya que en grandes distancias se producirían ruidos e interferencias, mismas que podrías corregirse mediante la utilización de repetidores que vuelven a regenerar la señal. Los elementos de conexión que se puede utilizar son: el cable de par trenzado y el cable coaxial de banda base

3.1.1.2 Banda ancha

Consiste en transmitir las señales en forma digital modulando la señal sobre ondas portadoras que pueden compartir el ancho de banda del medio de transmisión mediante multiplexación por división de frecuencia. Es decir, actúa como si en lugar de un único medio se estuvieran utilizando líneas distintas.

El ancho de banda depende de la velocidad de transmisión de los datos. Este método hace imprescindible la utilización de un módem para poder modular y demodular la información.

La distancia máxima puede llegar hasta los 50 km y permite usar además los elementos de conexión de la red para transmitir otras señales distintas de las propias de la red como pueden ser señales de televisión o señales de voz.

Los elementos de conexión que se pueden usar son: cable coaxial de banda ancha y cable de fibra óptica.

3.1.2 Medios de networking

Se entiende por medio de transmisión o networking a cualquier medio físico que pueda transportar información en forma de señales electromagnéticas. Los medios de transmisión permiten enviar la información de una estación de trabajo al servidor o a otra estación de trabajo y son una parte esencial de una red de área local.

Para que los equipos informáticos transmitan la información codificada, los medios de networking deben conectar físicamente a los equipos entre sí; esto puede ser mediante cable coaxial, cable de par trenzado y/o cable de fibra óptica.

3.1.2.1 Cable coaxial

Consiste en un alambre de cobre rígido como núcleo, rodeado por un material aislante. En la figura 3-1 se muestra como el aislante esta forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado, que actúa como blindaje del conductor interno. El conductor externo se cubre con una envoltura protectora de plástico. La construcción y el blindaje del cable coaxial le confieren una buena combinación de elevado ancho de banda y excelente inmunidad al ruido.

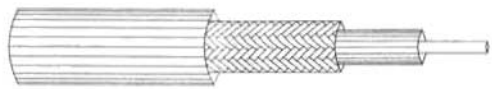


Figura 3-1 Cable coaxial

Para las LAN, el cable ofrece varias ventajas. El cable coaxial puede tenderse a mayores distancias que el cable de par trenzado sin necesidad de que un repetidor amplifique la señal. El cable coaxial es más económico que el cable de fibra óptica. Además, debido a que se ha utilizado desde hace mucho tiempo para todos los tipos de comunicación de datos, esta tecnología es muy conocida.

El cable coaxial está disponible en distintos grosores. Por regla general, cuanto más grueso sea el cable más difícil será trabajar con él. Es importante tener esto en cuenta, especialmente si el cable se debe hacer pasar a través de canales de cables y conductos existentes de tamaño limitado. Como es rígido, debido al revestimiento, este tipo de cable coaxial frecuentemente se denomina *thicknet* (red gruesa).

Como regla general, cuanto más difícil de instalar es un medio de networking, más cara resulta la instalación.

3.1.2.2 Cable de par trenzado no blindado

El cable de Par Trenzado No Blindado/Unshielded Twisted Pair (UTP) que se muestra en la figura 3-2 consta de pares de hilos de cobre trenzados aislados que se utiliza en varios tipos de redes. El aislamiento es de teflón, lo cual produce menor diafonía y una señal de mejor calidad a distancias más largas, lo que los hace más adecuados para la comunicación de computadoras a alta velocidad. Cada hilo se trenza en forma helicoidal con el propósito de reducir la interferencia eléctrica de pares similares; el cable UTP posee cuatro pares de cobre de calibre 22 o calibre 24, tiene un diámetro externo de aproximadamente 0.43 cm. Este tamaño pequeño resulta conveniente durante la instalación.

En la actualidad el UTP es muy popular debido a que puede utilizarse con la mayoría de las arquitecturas principales de networking,

Figura 3-2 Cable de par trenzado no blindado

El cable UTP se instala fácilmente y es el más económico de todos los tipos de cableado de LAN. Sin embargo, la ventaja real del UTP es su tamaño; como su diámetro externo es tan pequeño, este tipo de cable no llena los conductos de cableado tan rápidamente como lo haría el cable coaxial.

Los conectores RJ, utilizados con este tipo de cable; son conectores estándar que originalmente se utilizaban para conectar líneas telefónicas y que en la actualidad se emplean para conectar redes; prácticamente aseguran una conexión sólida y de buena calidad, lo cual reduce en forma notable las fuentes potenciales de ruido de red.

En líneas generales, el cable UTP es más propenso a sufrir ruido eléctrico e interferencias que los otros tipos de medios de networking. Antiguamente se podía decir que el UTP no permitía una transmisión de datos tan veloz como otros tipos de cable. Sin embargo, en la actualidad el UTP es el medio más veloz basado en cobre. La distancia entre las amplificaciones de señal es más corta para el UTP que para el cable coaxial.

3.1.2.3 Cable de par trenzado blindado

El cable de Par Trenzado Blindado/Shielded Twisted Pair (STP) combina las técnicas de blindado y de trenzado de cables. Tal como se especifica para las instalaciones de red, si se instala correctamente, el cable STP brinda una resistencia excelente, tanto ante la interferencia electromagnética como ante la interferencia de radiofrecuencia sin que aumente de forma significativa el peso o tamaño del cable.

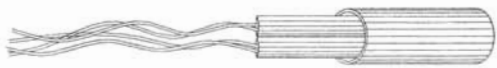


Figura 3-3 Cable de par trenzado blindado

El cable STP utiliza una cubierta de malla metálica de mayor calidad y protección que la del cable UTP, además el conjunto de pares se recubre con una lámina metálica fina, como se muestra en la figura 3-3. Este cable presenta todas las ventajas y desventajas del cable UTP; además de ofrecer mayor protección contra todos los tipos de interferencias externas que el cable UTP. Sin embargo, en general el cable STP es más caro que el cable UTP.

A diferencia del cable coaxial, en el caso del cable STP el blindaje no forma parte del circuito de datos. Por lo tanto, el cable debe estar conectado a tierra solamente en uno de los extremos. Por lo general, los instaladores conectan a tierra el cable STP en el armario para el cableado o en el hub.

Un cable STP que no esté conectado correctamente a tierra, puede transformarse en una fuente de problemas ya que permite que el blindaje actúe como una antena absorbiendo señales de otros cables y de fuentes de ruido eléctrico provenientes del exterior del cable. Por último, el cable STP no puede tenderse por tan grandes distancias como otros medios de networking, sin que sea necesario realizar amplificación.

3.1.2.4 Cable de fibra óptica

El cable de fibra óptica, es un medio de networking que puede conducir transmisiones de luz moduladas; éste cable no es susceptible a la interferencia electromagnética y permite una velocidad de datos más elevada que los cables UTP, STP y coaxial. Más específicamente, el cable de fibra óptica no transporta impulsos eléctricos como otros medios de networking con cable de cobre, sino que las señales que representan bits se transforman en haces de luz.

La comunicación por fibra óptica tiene su origen en inventos que datan del siglo XIX. Sin embargo, no fue hasta los años 60, cuando se inventaron las fuentes de luz láser en estado sólido y el vidrio de alta calidad libre de impurezas, que la comunicación por fibra óptica pasó a ser práctica.

Los precursores del uso generalizado del cable de fibra óptica fueron las empresas telefónicas que aprovecharon los beneficios que se obtenían al utilizar este cable para las comunicaciones de larga distancia.

El cable de fibra óptica consta de dos o más fibras de vidrio colocadas en envolturas individuales. En la figura 3-4 se puede apreciar un corte de éste cable, en ella se observa que cada fibra de vidrio está rodeada de capas de revestimiento reflector, un revestimiento plástico denominado *kevlar* (material de protección que se utiliza habitualmente en chalecos a prueba de balas) y una envoltura externa.

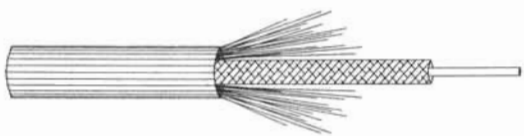


Figura 3-4 Cable de fibra óptica

La envoltura externa brinda protección al cable y generalmente es de plástico. Esta envoltura cumple con los códigos de protección contra incendios y de construcción adecuados. El propósito del kevlar es suministrar amortiguación y protección adicional a las frágiles fibras de vidrio, que tienen el grosor de un cabello. Cuando se necesitan cables de fibra óptica subterráneos, a veces se incluye un cable de acero inoxidable para reforzar el cable.

Las dos partes encargadas de guiar la luz en un cable de fibra óptica son el alma núcleo y revestimiento. El alma núcleo es un vidrio sumamente puro con un índice de refracción muy alto mientras que el revestimiento es de plástico o de vidrio con un índice de refracción ligeramente menor.

Cuando el revestimiento del alma núcleo tiene un índice de refracción bajo, la luz se captura en el alma núcleo de la fibra y a éste proceso se le denomina *reflexión interna total*; el cual permite que la fibra óptica actúe como un tubo de luz guiando el haz de luz a través de enormes distancias, incluso dando vuelta en codos, para llegar así al receptor y convertirla en señal eléctrica. El cable de fibra óptica no se ve afectado por la interferencia electromagnética y es completamente inmune a la interferencia de radiofrecuencia.

La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características:

- *Ancho de banda.* La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (UTP/STP) y el coaxial. El ancho de banda de la fibra óptica permite transmitir datos, voz, video etc.

- *Distancia.* La baja atenuación de la señal óptica permite realizar tendidos de fibra óptica sin necesidad de repetidores.

- *Integridad de datos.* En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores menor de 10^{-11}. Esta característica permite que los protocolos de comunicaciones de alto nivel, no necesiten implantar procedimientos de corrección de errores por lo que se acelera la velocidad de transferencia.

- *Duración.* La fibra óptica es resistente a la corrosión y a las altas temperaturas. Gracias a la protección de la envoltura es capaz de soportar esfuerzos elevados de tensión en la instalación.

- *Seguridad.* Debido a que la fibra óptica no produce radiación electromagnética, es resistente a las acciones intrusivas de escucha. Para acceder a la señal que circula en la fibra es necesario partirla, con lo cual no hay transmisión durante este proceso, y puede por tanto detectarse.

La desventaja del cable de fibra óptica es que es más caro y más difícil de instalar que los otros medios de networking. Como los conectores de fibra óptica son interfaces ópticas, se deben pulir hasta que queden perfectamente planos y sin rasguños, lo cual dificulta su instalación, misma que puede llevar varios minutos al realizar cada conexión.

Uno de los parámetros más característicos de las fibras es su *relación entre los índices de refracción del núcleo y de la cubierta* que depende también del radio del núcleo que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional.

Según este parámetro se pueden clasificar los cables de fibra óptica en dos clases:

- *Monomodo*; así se le denomina cuando el valor de la apertura numérica es inferior a 2,405 y cuando a través de la línea sólo viaja un único modo electromagnético; sólo se propagan los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo, en concreto un ancho de banda de hasta 50 GHz. Este tipo de fibras necesitan de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en MAN y en WAN. Resultan más caras de producir y el equipamiento es más sofisticado; puede operar con velocidades de hasta los 622 Mbps y tiene un alcance de transmisión de hasta 100 Km.

- *Multimodo*; así se le denomina cuando el valor de la apertura numérica es superior a 2,405 y cuando se transmiten varios modos electromagnéticos por la fibra. Este tipo de fibra es la más utilizada en las LAN por su bajo costo; los diámetros más frecuentes son de 62.5/125 y 100/140 micras. Las distancias de transmisión de este tipo de fibras están alrededor de los 2.4 Km y se utilizan a diferentes velocidades (10 Mbps, 16 Mbps, 100 Mbps y 155 Mbps).

  Existen dos tipos de fibra óptica multimodo:

  - *Con salto de índice*, la fibra óptica está compuesta por dos estructuras que tienen índices de refracción distintos. La señal de longitud de onda no visible por el ojo humano se propaga por reflexión; así se consigue un ancho de banda de hasta 100 MHz.

  - *Con índice gradual*, el índice de refracción aumenta proporcionalmente a la distancia radial respecto al eje de la fibra óptica. Es la fibra más utilizada y proporciona un ancho de banda de hasta 1 GHz.

