UNIVERSIDAD AUTONOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BASICAS E INGENIERIA

“REDES DE ALTA VELOCIDAD”

MONOGRAFIA

QUE PARA OBTENER EL TITULO DE
INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

PRESENTA:

RENE FLORES GUZMAN

ASESOR:

ING. SANDRA LUZ HERNANDEZ MENDOZA

PACHUCA HGO., OCTUBRE DE 2005

AGRADECIMIENTOS

Con respeto y admiración a mi padre por haberme apoyado en toda mi formación académica y por haber echo de mí una persona de bien; también a mí asesora Ing. Sandra Luz Hernández Mendoza por sus valiosas asesorias y que si su apoyo no habría sido posible esta monografía.

También a la Dirección General de Telecomunicaciones de la UAEH, en especial al LSC. David Rivero Borja encargado de monitoreo y operación de la red, por su tiempo y paciencia muchas gracias.

Además no podrían faltar la Dirección de Proyectos y Obras en especial al buen amigo Arq. Antonio Barrales Martínez por su apoyo incondicional en esta monografía.

A todos ellos GRACIAS

Índice

Figuras

Capítulo 1 Conceptos básicos Pág.

Capítulo 2 Tecnologías utilizadas en las redes de alta velocidad

Capitulo 3 Tendencias de protocolos de las redes de alta velocidad

Capítulo 4 Caso practico: red de alta velocidad de ciudad universitaria de la UAEH

Tablas

Capítulo 1 Conceptos básicos Pagina

Capítulo 3 Tendencias de Protocolos de las Redes de Alta Velocidad

Capítulo 4 Caso practico: red de alta velocidad de ciudad universitaria de la UAEH

Introducción

La gran importancia que tienen las redes de alta velocidad hoy en día, y la demanda de compartir recursos de una manera rápida y eficaz han provocado que existan nuevas tecnologías las cuales permiten transmitir grandes volúmenes de datos a altas velocidades y con una excelente calidad de servicio además de recibir información en cualquier momento y desde cualquier punto donde se encuentre el usuario.

Esta monografía hace referencia a las diferentes topologías que se encuentran en una red de alta velocidad, también se estudian sus componentes de interconexión como son switch, un router, etc., a su vez se describe los medios de transmisión existentes en un a red como la novedosa Fibra Óptica.

Las redes de alta velocidad han tenido cambios a través de los años, frente a la demanda excesiva de usuarios, esto ha provocado la evolución de nuevos y mejores protocolos de Internet.

Las nuevas tecnologías desarrolladas en las redes de alta velocidad son diversas y se adecuan a las necesidades propias de cada red, que hoy en día han respondido con eficiencia a la demanda de un mayor ancho de banda.

El caso de estudio muestra de una manera específica el funcionamiento de una red de alta velocidad relacionada con todos los componentes y tecnologías mencionados en este trabajo, a la vez se muestra un caso real en el ámbito laboral de nuestro perfil académico.

Justificación

Las instituciones privadas o públicas se basan en este tipo de redes para llevar a cabo sus operaciones ya sea de negocios o de investigación, es por esto que las redes de alta velocidad se han convertido en un medio de comunicación de primera necesidad, que en la actualidad han sido de gran importancia.

Sin embargo las instituciones buscan tecnologías que permitan un alto desempeño para el trato de su información que sea confiable y que se encuentre dentro de sus alcances económicos, además el gran avance tecnológico permite que estas instituciones tengan un panorama muy amplío y decidan cual es la que se adecua a sus necesidades de operación.

Es por ello la importancia de realizar la investigación de estas redes saber de una manera general y concisa el funcionamiento de una en un caso real, a pasar de que existen una gran variedad de tecnologías algunas son mas sofisticadas que otras y son preferidas por los ingenieros porque se adecuan mejor a las necesidades de transmisión.

Objetivo

Proveer información sobre los diferentes tipos de redes de alta velocidad así como también protocolos de nueva generación y dispositivos de redes que van desde el más mínimo hasta el mas sofisticado, además su utilización de estos en un caso práctico.

Objetivos específicos

- Conocer los diferentes tipos de redes además de los dispositivos de interconectividad de las redes.
- Identificar sobre nuevas tecnologías de protocolos que se han encontrado en evolución.
- Proveer de información detallada de las diferentes configuraciones de las redes en cuanto a cableado.
- Aplicar toda la información de las redes en un caso real su conexión, su administración etc.