3.1.3 Selección del medio de networking adecuado

Diversos criterios, tales como la velocidad de transferencia de datos y el costo, ayudan a determinar cual es el medio de networking que se debe utilizar. El tipo de material de conexión que se utiliza en una red determina, por ejemplo, la cantidad de datos que pueden transmitirse y la velocidad de dicha transmisión. Otros factores, tales como el gasto y el lugar en el que se utilizará el cable, también son importantes.

Para asegurar un rendimiento óptimo, es importante que los medios de networking transporten la señal de un dispositivo a otro con la menor degradación posible; para ello, utilizan técnicas de blindaje y de anulación. Las diferencias entre los tipos de blindaje y de anulación hacen que los cables difieran en tamaño, costo y dificultad de instalación.

Los medios de networking pueden utilizar distintos tipos de envoltura de cable. La envoltura es el revestimiento externo del cable. En general, es de algún tipo de plástico, revestimiento antiadherente o material compuesto. Al diseñar una LAN, es importante tener en cuenta que los medios de networking instalados entre las paredes o que atraviesan una unidad de distribución de aire, pueden servir de conducto para el fuego y hacer que un incendio se traslade desde un sector de un edificio a otro. Además algunas envolturas de los cables pueden emitir humo tóxico al quemarse.

Para evitar que esto suceda, se han implementado códigos de incendios, códigos de construcción y normas de seguridad que determinan el tipo de envolturas de cable que se pueden utilizar. Por lo tanto, el cumplimiento de dichos códigos también debe tenerse en cuenta al determinar el tipo de medios de networking que se deben utilizar en una LAN.

3.2 CAPA DE ENLANCE DE DATOS

En la capa física, todos los datos enviados a través de una red, parten desde una fuente y se dirigen a un destino, por lo que se puede concluir que la función de la capa física, es la transmisión de datos. Una vez que los datos fueron transmitidos, la *capa de enlace de datos* del modelo de referencia OSI proporciona acceso a los medios de networking y a la transmisión física a través de los medios, lo cual, permite que los datos ubiquen el destino propuesto en la red.

La capa de enlace de datos suministra un tránsito de datos confiable a través de un enlace físico; utiliza direcciones de Control de Acceso al Medio/Media Access Control (MAC) para ocuparse del direccionamiento físico (diferente del direccionamiento de la red, o lógico), de la topología de red, de la disciplina de línea (cómo utilizan el enlace de red los sistemas finales), la notificación de errores, la entrega ordenada de tramas y del control del flujo.

La dirección MAC es utilizada para definir una dirección de hardware o de enlace de datos para que varias estaciones puedan compartir el mismo medio y seguir manteniendo su identificación individual. Antes de que un paquete de datos se intercambie con un dispositivo conectado directamente en la misma LAN, el dispositivo que realiza el envío debe tener una dirección MAC que pueda utilizar como dirección de destino.

Cada equipo tiene una dirección física exclusiva para identificarse (esté o no conectado a la red). No existen dos direcciones físicas iguales; la dirección MAC, esta ubicada en una Tarjeta de Interfaz de Red/Network Interface Card (NIC), que aparece en la figura 3-5. De este modo, en una red, la NIC conecta un dispositivo con el medio; por esta razón, cada NIC, tiene una dirección MAC exclusiva.

Cuando un dispositivo desea enviar datos a otro dispositivo, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC del otro dispositivo. Cuando una fuente envía datos en la red, éstos datos llevan la dirección MAC del destino propuesto. A medida que estos datos viajan a través de los medios de networking, la NIC de cada dispositivo de la red verifica si la dirección MAC concuerda con la dirección del destino físico que transporta el paquete de datos. Si no existe una concordancia, la NIC hace caso omiso del paquete y éste continúa viajando por la red hasta la estación siguiente.

Sin embargo, cuando se produce una concordancia, la NIC hace una copia del paquete de datos y coloca la copia en la capa de enlace da datos del equipo. Aunque esta copia haya sido realizada por la NIC y haya sido colocada en el equipo, el paquete de datos original continúa viajando a través de la red, donde otras NIC podrán examinarla para saber si se puede encontrar una concordancia.

3.2.1 Tarjeta de interfaz de red (NIC)

La NIC actúa como la interfaz o conexión entre la computadora y el medio físico, convirtiendo los paquetes de datos en señales que se envían a través de la red.

Antes de que cada NIC salga de la fábrica, el fabricante de hardware le asigna una dirección física. Esta dirección se programa en un chip de la NIC.

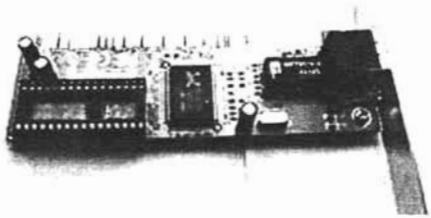


Figura 3-5 Tarjeta de interfaz de red (NIC)

Una NIC realiza las siguientes acciones:

- Prepara los datos del computador para su envío a la red. Los datos se mueven en la computadora, a través del bus de datos, en forma de bits en paralelo y cuando llegan a la tarjeta, los transmite en forma de bits en serie.

- Envía dichos datos a la red indicando su dirección para distinguirlos de las otras tarjetas de la red, la dirección de red son 12 dígitos hexadecimales y son determinadas por el IEEE. El comité asigna bloques de direcciones a cada fabricante de tarjetas. Los fabricantes introducen esas direcciones en chips en las tarjetas con un proceso conocido como *burning*, nacimiento de la dirección en la tarjeta. Con este proceso, cada tarjeta y por lo tanto cada computadora, tiene una dirección física única en la red.

- Controla el flujo de datos entre el computador y el sistema de cableado.

- Recibe los datos entrantes en serie del cable y los traduce en bytes en paralelo que la computadora pueda comprender.

Antes de que la tarjeta emisora envíe los datos a la red, se establece un dialogo electrónico con la tarjeta receptora para que ambas se pongan de acuerdo en lo siguiente:

- El tamaño máximo de los paquetes de datos que se quieren enviar;
- El total de datos a ser enviados antes de la confirmación;
- El intervalo de tiempo entre cada envío de paquetes de datos;
- El tiempo a esperar antes de que sea enviada la confirmación;
- Cuántos datos se puede almacenar en la memoria de cada tarjeta;
- La velocidad de transmisión de los datos.

Cada tarjeta indica a la otra sus parámetros y acepta o se adapta a los parámetros de la otra. Cuando todos los detalles de la comunicación han sido determinados, las dos tarjetas empiezan a enviar o recibir datos.

En la mayoría de las NIC, la dirección MAC se graba en la ROM. Cuando se inicializa la NIC, su dirección se copia en la RAM. Debido a que la dirección MAC está ubicada en la NIC, si se reemplaza la NIC de un equipo, la dirección física de la estación se cambia por la dirección de la nueva NIC.

3.3 CAPA DE RED

La capa de red provee una interfaz para las redes y presta los mejores servicios de entrega de paquetes de extremo a extremo a su usuario (la capa de transporte). La determinación de la ruta se produce en la capa de red. La función de determinación de la ruta permite que el router evalúe las rutas disponibles hacia un destino y establezca la mejor forma de manejar un paquete.

Los servicios de enrutamiento utilizan la información de topología de la red para evaluar las rutas que ésta contiene. Esta información la puede configurar el administrador de la red, o bien, puede obtenerse mediante procesos dinámicos que se ejecutan en la red.

En networking existen dos esquemas de direccionamiento: *el direccionamiento MAC* que ocurre en la capa de enlace físico y el *direccionamiento IP* que ocurre en la capa de red. Una dirección IP se basa en el Protocolo Internet. Cada LAN debe tener su propia dirección IP exclusiva, ya que la dirección IP es fundamental para que se produzca la interconexión en las WAN.

En un entorno de red IP, las estaciones terminales se comunican con otros servidores u otras estaciones terminales. Esto sucede porque cada nodo tiene una dirección IP, que es una dirección lógica única de 32 bits. Las direcciones IP normalmente son direcciones jerárquicas mientras que las direcciones MAC generalmente existen dentro de un espacio de direccionamiento plano.

Cada empresa que figura en la red se considera como una red única y exclusiva con la que se debe establecer el contacto antes de que se pueda contactar un host (ordenador conectado a la red, que tiene su propia dirección IP y que puede acceder a Internet) individual dentro de esa empresa. Cada red de empresa tiene una dirección y los hosts que residen en ella comparten la misma dirección de red, pero cada host se identifica mediante una dirección de host única en la red.

Una dirección IP incluye la dirección del dispositivo, así como también la dirección de la red en la que éste está ubicado. Por lo tanto, si un dispositivo se traslada de una red a otra, se debe cambiar la dirección IP del dispositivo para indicar que se ha realizado dicho cambio.

Las direcciones IP son flexibles debido a que se pueden establecer en el software. Las direcciones MAC están codificadas de forma permanente en el hardware. Ambos esquemas de direccionamiento son importantes para que las comunicaciones entre los equipos informáticos sean eficientes.

El direccionamiento IP hace posible que los datos que pasan por los medios de red de la Internet lleguen a su destino. La razón por la cuál las direcciones IP se escriben en forma de bits es que de éste modo los equipos informáticos pueden comprender la información que contienen. na dirección IP es un valor de 32 bits escrito en forma de cuatro octetos 11000000.00000101.00100010.00001011, la cuál también se expresa en número decimal 192.5.34.11

La razón por la cuál los datos llegan su destino en la Internet es que cada red conectada tiene un número de red único y exclusivo, para garantizar esto, la organización Centro Internacional de Información de Red (InterNIC), asigna bloques de direcciones IP a las empresas basándose en los tamaños de las redes.

Como se indica en la figura 3-6, cada dirección IP consta de dos partes: el número de red y el número de host. El número de red identifica la red de la que forma parte el dispositivo. El número de host identifica la conexión del dispositivo a esa red.

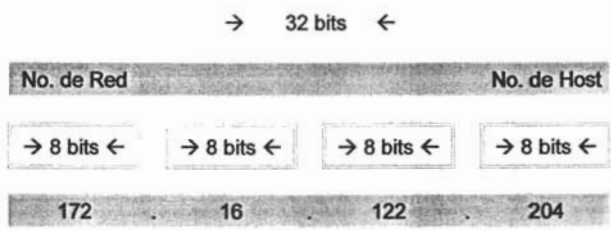


Figura 3-6 Dirección IP

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas). Las direcciones IP de clase A se reservan para entidades gubernamentales, clase B para empresas medianas y clase C para las demás.

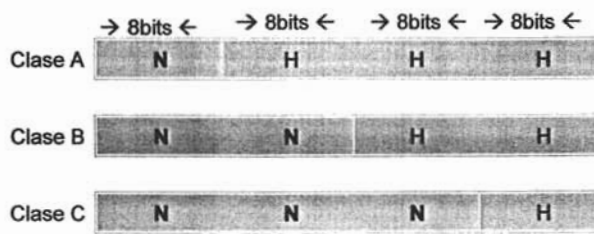
Cuando las direcciones IP de clase A se escriben en formato binario, el primer bit siempre es 0, en las direcciones IP de clase B , los primeros 2 bits siempre son 1 y 0; y en las direcciones IP de clase C , los 3 primeros bits son 1,1 y 0; como se muestra en la figura 3-7.

Clase	Tamaño de la dirección de red (en octetos)	Primer octeto (decimal)	Primer octeto (binario)	Número de direcciones locales
A	1	0 – 127	0000 0000 – 1111 1111	16, 777, 216
B	2	128 – 191	1000 0000 – 1011 1111	65, 536
C	3	192 – 223	1100 0000 – 1101 1111	256

- Las direcciones de clase D empiezan con un número entre 224 y 239.
- Las direcciones de clase E empiezan con un número entre 240 y 255.

Figura 3-7 Características de las clases de direcciones

En la figura 3-8 se muestra la representación de los bits que comprenden el número de red y el número de host que comprenden las direcciones IP clase A, B y C.



N = Número de red asignado por NIC

H = Número de host asignado por el administrador de la red

Figura 3-8 No. de host y de red en una dirección IP de clase A, B y C

3.4 CAPA DE TRANSPORTE

La capa de transporte define la conectividad de extremo a extremo entre aplicaciones de host. Los servicios de transporte incluyen cuatro servicios básicos:

- Dividir en segmentos las aplicaciones de la capa superior.
- Establecer operaciones de extremo a extremo.
- Enviar segmentos de un host final a otro host final.
- Garantizar la confiabilidad de los datos.

Esta capa, supone que pueden usar la red como una "nube" para enviar paquetes de datos desde el emisor hasta el receptor, tal como se indica en la figura 3-9.

La nube contiene cuestiones como por ejemplo: "¿Cuál de los distintos caminos es el mejor para una ruta determinada?". Es así como podemos comenzar a ver el papel que desempeñan los routers en este proceso.

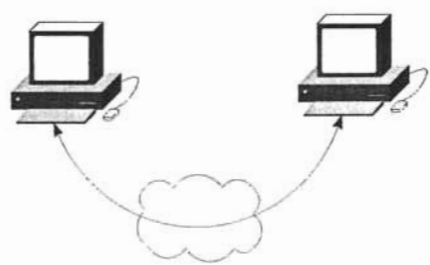


Figura 3-9 Funcionamiento de la capa de transporte

El flujo de datos de la capa de transporte proporciona servicios de trasporte desde el host hasta el destino. Este tipo de servicios suele denominarse *servicio de extremo a extremo*. El flujo de datos de la capa de transporte es una conexión lógica entre los puntos finales de una red.

3.4.1 Control de flujo

Al enviar segmentos de datos, la capa de transporte también puede organizar la integridad de éstos datos. Uno de los métodos para hacerlo se denomina *control de flujo*. El control de flujo evita el problema que se produce cuando un host ubicado en uno de los lados de la conexión hace que se desborden los búfers del host ubicado en el otro lado. Los desbordamientos pueden representar un problema grave, ya que pueden causar la pérdida de datos.

Los servicios de la capa de transporte permiten que el usuario solicite el transporte confiable de datos entre hosts y destinos. Para lograr dicho transporte confiable de datos, se utiliza una relación orientada a la conexión entre los sistemas finales que se comunican. El transporte confiable puede lograr lo siguiente:

- Garantizar que el emisor recibirá un acuse de recibo de los segmentos entregados.
- Permitir la retransmisión de cualquier segmento cuyo recibo no se haya confirmado.
- Colocar de nuevo los segmentos en su secuencia correcta en el destino.
- Evitar y controlar la congestión.

3.4.2 Establecimiento de una conexión con un sistema de iguales

En el modelo de referencia OSI, varias aplicaciones pueden compartir la misma conexión de transporte.

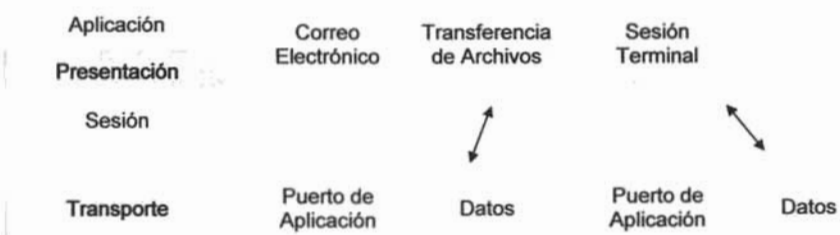


Figura 3-10 Conexión de transporte

Como se puede ver en la figura 3-10, la funcionalidad de transporte se logra segmento por segmento. Esto significa que las diferentes aplicaciones pueden enviar segmentos de datos según un sistema *first-come, first-served* (el primero en llegar es el primero en salir). Dichos segmentos pueden estar dirigidos al mismo destino o a muchos destinos diferentes.

Un usuario de la capa de transporte debe establecer una sesión orientada a conexión con su sistema de iguales. Para que comience la transferencia de datos, tanto el programa emisor como el programa receptor informan a sus respectivos sistemas operativos que se iniciará una conexión. Uno de los equipos hace una llamada que el otro equipo debe aceptar. Los módulos de software de protocolo de los dos sistemas operativos se comunican enviando mensajes a través de la red para verificar que se autoriza la transferencia y que ambos lados están preparados.

Una vez completa toda esta sincronización se considera que la conexión se ha establecido y comienza la transferencia de datos. Durante la transferencia, ambas máquinas se mantienen comunicadas a través de su software de protocolo para verificar la correcta recepción de los datos.

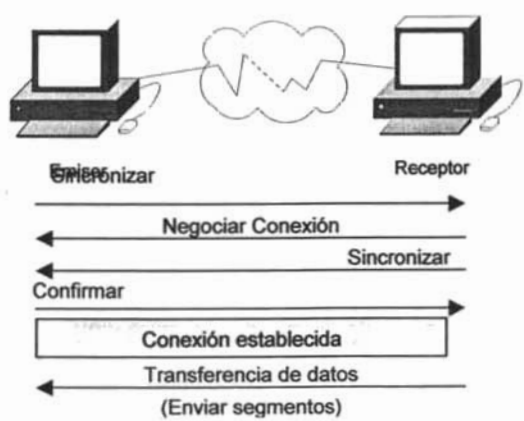


Figura 3-11 Conexión típica entre emisor y receptor

En la figura 3-11 se muestra una conexión típica entre sistemas emisores y receptores. El primer intercambio de señales solicita la sincronización, el segundo y tercer intercambio de señales confirman la petición de sincronización inicial y sincronizan los parámetros de conexión en sentido opuesto. El último segmento de intercambio de señales es una confirmación que se utiliza para

informarle al destino que ambos lados están de acuerdo en que se ha establecido una conexión. Una vez que se ha establecido la conexión, se inicia la transferencia de datos.

Cuando la transferencia de datos está en marcha, existen dos motivos por los cuales se puede producir una congestión. En primer lugar, un equipo de alta velocidad puede ser capaz de generar tráfico más rápidamente que lo que la red lo puede transferir; en segundo lugar, si varios equipos necesitan enviar simultáneamente datagramas (paquetes) al mismo destino, éste puede sufrir una congestión, aunque este problema no haya sido causado por un origen en particular.

Cuando los datagramas llegan demasiado rápido para que un host o un gateway los pueda procesar, éstos son almacenados en la memoria temporal. Si el tráfico continúa, con el tiempo el host o gateway se queda sin memoria y debe descartar los otros datagramas que lleguen.

En lugar de permitir que se pierdan los datos, la función de transporte, puede emitir un indicador de *"no está listo"* al emisor. Este indicador, que actúa como una señal de *"alto"*, le indica al emisor que deje de enviar datos. Cuando el receptor vuelve a ser capaz de manejar otros datos, el receptor le envía un indicador de transporte de *"listo"*, que se interpreta como una señal de *"siga"*. Como se indica en la figura 3-12, cuando el emisor recibe esta indicación, puede continuar con la transmisión de datos.

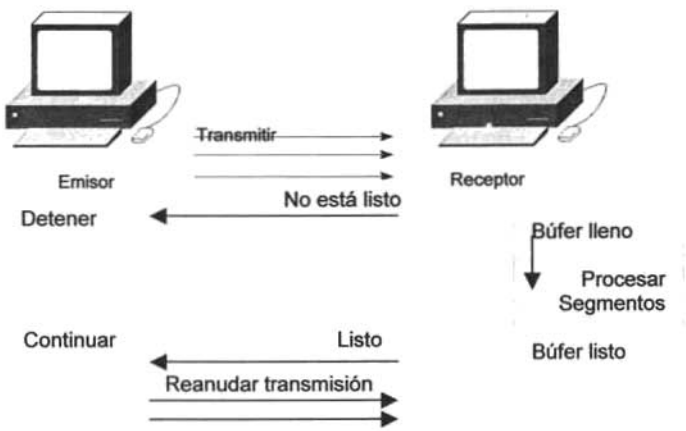


Figura 3-12 Transmisión entre emisor y receptor

3.4.3 Operaciones en ventana

En la forma más básica de la transferencia de datos orientada a conexión. Los paquetes de datos deben entregarse al receptor en el mismo orden en que se transmitieron, cuidando que ningún paquete de datos se pierda, se dañe, se duplique o se reciba en un orden diferente, ya que esto provocaría que el protocolo fallara. La solución básica consiste en que el receptor confirme la recepción de cada segmento de datos.

Si el emisor tiene que esperar el acuse de recibo después de enviar cada segmento, el desempeño será bajo. Como se dispone de tiempo después de que el emisor termina de transmitir el paquete de datos y antes de que termine de procesar cualquier acuse de recibo, éste intervalo se utiliza para transmitir más datos. La cantidad de paquetes de datos que un emisor puede tener pendiente sin haber recibido un acuse de recibo se conoce como *ventana*.

El método de operaciones en ventana permite controlar la cantidad de información que se transfiere de extremo a extremo. Algunos protocolos miden la información en términos del número de paquetes; otros como TCP/IP miden la información en términos del número de bytes.

La figura 3-13 muestra la transferencia de datos entre el emisor y receptor con un tamaño de ventana 3, el emisor puede transmitir tres paquetes de datos antes de esperar el acuse de recibo.

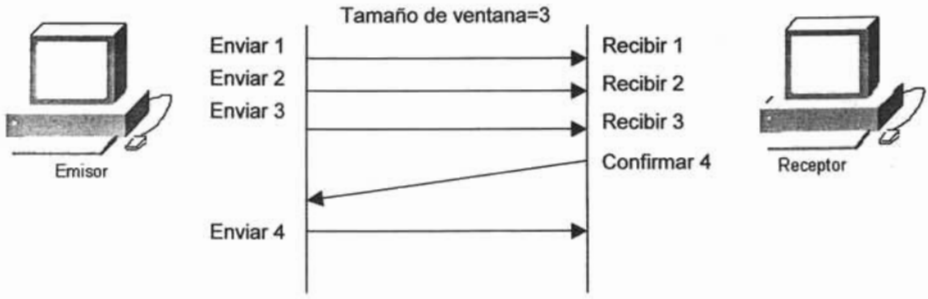


Figura 3-13 Operaciones en ventana

3.4.4 Acuse de recibo

La entrega confiable garantiza que el flujo de datos enviado desde un equipo sea entregado a través de un enlace de datos a otro equipo sin duplicación ni pérdida de datos. El *acuse de recibo positivo con retransmisión* es una técnica que garantiza la entrega confiable de los flujos de datos; requiere que el reflector se comunique con el origen, enviando un mensaje de confirmación al recibir los datos. El emisor lleva un registro de cada paquete de datos que envía y espera el acuse de recibo antes de enviar el próximo paquete, también pone en funcionamiento un temporizador de tal manera que evita que al enviar y retransmitir un segmento el tiempo se agote antes de que llegue el acuse de recibo.

La figura 3-14 muestra al emisor transmitiendo los paquetes de datos 1,2,3. El receptor confirma la recepción de los paquetes solicitando el paquete número 4. El emisor, al recibir el acuse de recibo, envía los paquetes 4, 5 y 6. Si el paquete 5 no llega al destino, el receptor confirma con una solicitud de reenvío del paquete número 5. El emisor vuelve a enviar el paquete número 5 y debe recibir un acuse de recibo para continuar así con la transmisión del paquete numero 7.

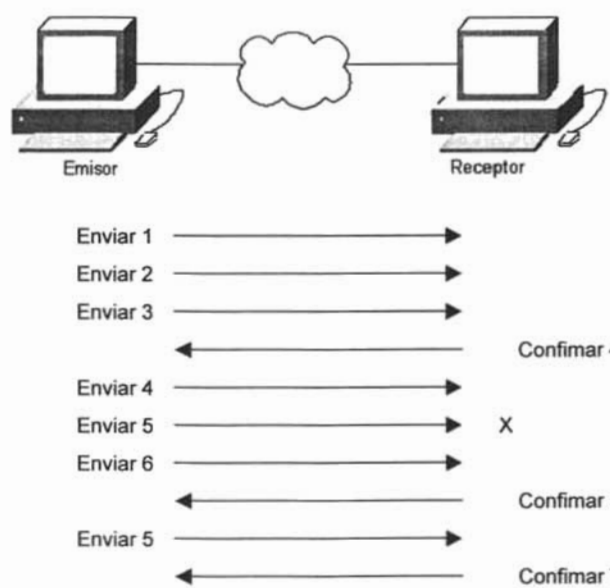
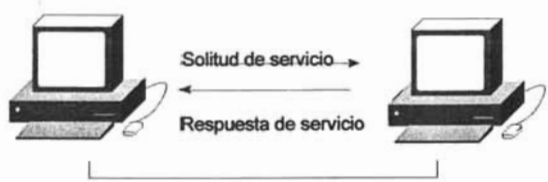


Figura 3-14 Acuse de recibo

3.5 CAPA DE SESION

El protocolo de ésta capa convierte el flujo de datos suministrados por las cuatro capas inferiores en sesiones mediante la implementación de diversos mecanismos de control. Entre estos mecanismos se incluyen la contabilidad, el control de conversación (al determinar, por ejemplo, quien puede conversar y cuando puede hacerlo) y la negociación de parámetros de sesión.