Capítulo 1

Conceptos básicos

Reseña:

En este capítulo se mencionan los conceptos básicos de manera detallada de las Redes para la fácil comprensión del lector en los capítulos subsecuentes.

1.1 Concepto de Red

Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más computadoras. [1]

1.2 Objetivo de las redes

Su objetivo general consiste en hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a miles de kilómetros de distancia de los datos, no debe evitar que éste los pueda utilizar como si fueran originados localmente. [2]

1.3 Beneficios de las redes

Los beneficios de las redes son los siguientes:

- Las organizaciones modernas de hoy en día suelen estar dispersas geográficamente, y sus oficinas están situadas en diversos puntos de un país e incluso en diferentes lugares del mundo. Muchas computadoras y terminales de cada una de las localizaciones necesitan intercambiar información y datos, a menudo a diario. Las redes proporcionan la posibilidad de que dichas computadoras puedan intercambiar datos y hacer accesibles los programas y lo datos a todo el personal de la empresa.
- Las redes también pueden facilitar la función crítica de tolerancia ante fallos. En el caso de que un computador falle, otro puede asumir sus funciones y su carga. Esta posibilidad es de especial importancia por ejemplo, en sistemas dedicados al control del tráfico aéreo. En el caso de un fallo en loas computadoras otra pueden tomar el relevo y asumir el control de las operaciones.

- Enlazar en red sus computadoras, junto con sus impresoras, escáners, sistemas de almacenamiento y copias de seguridad, e incluso máquinas de fax y sistemas telefónicos, hace que sus usuarios puedan acceder más

fácilmente a todo este equipo. Al mismo tiempo, las redes le permiten planificar su inversión en software para obtener el máximo valor, ya que las versiones de red tienen un costo considerablemente menor por usuario que las compras individuales. La administración del software, en gran medida para garantizar que su empresa cumple las leyes sobre licencias, también se facilita. [3]

1.4 Clasificación de las Redes

Las posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las que se muestran en la siguiente tabla:

Extensión ó cobertura	**Topología**	**Conexión**	**Arquitectura**	**Medio de transmisión**	**Propiedad**
LAN MAN WAN GAN SAN	Bus Estrella Anillo Arbol	Punto a punto Difusión Conmutada	Arcnet Ethernet Token Ring Bus Pasing	Cableada Inalambrica	Publica Privada

Tabla 1.1 Clasificación de las redes

1.4.1 Clasificación de las redes según su extensión ó cobertura

LAN. Redes de área local (Local Área Network)

Son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo

velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).

MAN. Redes de área metropolitana (Metropolitana Área Network)

Son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.

WAN. Redes de área amplia (Wide Área Network)

Tienen un tamaño superior a una MAN, y consisten en una colección de servidores o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de ruteadores, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o el servidor adecuado, enviándose éstos de un ruteador a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros. Podemos ver Internet como la WAN suprema. [4]

SAN. (Red de área de almacenamiento)

Un sistema NAS o SAN puede ser individual o enlazarse en red, pero además del disco duro incluye el software específico de su función, que consiste fundamentalmente en distribuir los archivos al usuario. A NAS se le asigna una dirección IP, es decir, el número de identificación (en este caso, del dispositivo de almacenamiento) en la red, y se configura por medio de un programa navegador. Por su parte, SAN (siglas en inglés de Red de Área de Almacenamiento) es una subred de dispositivos de almacenamiento que están conectados entre sí por medio de conmutadores especiales, así como a un servidor o a un grupo de servidores que actúan como punto de acceso a la SAN.

Esta arquitectura permite, por ejemplo, hacer copias de seguridad de todos los datos de la red sin sobrecargarla, y pone los dispositivos de almacenamiento

incluso a medida que se van agregando a la red a la disposición de todos los servidores. Una SAN puede estar situada lejos de la ubicación de la red principal y conectada a ésta por medio de diferentes tecnologías de comunicación. [50]

GAN. (Red de área global)

Se trata de una red de tipo internacional que se extiende a todos los departamentos, oficinas y sucursales de una compañía. Las redes globales (global networks) presentan su propia serie de problemas, que incluyen los relacionados con los diferentes usos de horarios, idiomas, normas establecidas, así como las compañías internacionales u oficinas de teléfonos y telegrafía. Sin embargo, para los grandes consorcios y compañías de giro internacional el uso de estos sistemas implica comunicación a menor costo del que representaría trasladarse constantemente de un sucursal a otra, además de incrementar el tiempo de respuesta en cuanto a la toma de decisiones. [49]

1.4.2 Clasificación de las redes según la Topología

La topología de red es la forma en que se distribuyen los cables de la red para conectarse con el servidor y con cada una de las estaciones de trabajo; es similar a un plano de la red dibujado en el papel, ya que se pueden tender cables a cada nodo y servidor de la red.