La capa de sesión establece, administra y finaliza sesiones entre aplicaciones. Esencialmente, como se indica en la figura 3-15, la capa de sesión coordina las solicitudes de servicio y las respuestas que se producen cuando las aplicaciones se comunican entre distintos hosts. El control de conversación de sesión se implementa a través del uso de un token, cuya posesión proporciona el derecho de comunicarse; el token se puede solicitar, y a los sistemas finales se les pueden otorgar prioridades que establecen el uso desigual del token.



- Sistema de archivos de red (NFS)
- Lenguaje de consulta estructurado (SQL)
- Llamada de procedimiento remoto (RPC)
- Sistema X Window
- Protocolo de sesión Apple Talk (ASP)
- Protocolo de control de sesión de arquitectura de red digital (SCP)

Figura 3-15 Funciones de la capa de sesión

3.6 CAPA DE PRESENTACION

La capa de presentación normalmente es un protocolo de paso para la información que proviene de las capas adyacentes. Esto permite que aplicaciones pertenecientes a distintos sistemas informáticos se comuniquen entre sí de forma transparente para dichas aplicaciones.

La capa de presentación proporciona el formateo y la conversión de los códigos. El formateo de códigos se utiliza para garantizar que las aplicaciones tengan información significativa para procesar. De ser necesario, esta capa puede convertir distintos formatos de datos.

La capa de presentación no solo se ocupa del formato y de la representación de los datos, sino que también se ocupa de la estructura de los datos que usan los programas; además de organizar los datos para su transferencia. Por ejemplo, se tienen dos sistemas, uno de los sistemas utiliza el código ampliado de caracteres decimales codificados en binario (EBCDIC) y el otro sistema utiliza el código americano normalizado para el intercambio de la información (ASCII) para representar los datos. Cuando ambos sistemas necesitan comunicarse, se requiere de la capa de presentación para convertir y traducir los datos de un formato a otro.

Otra de las funciones que se manejan en la capa de presentación es el cifrado de datos (comprimen el texto y convierten las imágenes gráficas en flujos de bits para que puedan ser transmitidas a través de una red), utilizado cuando es necesario proteger la información transmitida para que ésta no sea interceptada por receptores no autorizados. Para lograr esto, los procesos y los códigos ubicados en la capa de presentación deben convertir los datos.

Los estándares de la capa de presentación también guían la forma en que se presentan las imágenes gráficas. Tal como se indica en la figura 3-16, se puede usar un PICT, un formato de imagen que se utiliza para transferir imágenes gráficas de QuickDraw entre programas de Macintosh y PowerPC. Otro formato de presentación que se puede utilizar es el Formato de Archivos de Imágenes Etiquetadas/Tagged Image File Format (TIFF). Normalmente TIFF se usa para imágenes de mapas de bits de alta resolución. Otro de los estándares de la capa de presentación que se puede usar para imágenes gráficas es el del Grupo Común de Expertos en Fotografía/ Joint Photographic Experts Group (JPEG).

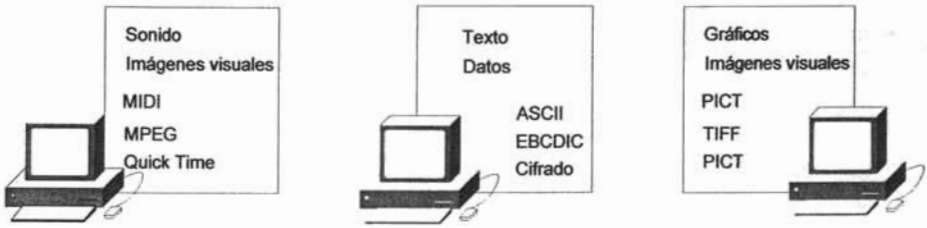


Figura 3-16 Funciones de la capa de sesión

Existen otros estándares de la capa de presentación que sirven de guía para la presentación de sonidos y películas. Entre éstos se incluyen la Interfaz Digital de Instrumentos Musicales/Musical Instruments Digital Interface (MIDI) para la música digitalizada, el estándar del Grupo de Expertos en Imágenes en Movimiento/Moving Picture Experts Group (MPEG) para la compresión y codificación de películas de video para CD, almacenamiento digital y velocidad de transmisión de hasta 1.5 Mbps, y QuickTime, un estándar que maneja audio y video para programas de Macintosh y PowerPC.

3.7 CAPA DE APLICACION

Brinda soporte para el componente de comunicación de una aplicación; las aplicaciones informáticas pueden utilizar solamente la información que reside en el equipo en el que funcionan dichas aplicaciones; en la figura 3-17 se enumeran varios tipos de aplicaciones de red. Netscape Navigator e Internet Explorer son probablemente las aplicaciones más conocidas.

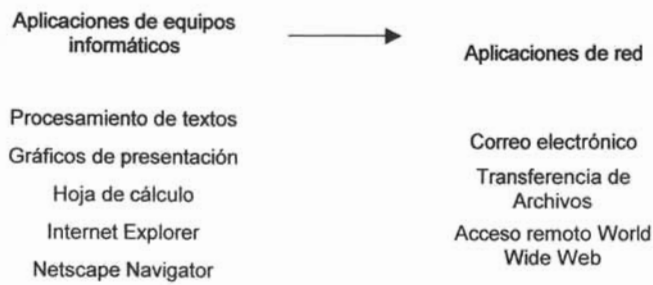


Figura 3-17 Aplicaciones de la red

Un procesador de textos puede incorporar un componente de transferencia de archivos que permita transferir un documento electrónicamente a través de la red. Este componente de transferencia hace que un procesador de textos pueda considerarse como una aplicación en el contexto OSI y pertenece a la capa de aplicación del modelo de referencia OSI. Los exploradores de la Web como Netscape Navigator e Internet Explorer también incluyen componentes de transferencia de datos. Un ejemplo de esto es lo que sucede cuando se visita un sitio Web; las páginas Web se transfieren a su equipo.

La capa de aplicación del modelo de referencia OSI incluye las aplicaciones en sí, así como también los *elementos del servicio de aplicaciones* (ASE), Los ASE facilitan la comunicación desde las aplicaciones hasta las capas inferiores. Los tres ASE más importantes son el elemento del servicio de control de asociación (ACSE), el *elemento del servicio de operaciones remotas* (ROSE) y el *elemento de servicio de transferencia confiable* (RTSE).

El ACSE asocia los nombres de las aplicaciones entre sí a modo de preparación para la comunicación de aplicación a aplicación. El ROSE implementa un mecanismo genérico de petición – respuesta que permite las operaciones remotas de modo similar al de las llamadas procedimiento remoto (RPC). El RTSE ayuda a que se produzca una entrega confiable al simplificar el uso de las construcciones de la capa de sesión.

Cinco de las aplicaciones OSI comunes son:

- *Protocolo de información de administración común/Common Management Information Protocol (CMIP):* proporciona capacidades de administración de la red. Al igual que SNMP y NetWiew, CMIP permite intercambiar la información de administración entre sistemas finales y estaciones de administración (que también son sistemas finales).

- *Servicios de directorio (DS)*: derivado del Comité Consultivo Internacional Telegráfico y Telefónico (CCITT; ahora denominada especificación X.500 del sector de normalización de las telecomunicaciones de la unión de telecomunicaciones internacional [ITU-T]), este servicio suministra capacidades distribuidas de base de datos que son útiles para la identificación y el direccionamiento de nodos de capas superiores.

- *Administración y acceso a la transferencia de archivos/File Transfer, Access and Management (FTAM):* proporciona servicio de transferencia de archivos. Además de la transferencia de archivos clásica, para la cual ofrece diversas opciones, también brinda funcionalidad distribuida de acceso de archivos similar a la de Netware de Novell, Inc., o al Sistema de Archivos de Red/Network File System (NFS) de Sun Microsystems, Inc.

- *Sistema de tratamiento de mensajes/Message Handling System (MHS)*: suministra un mecanismo de transporte subyacente para las aplicaciones de envío e mensajes electrónicos y otras aplicaciones que requieran servicios de almacenamiento y envío. Aunque cumplen propósitos similares, el MHS no es lo mismo que el MHS de Netware de Novell.

- *Protocolo de terminal virtual/Virtual Terminal Protocol (VTP)*: suministra emulación de terminales. En otras palabras, permite que un sistema informático aparezca ante un sistema final remoto como si fuera una terminal conectada directamente. Con VTP, los usuarios pueden ejecutar tareas remotas en mainframes.

CAPITULO IV

TOPOLOGIAS, DISPOSITIVOS Y TECNOLOGIAS DE RED

4.1 TOPOLOGIAS

Se denomina topología a la disposición física en la que se encuentran conectadas las estaciones de trabajo y servidores. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc. Se distinguen dos aspectos diferentes para considerar una topología:

- La *topología física,* es la disposición real de las máquinas, dispositivos de red y medios.

- La *topología lógica,* es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son de broadcast y transmisión de tokens.

Un diseño de red puede tener distinta topología física y lógica, es decir, la forma en que esta cableada una red no tiene porque reflejar necesariamente la forma en que viajan las señales a través de ella.

Las topologías físicas más comunes son: la topología de bus, la topología en estrella, la topología estrella extendida y la topología en anillo.

4.1.1 Topología de bus

Es una topología en la que todos los dispositivos de la LAN se encuentran conectados a un medio lineal de networking; este medio lineal a menudo se denomina línea de enlace troncal o bus, como se muestra en la figura 4-1. Todos los dispositivos, como las estaciones de trabajo y/o servidores, se encuentran conectados independientemente al cable de bus común mediante algún tipo de conexión.

El cable de bus debe terminar en una resistencia de terminación o terminador, que absorbe las señales eléctricas da tal manera que no reboten o se reflejen hacia delante y hacia atrás en el bus.

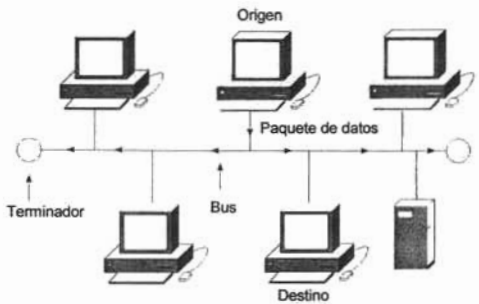


Figura 4-1 Topología de bus

Transmisión de señales en una topología de bus

En una topología de bus la señal viaja en ambas direcciones desde el equipo origen a través de los medios de networking, estas señales están disponibles para todos los dispositivos de la LAN. Cada dispositivo verifica los datos, si la dirección MAC/IP de destino portada por los datos no concuerda con la de un dispositivo determinado, éste hace caso omiso de los datos. Sin embargo, si la dirección MAC/IP de destino portada por los datos concuerda con la de un dispositivo determinado, éste copia los datos y los transmite a las capas de enlace de datos y de red del modelo de referencia OSI.

Cada extremo del cable posee un terminador, cuando una señal alcanza el extremo del bus, el terminador la absorbe. Esto evita que las señales reboten y que sean recibidas nuevamente por las estaciones de trabajo conectadas al bus. Para garantizar que sólo una estación de trabajo realice varias transmisiones a la vez, la topología de bus utiliza una *detección de colisión,* debido a que si más de un nodo intentara transmitir simultáneamente, los datos de cada dispositivo chocarían entre sí y como consecuencia se dañarían. Al área de la red dentro de la cuál se originan y chocan los paquetes de datos se denomina *dominio de colisión.* En una topología de bus, cuando un dispositivo de red detecta que se ha producido una colisión, la NIC emite una postergación; debido a que se basa en un algoritmo, la duración de esta demora de retransmisión forzada es diferente para todos los dispositivos de la red, lo que reduce al mínimo la posibilidad de otra colisión.

Ventajas y desventajas de la topología de bus

Una topología de bus típica presenta un diseño de cableado sencillo que usa medios de networking de longitud reducida. Por lo tanto, el costo de la implementación de este tipo de topología es generalmente bajo en comparación con el de otras topologías. Sin embargo el bajo costo de implementación se ve contrarrestado por sus elevados costos de administración. De hecho la principal desventaja es que el diagnóstico de errores y el aislamiento de los problemas de networking pueden resultar problemático debido a que hay pocos puntos de concentración.

Debido a que el medio de networking no pasa a través de los nodos conectados a él, si un dispositivo de la red falla, no afecta a los demás dispositivos de la red. Aunque esto puede representar una ventaja de la topología de bus, también se ve contrarrestado por el hecho de que el cable único utilizado puede actuar como punto único de fallo; así si falla el medio de networking usado para el bus, ninguno de los dispositivos ubicados a lo largo de dicho medio podrá transmitir señales.

4.1.2 Topología en estrella

Las LAN basadas en una topología en estrella usan un *nodo central de control*; los medios de networking conectan éste nodo o enlace central, como por ejemplo un hub o switch, a cada uno de los dispositivos conectados a la red, tal como se muestra en la figura 4-2.

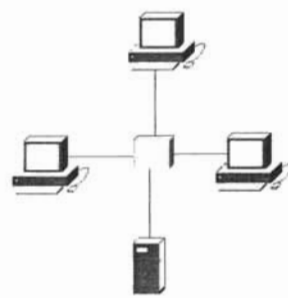


Figura 4-2 Topología en estrella

La topología en estrella es una de las más empleadas en los sistemas de comunicación de datos; se utiliza porque resulta fácil de controlar, su software no es complicado y su flujo de tráfico es

sencillo ya que todo el tráfico de la red atraviesa el nodo central. Los datos se envían primero al nodo central, y luego los dirige hacia el resto de las estaciones de trabajo o bien hacia la ruta del dispositivo asociado con la dirección de destino que portan los datos.

En una topología en estrella, el hub puede ser pasivo o activo. El hub pasivo simplemente conecta los medios de networking; mientras que un hub activo además de conectar los medios de networking, regenera la señal y actúa como un repetidor multipuerto. Al regenerar la señal, los hubs activos permiten que los datos recorran mayores distancias.

Ventajas y desventajas de la topología en estrella

Una red con topología en estrella es más fácil de diseñar e instalar; esto se debe a que cada estación está conectada directamente a un nodo central. El diseño utilizado para los medios de networking es de fácil modificación y el diagnóstico de problema es relativamente sencillo ya que es posible aislar las líneas para identificar el problema. Además, se pueden agregar fácilmente estaciones de trabajo a la red; si se rompe o se provoca un corto circuito en un segmento del medio de networking, solamente se pierde el uso del dispositivo conectado a ese segmento y el resto de la red sigue funcionando. En resumen, una topología en estrella significa mayor confiabilidad.

Una desventaja es que los costos de instalación son más elevados, debido a que por cada dispositivo se utiliza un tendido de cable. Además, todas las estaciones de trabajo podrían sufrir saturaciones y problemas en caso de avería del nodo central.

4.1.3 Topología en estrella extendida

Si una topología en estrella simple no ofrece suficiente cobertura para el área donde se debe colocar la red, puede extenderse mediante dispositivos de internetworking que no producen una atenuación de la señal. Esta topología se denomina *topología en estrella extendida* y se muestra en la figura 4-3.

Cuenta con las mismas propiedades, ventajas y desventajas de la topología en estrella.

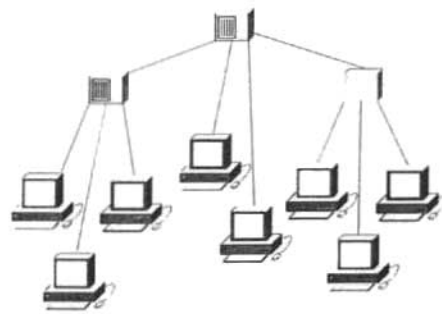


Figura 4-3 Topología en estrella extendida

4.1.4 Topología en anillo

La estructura en anillo es una configuración bastante extendida, se llama así por el aspecto circular del flujo de datos. En la mayoría de los casos los datos fluyen en una sola dirección y cada estación recibe la señal y la retransmite a la siguiente del anillo. La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos, tan frecuentes en los sistemas en estrella y árbol. Además la lógica necesaria para poner en marcha una red de este tipo es relativamente simple; cada componente sólo ha de llevar a cabo una serie de tareas muy sencillas como aceptar los datos, enviarlos a la estación de trabajo conectado al anillo o retransmitirlo al próximo componente del mismo.

Sin embargo, como todas las topologías, ésta también tiene algunos defectos. El problema más importante es que todos los componentes del anillo están unidos por un mismo canal; como se muestra en la 4-4, por lo que si falla el canal entre dos nodos, toda la red se interrumpe. Por eso algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se produce la pérdida de algún canal. Otros fabricantes construyen conmutadores que redirigen los datos automáticamente, saltándose el nodo averiado, hasta el siguiente nodo del anillo, con el fin de evitar que el fallo afecte a toda la red.

Figura 4-4 Topología en anillo

4.2 DISPOSITIVOS DE NETWORKING

El enviar datos a todos los dispositivos de la red puede funcionar en el caso de una red relativamente pequeña, pero se puede ver con facilidad que cuanto más grande sea una red, más tráfico se producirá en ella. Esto puede representar un problema grave, ya que se puede transportar solamente un paquete de datos a la vez a través de un cable. De no existir otro cable que interconecte cada dispositivo de una red, el flujo de datos que se transmite por la red será considerablemente más lento. Es por esto que por medio de los *dispositivos de networking* se puede controlar la cantidad de tráfico de una red y acelerar el flujo de datos a través de la misma.

Los dispositivos de networking se utilizan para conectar redes; a medida que aumenta el tamaño y la complejidad de las redes informáticas aumentará la cantidad de dispositivos de networking necesarios para conectarlas.

Todos los dispositivos de networking comparten uno o más propósitos comunes:

- Permiten que se conecte a la red una mayor cantidad de nodos.
- Aumentan la distancia a la que una red puede extenderse.
- Localizan el tráfico que se produce en la red.
- Pueden fusionar redes existentes.
- Aíslan los problemas de red para que se puedan corregir más fácilmente.

Un nodo es el punto final de una conexión de red o punto de unión que comparten dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo; varían en cuanto al enrutamiento y a otras aptitudes funcionales, pueden estar interconectados mediante enlaces y sirven como puntos de control en la red.

La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

La simbología más utilizada para los dispositivos de networking se muestra en la figura 4-5.

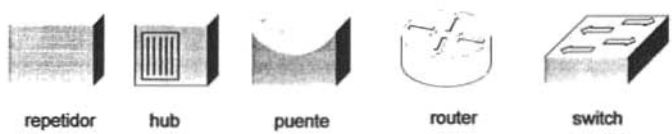


Figura 4-5 Dispositivos de networking

4.2.1 Repetidor

Son dispositivos de networking ubicados en la capa física del modelo de referencia OSI. Los datos se envían a través de la red en forma de impulsos eléctricos o de luz, los cuáles se transmiten a través de los medios de networking; a estos impulsos se les denomina señales. Cuando las señales salen por primera vez de una estación transmisora, están limpias y son claramente reconocibles; sin embargo, cuanto más largo es el cable, éstas se atenúan. Las especificaciones para el cable ethernet de par trenzado de la categoría 5e, establecen que la distancia máxima que las señales pueden transmitirse a través de una red es de 100 metros. Si una señal viaja más allá de esa distancia, no se garantiza que una NIC pueda leer la señal.

Un repetidor brinda una solución sencilla para éste problema, ya que recibe la señal debilitada, la limpia, la amplifica y la envía a través de la red, aumentando de ésta manera la distancia a la que puede operar la red; así como también es posible incorporar una mayor cantidad de nodos.

4.2.2 Hub

En una LAN, cada estación de trabajo está conectada a la red a través de algún tipo de medio de transmisión. Generalmente, cada servidor de archivos tiene solo una NIC. Por lo tanto, sería imposible conectar cada estación directamente al servidor de archivos. Para solucionar este problema, muchas LAN utilizan hubs, que son dispositivos de networking muy comunes.

Figura 4-6 El hub funciona como el centro de una red.

En términos generales, la palabra hub se utiliza en lugar de repetidor cuando se hace referencia al dispositivo que funciona como centro de una red, tal como se indica en la figura 4-6

Algunas de las propiedades de los hubs son las siguientes:

- Amplifican señales.
- Propagan señales a través de la red.
- No necesitan filtrarse.
- No requieren determinación de ruta o switching.
- Se utilizan como punto de concentración de la red.

Un hub recibe conexiones de todos los equipos conectados al mismo, de manera que existe una línea física entre cada equipo y el concentrador. El concentrador tiene un elemento interno, denominado plano posterior (backplane), al que se conectan todas las conexiones, formando un bus para todos ellos; todos los equipos comparten ese bus.

La desventaja de utilizar un hub es que no puede filtrar el tráfico de red. El filtrado habitualmente se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, como por ejemplo, una dirección de origen o una dirección de destino o protocolo y poder así determinar si desea enviar o descartar ese tráfico basándose en los criterios establecidos.

En un hub, los datos que llegan a un puerto se envían a todos los demás puertos, por consiguiente un hub transmite a todas las otras secciones o segmentos de una red sin tener en cuenta si los datos deben dirigirse a ese lugar o no y por lo tanto es posible que más de un usuario intente enviar datos por la red al mismo tiempo, lo que produciría una colisión. Una de las formas que existen para solucionar los problemas emergentes del tráfico excesivo en una red y del exceso de colisiones son utilizando un switch.

4.2.3 Switch

Es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red como anchos de banda pequeños y embotellamientos, opera en la capa de enlace del modelo de referencia OSI y reenvía los paquetes en base a la dirección MAC; siempre opera en una LAN y conecta segmentos de red en lugar de interconectar redes

Puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto, Su velocidad de operación es mayor que la de un puente, el cuál introduce mayores tiempos de retardo. En un switch se puede repartir el ancho de banda de la red de una manera apropiada en cada segmento de red o en cada nodo, de modo transparente a los usuarios. Esto proporciona facilidades para la construcción de redes virtuales.

Gran parte de los modelos comerciales de los switches son apilables, y por tanto, fácilmente escalables, por lo que les da una flexibilidad semejante a los repetidores, pero con la funcionalidad de los puentes en cuanto a la gestión del tráfico de la red se refiere.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final y reduciendo el número de estaciones a competir por el medio. No están diseñados con el propósito principal de un control íntimo sobre la red o como la última fuente de seguridad, redundancia o manejo.

Mientras que en el hub el ancho de banda de la máquina es compartido por todos los puertos mediante una multiplexación en el tiempo (sólo una estación puede transmitir de un puerto a otro en cada instante), en el switch el ancho de banda está por encima del ancho de banda de cada uno de los puertos.

Algunos switches de muy alto rendimiento se conectan en forma modular a un bus de muy alta velocidad (backplane), por lo que el ancho de banda del éste es la suma de los anchos de banda de cada uno de los puertos con lo que se garantiza que la conmutación será de alta velocidad y que unos segmentos de red no interferirán en otros.

4.2.4 Puente

Opera en la capa de enlace de datos del modelo de referencia OSI, divide en segmentos la red y filtra el tráfico basado en una estación o dirección MAC; elimina el tráfico innecesario y reduce las posibilidades de que se produzcan colisiones, solamente se ocupa de dejar pasar o no los paquetes.

Entre las propiedades más importantes de los puentes se encuentran las siguientes:

- Son más inteligentes que los hubs; es decir, pueden analizar los paquetes que llegan y enviarlos o impedir que pasen según la información de direcciones.
- Recogen y transmiten paquetes entre dos segmentos de red.
- Controlan las difusiones (broadcast) hacia la red.
- Mantienen tablas de direcciones.

En la figura 4-7 se muestra la interconexión de un puente

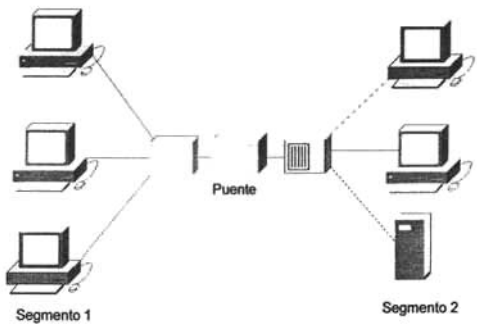


Figura 4-7 El puente conecta segmentos.