Las principales modelos de topología son:

- Topología en anillo
- Topología en bus
- Topología en árbol
- Topología en estrella

1.4.2.1 Topología en anillo

El anillo consiste en una serie de repetidores conectados entre sí mediante un único enlace de transmisión unidireccional que configura un camino cerrado. La

información se transmite secuencialmente de un repetidor al siguiente a lo largo del anillo, de tal forma que cada repetidor regenera la señal que recibe y la retransmite al siguiente, salvo que la información esté dirigida a él, en cuyo caso la recibe en su memoria. Los repetidores constituyen un elemento activo de la red, siendo sus principales funciones las de contribuir al correcto funcionamiento del anillo ofreciendo todos los servicios necesarios y proporcionar el punto de acceso a las estaciones de la red. Normalmente los repetidores están integrados en las computadoras personales y en las estaciones de trabajo. Las redes en anillo permiten un control eficaz, debido a que, en cada momento, se puede conocer en qué trama está circulando la señal, puesto que se sabe la última estación por donde ha pasado y la primera a la que todavía no ha llegado. La desventaja fundamental es la falta de fiabilidad. Un fallo en el anillo inhabilitaría todas las estaciones. Ver figura 1.1

Figura 1.1 Topología en anillo [5]

1.4.2.2 Topología en bus

En esta topología todas las estaciones se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando una estación transmite, su señal se propaga a ambos lados del emisor, a través del bus, hacia todas las estaciones conectadas al mismo, por este motivo, al bus se le denomina también canal de difusión. La mayor parte de los elementos de las redes en bus tienen la ventaja de ser elementos pasivos, es decir, todos los componentes activos se encuentran en las estaciones por lo que una avería en una estación no afecta más que a ella misma. Por otra parte, un inconveniente de este tipo de

redes es que si falla el propio bus, queda afectada toda la red. Las principales ventajas que tiene esta topología son la modularidad, es decir, la facilidad de añadir y quitar estaciones. Entre las desventajas se puede citar el hecho de que varias estaciones quedan desconectadas al fallar un tramo del bus. Ver figura1.2.

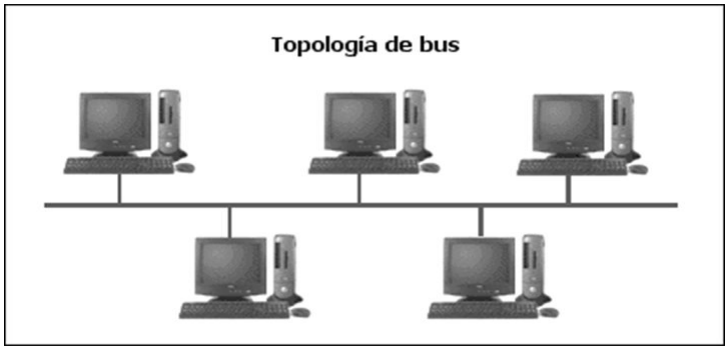


Figura 1.2 Topología en bus [5]

1.4.2.3 Topología en árbol

Es una variante de la topología en bus, consistente en un bus principal denominado tronco del que parten varios buses secundarios denominados ramas, cada una de las cuales es capaz de admitir varias estaciones. Al igual que en la topología en bus, las señales se propagan por cada ramal de la red y llegan a todas las estaciones. Además de las ventajas e inconvenientes de las redes en bus, la red en árbol tiene una mayor adaptabilidad al entorno físico donde se instala la red, con lo que el costo de cableado es aún menor. Ver figura 1.3.

Figura 1.3 Topología en árbol [5]

1.4.2.4Topología en estrella

En la topología en estrella todas las estaciones están conectadas mediante enlaces bidireccionales a una estación o nodo central que controla la red. Este nodo central asume las funciones de gestión y control de las comunicaciones proporcionando un camino entre cada dos estaciones que deseen comunicarse. La principal ventaja de la topología en estrella es que el acceso a la red, es decir, la decisión de cuando una estación puede o no transmitir, se halla bajo control de la estación central. Además la flexibilidad en cuanto a configuración, así como la localización y control de fallos es aceptable al estar todo el control en el nodo central. El gran inconveniente que tiene esta topología es que si falla el nodo central. Toda la red queda desactivada. Otros pequeños inconvenientes de este tipo de red son el costo de las uniones físicas puesto que cada estación está unida a la unidad central por una línea individual, y además, las velocidades de transmisión son relativamente bajas. Ver figura 1.4. [15]

Figura 1.4 Topología en estrella [5]

1.4.3 Clasificación de las redes según su conexión

1.4.3.1 Redes de difusión.

Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.