Para filtrar o entregar el tráfico de red de forma selectiva, los puentes crean tablas de red de todas las direcciones MAC ubicadas en una red y en otras redes y las asignan. Si llegan datos a través de los medios de networking, el puente compara la dirección MAC de destino que transportan los datos, con las direcciones MAC que aparecen en las tablas. Si el puente determina que la dirección MAC de destino de los datos proviene del mismo segmento de red que la dirección de origen, no envía los datos a otros segmentos de la red; pero si éste Si éste determina que la dirección MAC de destino de los datos no proviene del mismo segmento de red que la dirección origen, entonces envía los datos a todos los otros segmentos de la red.

Algunas de las ventajas que se cubren con el uso de un puente frente a una gran red son: una mayor *fiabilidad*, ya que si falla una de las redes la otra puede seguir funcionando, mayor *aislamiento* de la información manteniendo dentro de cada segmento el tráfico propio y mayor *rendimiento*, al circular por cada segmento sólo el tráfico de dicho segmento entre otras.

Se encarga también de comprobar el campo de control de errores de la trama con el fin de asegurarse de la integridad de la misma; si encontrara un error, eliminaría la trama de la red, con lo que tramas erróneas o incompletas no traspasarán la frontera del segmento de red donde se produjo el fallo. Algunos puentes son capaces de retocar de modo sencillo el formato de la trama (añadir o eliminar campos), con el fin de adecuarla al formato del segmento destinatario de la misma. El puente reexpide la trama si determina que el destinatario se encuentra en un segmento de red accesible por alguno de sus puertos.

Puesto que los puentes sólo pueden operar con direcciones MAC, no pueden tomar decisiones de encaminamiento que afecten a los protocolos o sistemas de direccionamiento de la capa de red. Existen distintas estrategias para redirigir los mensajes por el camino apropiado:

- *Puente transparentes*, usados principalmente en entornos Ethernet.
- *Puente con enrutamiento fuente*, usados principalmente en entornos Token Ring.
- *Puente con enrutamiento fuente-transparente*, que se utilizan para la interconexión de entornos Ethernet con entornos Token Ring.

Una segunda clasificación en los puentes atiende a si las redes que se van a conectar están próximas, estos son: los puentes locales y puentes remotos.

- *Puente local*, proporciona conectividad entre segmentos de una red dentro de un área local, como puede ser una oficina, una planta de un edificio o un edificio.
- P*uente remoto*, conecta segmentos de redes en áreas diferentes, normalmente interconectados mediante líneas de telecomunicaciones, por ejemplo, enlaces dedicados, líneas RDSI, línea telefónica, etc.

En la figura 4-8 se muestra la representación esquemática de la diferencia entre un puente local y un puente remoto.

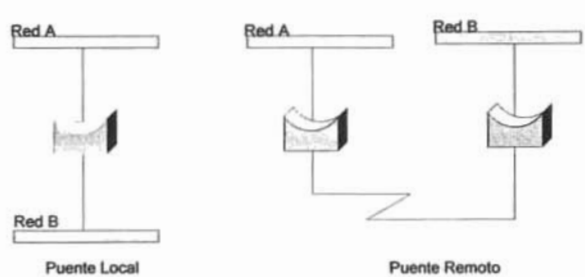


Figura 4-8 Tipos de puentes, locales y remotos.

4.2.5 Router

Se utilizan para conectar redes separadas y para que éstas puedan acceder a Internet, proporcionan enrutamiento punto a punto transmitiendo paquetes de datos y enrutando el tráfico entre distintas redes basándose en el protocolo de red o en la información de la capa de red. Tal como se indica en la figura 4-9, tienen la capacidad de tomar decisiones con respecto a cual es la mejor ruta para la entrega de datos de la red.

Los routers solucionan el problema del exceso de tráfico de broadcast (difusión) ya que no envían tramas de broadcast a menos que se les indique específicamente que lo hagan; además de proporcionar seguridad, control y redundancia entre dominios individuales de broadcast y dar servicio de firewall y acceso económico a una WAN.

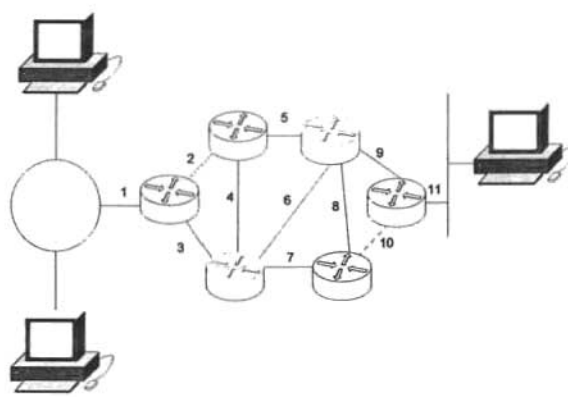


Figura 4-9 Los routers determinan cual es la mejor ruta para entregar datos en la red

Los routers se diferencian de los puentes en varios aspectos:

El puenteado se produce en la capa de enlace de datos, mientras que el enrutamiento se produce en la capa de red del modelo de referencia OSI. Los puentes utilizan direcciones físicas o direcciones MAC para tomar decisiones sobre el envío de datos. Los routers utilizan direcciones de capa de red, denominadas Protocolo de Internet/Internet Protocol (IP) o direcciones lógicas en lugar

de direcciones MAC. Las direcciones IP se implementan en el software y se refieren a la red en la que está ubicado un dispositivo.

Un puente sólo puede conectar redes con el mismo protocolo de la capa de enlace de datos o protocolos relativamente similares (Ethernet y Token Ring). Un router se suele emplear para la interconexión de redes con protocolos de la capa de enlace de datos diferentes, siempre y cuando compartan el mismo protocolo de la capa de red. Los routers comerciales suelen tener capacidad para encaminar los protocolos más utilizados: IP, IPX, Apple Talk, DECnet, etc.

Resolución de direcciones

Para que funcione correctamente el enrutamiento de la capa de red es necesario realizar una correspondencia entre las direcciones de red y las direcciones de la capa de enlace de datos; éstas direcciones vienen asignadas con la interfaz de red desde fábrica y son las que se utilizan en último término para la comunicación a través de la red. Las direcciones de la capa de red las asigna el administrador de la red a su elección, siendo independientes de la capa de enlace de datos.

Las direcciones de la capa enlace de datos se pueden obtener, a partir de las direcciones de la capa de red, mediante el Protocolo de Resolución de Direcciones/Address Resolution Protoco (ARP). Por ejemplo, se tienen dos computadoras A y B en la misma red; la computadora A difunde un mensaje ARP pidiendo la dirección MAC de B. Este mensaje lo reciben todos los equipos conectados a la LAN, pero solo responde B con su dirección MAC. En ese momento B ha apuntado en su caché de ARP la dirección MAC de B. De esta forma cuando A envíe un mensaje a B sólo tiene que consultar en su caché la dirección MAC de B a la que tiene que enviar el mensaje.

El protocolo es un poco diferente cuando la computadora de destino se encuentra en otra red. Por ejemplo, se tienen dos computadoras A y Z situadas en redes diferentes interconectadas a través de uno o más routers. Cuando A intenta obtener la dirección MAC de Z, difunde por la red un mensaje ARP; igual que antes todos los equipos conectados a la LAN reciben el mensaje. El router también recibe el mensaje y observa en su tabla de enrutamiento que es para una computadora que se encuentra en otra red; entonces responde a la petición de dirección MAC con se propia dirección MAC haciendo de sustituto de la computadora de destino.

Cuando A reciba la respuesta apuntará como dirección MAC de la computadora Z la dirección MAC del router;. Cuando A envía un mensaje a Z, busca su dirección MAC y la encuentra en su caché de ARP, que en realidad es la del router, y le envía a este último el mensaje. El router recibe el mensaje y lo redirige hacia la computadora Z. Esta segunda parte, cuando la máquina de destino se encuentra en una red diferente, se puede eliminar si se actúa de manera

4.2.6 Gateway

Actúa en las capas superiores de la red, pudiendo llegar a la capa de aplicación. Se utiliza en aquellos casos en que la adaptación entre las dos redes requiera una conversión de los protocolos superiores al protocolo de red proporcionan conectividad entre redes de distinta naturaleza.

Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y, paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida. Los gateways también pueden interconectar redes entre sí.

4.3 TECNOLOGIAS DE RED

Ethernet, Interfaz de Datos Distribuida por Fibra/Fiber Distributed Data Interface (FDDI) y Token Ring son tecnologías de red ampliamente utilizadas que pueden encontrarse prácticamente en todas las LAN en uso, como se muestra en la figura 4-10.

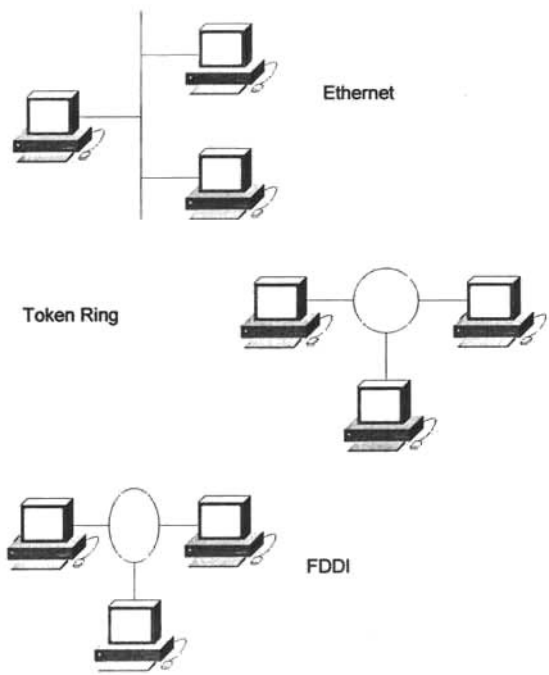


Figura 4-10 Tecnologías de red

Los *estándares de LAN* especifican el cableado y la señalización en la capa física y en la capa de enlace de datos del modelo de referencia OSI. La tecnología de red mas utilizada en la actualidad es la Ethernet.

4.3.1 Estándares de LAN Ethernet e IEEE 802.3

El Centro de Investigación de Palo Alto/Palo Alto Research Center (PARC), de Xerox Corporation, desarrolló Ethernet en los años 70. Las primeras LAN requerían poco ancho de banda para ejecutar las tareas de red sencillas que eran necesarias en aquella época: enviar y recibir correo electrónico, transferir archivos de datos y administrar los trabajos de impresión.

En 1980, el Instituto de Ingeniería Eléctrica y Electrónica/Institute of Electrical and Electronics Engineers (IEEE) presentó la especificación IEEE 802.3 cuya base tecnológica era Ethernet. Poco después, Digital Equipment Corporation, Intel Corporation y Xerox Corporation desarrollaron y presentaron de forma conjunta una especificación Ethernet (Versión 2.0) que es substancialmente compatible con IEEE 802.3. Estos dos estándares, Ethernet e IEEE 802.3 actualmente dominan el mercado de los estándares de LAN.

La LAN Ethernet se conoce como una tecnología de medios compartidos, es decir, todos los dispositivos están conectados a los mismos medios de entrega. *Medio de entrega* es el método utilizado para transmitir y recibir datos; los datos electrónicos se pueden transmitir a través de cable de cobre, cable coaxial grueso (thicknet), cable coaxial delgado (thinnet), transferencia inalámbrica de datos, etc.

El diseño original de Ethernet representaba un punto medio entre las redes de larga distancia y baja velocidad y las redes especializadas de las salas de equipos de informática, que transportaban datos a altas velocidades a través de distancias muy limitadas. Ethernet se adecua bien a las aplicaciones en las que un medio de comunicación local debe transportar una cantidad importante de tráfico de forma ocasional y esporádica a velocidades de datos muy elevadas.

Los estándares Ethernet e IEEE802.3 definen una LAN con topología física de estrella y lógica de bus y se caracterizan por su alto rendimiento de una velocidad de señalización de banda base de 10-100 Mbps.

Existen tres estándares definidos de cableado en una red Ethernet.

- *10 Base 2*, usa un cable coaxial delgado, por lo que se puede doblar más fácilmente; además de ser barato y fácil de instalar. Acepta segmentos de red de hasta 185 metros y 30 nodos.

- *10 Base 5*, usa un cable coaxial grueso; puede tener hasta 100 nodos conectados con una longitud de cable de hasta 500 metros.

- *10 Base T*, cada estación tiene una conexión con un hub o switch central, usa un cable de par trenzado, es la tecnología más común hoy en día. Acepta segmentos de red de hasta 100 metros.

Los estándares 10 Base 5 y 10 Base 2 permiten que varias estaciones accedan al mismo segmento de LAN. Las estaciones se conectan al segmento a través de un cable que parte desde una *Interfaz de Unidad de Conexión* (AUI) de la estación hasta un transceptor que se denomina Unidad de conexión al medio/Multistation Access Unit (MAU), conectado al cable coaxial Ethernet.

El estándar 10 Base T brinda acceso solo a una estación, las estaciones casi siempre están conectadas a un hub o a un switch (en este diseño, el hub o switch es equivalente a un segmento Ethernet).

Las capas de enlace de datos Ethernet y 802.3 brindan transporte de datos a través del enlace físico que une dos dispositivos, por ejemplo, en la figura 4-11, los tres dispositivos se pueden conectar directamente entre sí a través de una LAN Ethernet.

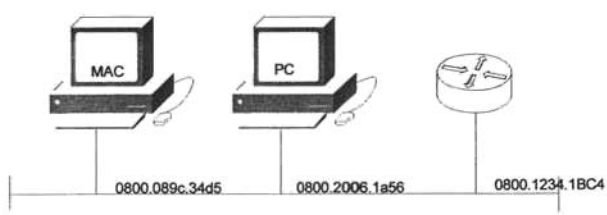


Figura 4-11 Distintos tipos de acceso

La Macintosh que aparece a la izquierda y la PC basada en Intel que aparecen en medio, muestran las direcciones MAC utilizadas por la capa de enlace de datos. El router que aparece a la derecha también utiliza una dirección MAC para cada una de sus interfases.

4.3.1.1 Funcionamiento de Ethernet/802.3

En una red Ethernet, la transmisión de un nodo atraviesa la totalidad del segmento y cada nodo la recibe y la examina. Cuando la señal llega al final de un segmento, los terminadores la absorben para evitar que retroceda dentro del segmento. Sólo se puede realizar una transmisión en la LAN en un momento dado. Por ejemplo, en la figura 4-12 aparece una red de bus lineal donde la estación A transmite un paquete cuya dirección de destino es la estación D. Todas las estaciones reciben este paquete, la estación D reconoce la dirección MAC y procesa la trama, mientras tanto las estaciones B y C no reconocen la dirección y descartan la trama.

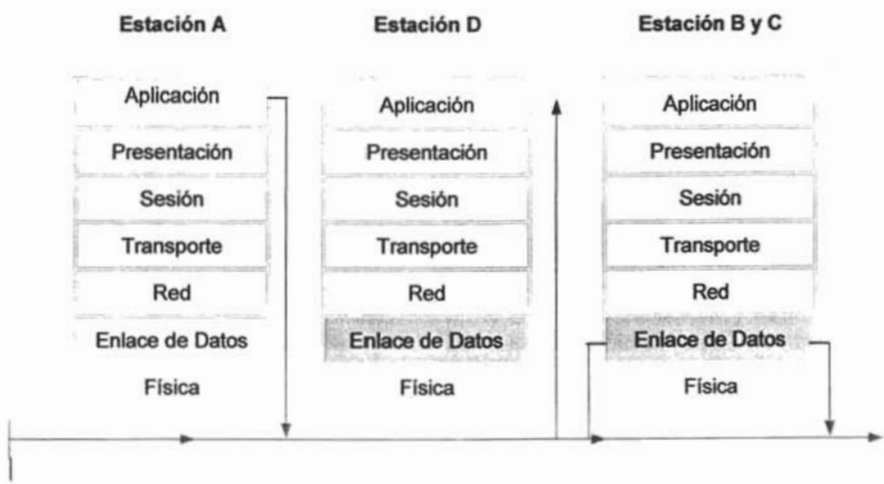


Figura 4-12 Funcionamiento de una red Ethernet

4.3.1.2 Broadcast Ethernet/802.3

La difusión (broadcast) es una poderosa herramienta que envía una única trama a muchas estaciones a la vez. Esta técnica utiliza una dirección de destino de enlace de datos conformada por números uno (FFFF.FFFF.FFFF. en sistema hexadecimal).

Como se muestra en la figura 4-13, si la estación A transmite una trama con una dirección de destino formada por números uno, las estaciones B, C y D deben recibir y transmitir la trama a las capas superiores para su posterior procesamiento.

Figura 4-13 Difusión broadcast

La difusión (broadcast) puede afectar seriamente al desempeño de las estaciones al interrumpirlas innecesariamente. Por este motivo, se deben utilizar sólo cuando se desconoce la dirección MAC de destino o cuando el destino es todas las estaciones.

4.3.1.3 Medios de acceso

Ethernet es una *tecnología de medios compartidos*, lo que significa que todos los dispositivos de red deben negociar el derecho para realizar la transmisión. El método de acceso al medio más utilizado en las redes locales es el Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones/Carrier Sense Multiple Access with Collision Detection (CSMA/CD), utilizado por Ethernet /IEEE802.3 100 Base T y otros.

Acceso múltiple con detección de portadora y detección de colisiones

En este método cuando un nodo tiene que transmitir en primer lugar observa el medio para ver si existe algún nodo transmitiendo.

Si no detecta señal en el medio empieza la transmisión. Durante la transmisión observa la línea para ver si algún otro nodo comenzó a transmitir mientras el lo hacía. El que un nodo empiece a transmitir cuando otro ya ha iniciado la transmisión se debe a la distancia que los separa a ambos. Desde que un nodo empieza a transmitir hasta que otro recibe esa señal pasa un tiempo, en el cuál un segundo nodo puede haber detectado que el medio estará libre y haber empezado a transmitir.

Si detecta una señal en el medio se queda escuchando hasta que la transmisión termina y en ese momento empieza a transmitir inmediatamente.

Si se detecta una colisión como se muestra en la figura 4-14, la estación deja inmediatamente de transmitir. Espera un tiempo aleatorio y vuelve a intentarlo. Si al intentar transmitir vuelve a producirse una colisión se utiliza un algoritmo denominado *Binary Exponential Backoff* en el que el tiempo que se espera para volver a intentar transmitir se va duplicando en cada intento. Si tras 16 intentos no se consigue la transmisión, se devuelve un error a quien solicitó la transmisión. Este modelo se denomina *persistente*. Los nodos una vez que han detectado una colisión vuelven a transmitir de manera persistente.

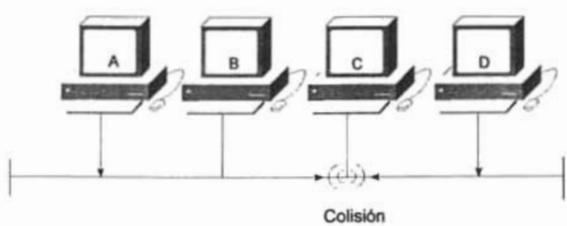


Figura 4-14 Colisión en CSMA/CD

4.3.2 Fast Ethernet

Desde la aparición del estándar IEEE 802.3, se ha ido demandando una red que permitiese una mayor velocidad de transmisión. La especificación de una red Ethernet a 100 Mbps se denomina 100 Base T. Su concepción es la de mantener el nivel de enlace MAC, del estándar IEE802.3, pero modificado, debido a que debe manejar mayores velocidades de transmisión, medios físico de transmisión distintos al definido en el estándar de Ethernet.

Existen tres medios definidos para Fast Ethernet:

- *100 Base TX,* sobre dos hilos de par trenzado STP o UTP de categoría 5
- *100 Base T4,* sobre cuatro hilos de par trenzado STP o UTP de categoría 3, 4, 5, 5e o 6
- *100 Base FX,* sobre fibra óptica multimodo

Las redes Fast Ethernet disponen de un mecanismo denominado auto negación que permite a un dispositivo intercambiar información con el concentrador al que se encuentra conectado para informarle de sus capacidades, mejorando de esta forma el entorno. Esta información se envía mediante pulsos que permiten comprobar la integridad del enlace, de la misma forma que hace Ethernet, pero que transmiten información extra.

En este proceso de autonegación el dispositivo y el concentrador intercambian información sobre la velocidad de transferencia, ya que los concentradores Fast Ethernet también suelen admitir conexiones Ethernet normal a 10 Mbps, modo de comunicación Full Duplex para aquellos dispositivos que lo permitan y una configuración automática de aquellos nodos con 100 Base TX o 100 Base T4. Si un extremo del enlace no admite autonegación, el dispositivo se pone automáticamente en el modo 10 Base T.

En este entorno en el que puede haber dispositivos a 10 Mbps los concentradores han de realizar una función intermedia para adaptar los flujos entre estos dos dispositivos. Por ello es necesaria la existencia de un sistema de control de flujo mediante el cual el concentrador, cuando una estación le envía un flujo mediante de información muy grande y se van llenando los buffers de comunicación con el nodo más lento. Cuando vuelva a disponer de sitio vuelve a enviar una trama indicándole que puede continuar.

Si llegase información al concentrador cuando éste tiene su buffer lleno tiraría las tramas que no es capaz de almacenar temporalmente.

4.3.3 Gigabit Ethernet

Gigabit Ethernet es una extensión del estándar IEE 802.3, pero multiplicando por diez la velocidad de Fast Ethernet, hasta una velocidad de 1 Gbps. Surge como competidor de los protocolos utilizados en redes troncales. Su mayor ventaja es la de utilizar un protocolo bien conocido desde hace tiempo y por tanto, al que se pueda actualizar fácilmente utilizando los conocimientos que ya se disponen en los equipos técnicos de gestión de red.

Para conseguir una velocidad de 1 Gbps, se modifican las características de la capa física del estándar IEEE 802.3. El resto de las capas de red hacia arriba permanece igual

La especificación de Gigabit Ethernet considera el uso de tres medios de transmisión: Onda Larga/Long Wave (LW) con un láser por fibra monomodo o fibra multimodo, llamado también 1000 Base LX, Onda Corta/ Short Wave (SW) con un láser sobre fibra multimodo, llamado también 1000 Base SW y por cable de par trenzado de 150 ohmios, llamado 1000 Base CX.

CAPITULO V

SISTEMA DE CABLEADO ESTRUCTURADO

5.1 SISTEMA DE CABLEADO ESTRUCTURADO

Un sistema de cableado estructurado es una infraestructura flexible de cables que soporta múltiples sistemas de comunicaciones, independientemente del fabricante de los componentes del mismo. En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema. Esto permite la comunicación con cualquier dispositivo, en cualquier momento.

En otras palabras, un sistema de cableado estructurado es una red de telecomunicaciones, compuesta por módulos o subsistemas que se adaptan a las necesidades de la empresa y tiene como entorno uno o varios edificios.

Las características de un sistema de cableado estructurado son las siguientes:

- Cuentan con una alta capacidad de integración,
- Están basados en estándares,
- Funcionan bajo una topología de estrella extendida,
- Son flexibles y prevén posibilidades de crecimiento,
- Son de fácil administración por parte del cliente,
- Soportan múltiples servicios,
- Son económicos al momento de cambios y expansiones,
- Tienen un bajo costo de mantenimiento,
- Mantienen una excelente relación Precio / Valor

Lo cual brinda ciertas ventajas como que se puede tener una administración centralizada, la canalización para todos los servicios es una, se ocupa un menor espacio de cuarto de equipo, entre otras.

5.2 ELEMENTOS DE UN SISTEMA DE CABLEADO ESTRUCTURADO

La infraestructura de telecomunicaciones ha sido dividida en 7 elementos o subsistemas, los que soportarán la implementación de un cableado basado en los estándares.

5.2.1 Area de trabajo

Es el espacio dentro del edificio donde los ocupantes interactúan con los dispositivos de telecomunicaciones. Unicamente cubre desde la salida de telecomunicaciones hasta el equipo del usuario; pudiendo ser éste cualquiera de un número diferente de dispositivos como computadoras, teléfonos, impresoras, fax, etc.

Para los objetivos de planificación, el espacio estimado para cada área de trabajo es de 3 x 3 metros aproximadamente; ya que el cableado del área de trabajo puede tener un máximo de 3 m y puede variar su forma dependiendo de la aplicación. El cableado generalmente no es permanente y se diseña de forma tal de ser relativamente fácil su cambio.

Los faceplates, cajas universales, jacks y otros dispositivos de conectividad deben instalarse entre la boca de la pared y la estación de trabajo.

5.2.2 Cableado horizontal

El esquema del cableado horizontal comprende la mayoría del cableado a instalarse; es el cableado que conecta a la salida del usuario con el punto de interconexión horizontal o distribuidor de piso al área de trabajo. La máxima longitud de este cableado es de 90 m.

5.2.3 Cuarto de telecomunicaciones

La función principal del cuarto de telecomunicaciones es la terminación del cableado horizontal; contiene el punto de transición entre el cableado horizontal y de backbone. Por lo que debe contener

los equipos de telecomunicaciones, las terminaciones de cables, el hardware de interconexión y las interconexiones asociadas.

Un edificio debe tener mínimo un cuarto de telecomunicaciones por piso; la excepción a esta regla puede ser un piso donde la mayoría del espacio este ocupado por un área de recepción y pueda no requerir un cuarto de telecomunicaciones, en este caso puede alimentarse de un cuarto de telecomunicaciones del piso adyacente. Un único cuarto no puede atender a más de 1000 m^2. Para cada 1000 m^2 adicionales debe colocarse un cuarto más.

El cuarto de telecomunicaciones debe ubicarse tan cerca como sea posible del centro del área que atenderá y debe dedicarse solo a la función de telecomunicaciones y a las facilidades de soporte relacionadas. En un lugar libre de humedad excesiva, polvo y otros contaminantes que puedan dañar el hardware de red.

5.2.4 Cableado de backbone

Provee interconexiones entre edificios y dentro del edificio; entre puntos de interconexiones principales e intermedios (distribuidores de campus y de piso) y entre puntos de interconexión intermedia y horizontales (distribuidores de edificio y de piso).

Los interbuilding son backbones entre edificios y los intrabuilding son backbones dentro del edificio entre distintos distribuidores. Los backbones intrabuilding pueden correr verticalmente entre pisos y/u horizontalmente.

5.2.5 Cuarto de equipos

Provee un ambiente controlado central para albergar el equipo de telecomunicaciones, los puntos de interconexión, hardware de conectividad, empalmes, las facilidades de puesta a tierra y anclaje y los aparatos de protección.

5.2.6 Entrada de facilidades

Consiste en la entrada de servicios de telecomunicaciones al edificio, a través de la pared del edificio dentro del cuarto de entrada: puede contener las canalizaciones para backbone que vinculan con otros edificios en una configuración de campus.

5.2.7 Administración

La administración no es un elemento físico de la infraestructura de telecomunicaciones pero mantiene los registros de todos los otros elementos de cómo están implementados dentro de la infraestructura. Es también el método que gobierna cómo los elementos son etiquetados para su identificación.

5.3 ESTANDARES DE LOS MEDIOS DE NETWORKING

Los estándares son conjuntos de normas o procedimientos de uso generalizado o bien, que se han especificado oficialmente y que funcionan como una especie de plano para asegurar una mayor compatibilidad e interoperabilidad entre los diferentes tipos de tecnologías de red producidas por diversas empresas de todo el mundo.

A principios de los años 90, la industria de telecomunicaciones reconoció la necesidad de establecer lineamientos para el cableado de voz y datos de edificios. Estos lineamientos proveen la dirección para efectuar instalaciones correctas de los nuevos productos para telecomunicaciones así como los detalles para realizar movimientos, adiciones y cambios en una instalación existente.

Los estándares para networking son desarrollados y publicados por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), Underwriters Laboratory (UL), Asociación de Industrias Electrónicas (EIA), y la Asociación de la Industria de las Telecomunicaciones (TIA). Las últimas dos organizaciones publican en forma conjunta una lista de estándares, que con frecuencia se denominan estándares EIA/TIA. Además de estos grupos y organizaciones, diversos organismos locales, estatales y nacionales publican especificaciones y requisitos que pueden afectar al tipo de cable utilizado en una LAN.

Los estándares son escritos y aprobados por comités formados por profesionales de la industria; éstos no son mandatarios y no tienen jurisdicción sobre los productos y sistemas que cubren y pueden adoptarse voluntariamente por las organizaciones de forma de hacer más atractivo el producto o servicio al usuario final.

A continuación se muestra una síntesis de los estándares y organizaciones que actualmente tienen mayor impacto en la industria de las telecomunicaciones en cuanto a los sistemas de cableado estructurado.

5.3.1 Estándar EIA/TIA-568B

Es el estándar para el cableado de telecomunicaciones de edificios comerciales, y se ha convertido en el estándar americano de la industria. Su objetivo es permitir el planeamiento e instalación de un sistema de cableado estructurado para edificios comerciales; especificando un sistema de cableado estructurado genérico que soporta un ambiente multiproducto y multifabricante. En otras palabras proveen una estructura común para el diseño e instalación de cables de telecomunicaciones y hardware de conectividad en los edificios comerciales.

EIA/TIA-568B define el cableado horizontal como un medio de networking que se extiende desde la toma para telecomunicaciones hasta el conector transversal horizontal. Este elemento incluye el medio de networking que se tiende a lo largo de un recorrido horizontal, la toma de telecomunicaciones, las terminaciones mecánicas en el armario para el cableado y los cables de conmutación o jumpers en el armario para el cableado. El cableado horizontal describe el medio de networking que se utiliza en el área que va desde el armario para el cableado hasta una estación de trabajo.

5.3.2 Estándar EIA/TIA-569A

Estándar sobre espacios y canalizaciones de telecomunicaciones para edificios comerciales. Su objetivo es estandarizar el diseño y las prácticas de construcción dentro y entre edificios que serán el soporte para los cables y equipos de telecomunicaciones.

Básicamente, cubre las canalizaciones (cómo los cables vinculan una estación de trabajo con otra) y espacios (las ubicaciones de los equipos de telecomunicaciones y las terminaciones) y cómo deberían ser diseñadas y utilizadas dentro de la infraestructura de telecomunicaciones.

Algunas de las secciones más importantes son:

- *Canalizaciones horizontales*: incluye lineamientos para el planeamiento e instalación de pisoducto, piso elevado, caños, bandejas, cable canal, cielo raso y canalizaciones perimetrales que puedan utilizarse para la distribución de los sistemas de cableado horizontal.

- *Canalizaciones para backbone*: incluye las canalizaciones dentro del edificio (*intrabuilding*) y entre edificios (*interbuilding*). El término backbone ha reemplazado al término raiser comúnmente usado en la industria telefónica en USA.

- *Area de trabajo*: trata lo relacionado a la canalización de sistemas de cables y la ubicación de puestos de trabajo.

- *Cuarto de telecomunicaciones, cuarto de equipos y entrada de facilidades:* cubre el diseño y objetivo de estos espacios incluyendo sus dimensiones, ubicación, canalizaciones, cargas de piso, cobertura de paredes, iluminación y alimentación.

5.3.4 Estándar EIA/TIA-606A

Estándar sobre administración para la infraestructura de telecomunicaciones de edificios comerciales.

Su objetivo es proveer un esquema de administración uniforme independiente de las aplicaciones y establecer lineamientos para los dueños, usuarios, fabricantes, consultores, contratistas, diseñadores e instaladores involucrados en la administración (y etiquetado) y en la infraestructura de telecomunicaciones. Esté estándar reconoce la importancia de una documentación adecuada para facilitar una administración precisa sobre el cableado instalado durante la vida útil del edificio, incluyendo cables, hardware de conexión, canalizaciones y espacios.

EIA/TIA-606A incluye:

- *Conceptos de administración:* define tres componentes principales que crean el concepto de administración: identificadores, vínculos y documentación.

- *La administración de canalizaciones y espacios, sistema de cableado y aterramiento*: especifica la forma en la cual éstos puntos son etiquetados y administrados.

- *Etiquetado y código de colores*: especifica los requerimientos de etiquetado en detalle y el código de colores como una forma de identificar más fácilmente el tipo de elemento de telecomunicaciones que se está observando solamente mirando la etiqueta.

5.3.5 Estándar EIA/TIA-607

Requerimientos de aterramiento y anclaje en edificios comerciales para la industria de telecomunicaciones.

Su objetivo es permitir el planeamiento, diseño e instalación del sistema de tierra para telecomunicaciones con o sin conocimiento previo del sistema de telecomunicaciones que se instalará. Esta infraestructura de tierra soporta un ambiente multifabricante y multiproducto, así como las prácticas de aterramiento de varios sistemas.

Entre otras funciones, discute el diseño y los componentes requeridos para proveer protección eléctrica a los usuarios y a la infraestructura de telecomunicaciones a través del uso de una configuración apropiada y un sistema de tierra correctamente instalado.

Este estándar no define los productos de aterramiento que deben usarse o los procedimientos para el montaje de equipos y hardware, para unir al Backbone de Tierra de Telecomunicaciones/Telecomunications Bonding Backbone (TBB). La información acerca de la protección eléctrica de los circuitos y los métodos de aterramiento y anclaje pueden encontrarse en el Código Eléctrico Nacional/National Electric Code (NEC) y en el Código de Seguridad Eléctrica y Nacional/National Electrical Safety Code (NESC).

Las LAN son redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña; éstas, permiten que las empresas que utilizan tecnología informática, compartan toda clase de dispositivos (equipos, impresoras, servidores, etc.) de manera eficiente para así unificar sus sistemas de comunicaciones, mejorar la seguridad y el control de la información.

Para ello, fue diseñado un modelo que se encarga de facilitar el proceso de traslado de información entre equipos a través de un medio de red, éste es el modelo de referencia OSI; un esquema de red descriptivo que asegura una mayor compatibilidad e interoperabilidad entre las distintas tecnologías de red.

El modelo de referencia OSI de divide en siete capas: capa de aplicación, que se encarga de los procesos de red hacia las aplicaciones; capa de presentación, encargada de la presentación de datos; capa de sesión, se encarga de la comunicación entre hosts; capa de transporte, se encarga de las conexiones extremo a extremo; capa de red, se encarga de los direccionamientos y mejor ruta, capa de enlace de datos, encargada del acceso a los medios y capa física, que se encarga de la transmisión binaria.

Ethernet o IEEE 802.3, es el estándar más popular para las LAN utilizado actualmente; emplea una topología lógica de bus y una topología física de estrella o de bus. Permite la transmisión de datos a través de la red a una velocidad de 10/100 Mbps, utiliza un método de transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones/Carrier Sense Multiple Access, Collision Detect (CSMA/CD).

La sociedad de nuestros días emplea la información para reducir los costos de producción de los bienes que consumimos, y en general para mejorar nuestra calidad de vida. Gracias a los sistemas de comunicaciones y a las redes de computadoras e Internet, hoy es posible el intercambio de información rápido y económico para familias, empresas y personas de todo el mundo. Básicamente, el empleo de redes confiere una gran flexibilidad a todo tipo de entornos ya que proveen accesibilidad de forma directa y también de forma remota.

Sánchez Allende, Jesús
REDES: INICIACION Y REFERENCIA
Editorial Mc Graw Hill; Madrid; 2000

Black Uyless D.
REDES DE COMPUTADORAS: PROTOCOLOS, NORMAS E INTERFACES
Editorial Ra Ma, España; 1990

Vito Amato
ACADEMIA DE NETWORKING DE NETWORKING DE CISCO SYSTEMS
Cisco Systems, Inc; 2000

Raya, José Luis ; Raya, Cristina
REDES LOCALES
Editorial Ra Ma, Madrid; 2001

Tanenbaum, Andrew S.
REDES DE ORDENADORES
Editorial Prentice Hall, New Jersey; 2000

Huidobro, José Manuel
SISTEMAS DE COMUNICACIONES
Editorial Paraninfo, Madrid; 1993

Huidobro; José Manuel
TODO SOBRE COMUNICACIONES
Editorial Paraninfo, Madrid; 1998

Raya; José Luis
REDES LOCALES Y TCP IP
Editorial Ra Ma, España; 2001

M. Schwartz
CABLEADO DE REDES
Editorial Paraninfo, Madrid; 1985

Abad Domingo, Alfredo
REDES DE AREA LOCAL
Editorial Mc Graw Hill, Madrid; 2005

González Sainz, Nestor
COMUNICACIONES Y REDES DE PROCESAMIENTO DE DATOS
Editorial Mc Graw Hill, Estados Unidos y Reino Unido; 1991