1.4.3.2 Redes punto a punto

Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos ruteadores. Ver figura 1.5 [5]

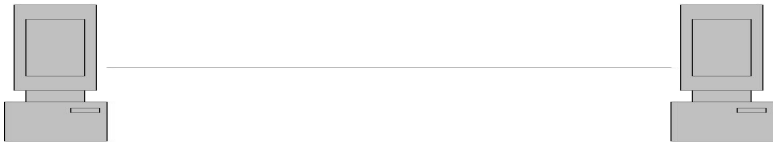


Figura 1.5 Redes punto a punto

1.4.3.3 Redes de conmutación

Cuando los datos hay que enviarlos a largas distancias (e incluso a no tan largas), generalmente deben pasar por varios nodos intermedios como se muestra en la figura 1.6. Estos nodos son los encargados de encauzar los datos para que lleguen a su destino. En estas redes, los datos que entren en las redes provenientes de alguna de las estaciones, son conmutados de nodo en nodo hasta que lleguen a su destino. [7]

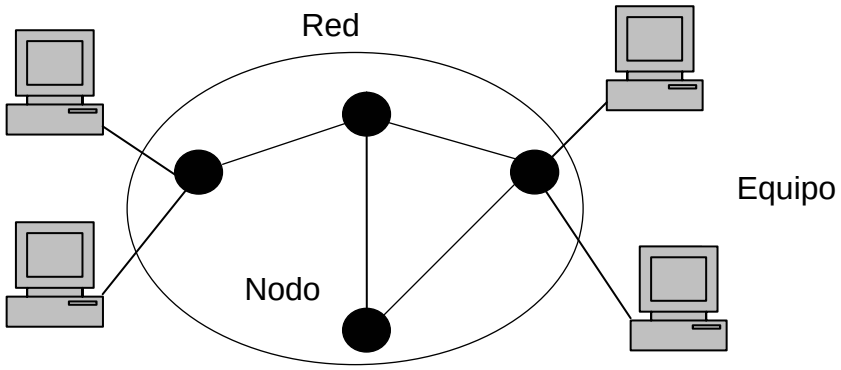


Figura 1.6 Redes de conmutación

A) Redes de conmutación de circuitos. La comunicación entre los equipos terminales de datos (*Data Terminal Equipment, DTE*) se establece empleando un camino fijo y dedicado a través de un canal físico de comunicación empleando conmutadores (*switches*). [8]

B) Redes de conmutación de mensajes. Un mensaje que se transmite por conmutación de mensajes va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. [9]

C) Redes de conmutación de paquetes

Estas redes utilizan la misma filosofía que las de conmutación de mensajes, salvo que el mensaje se fragmenta en paquetes para su transmisión.

En función del mecanismo de encaminamiento elegido para esos paquetes, se subdividen en dos tipos:

- **Técnica de datagramas:** cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control (por ejemplo número de paquete, nombre, dirección de destino, etc.) y lo envía hacia su destino. Puede ocurrir que por haber tomado caminos diferentes, un paquete con número por ejemplo 6 llegue a su destino antes que el número 5. También puede ocurrir que se pierda el paquete número 4. Todo esto no lo sabe ni puede controlar el emisor , por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido (para su posible reclamación al emisor) , y para esto , debe tener el software necesario.
- **Técnica de circuitos virtuales :** antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de Petición de Llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos . De esta forma se establece un camino virtual para todo el grupo de paquetes. Este camino virtual será numerado o nombrado inicialmente en el

emisor y será el paquete inicial de Petición de Llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número. De esta forma, el encaminamiento sólo se hace una vez (para la Petición de Llamada). El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez. [6]

1.4.4 Clasificación según su arquitectura

1.4.4.1 ArcNet

Utiliza un método de acceso de paso de testigo en una topología de bus en estrella con una tasa de transmisión de 2,5 Mbps. ArcNet Plus, una sucesora de la ArcNet original, permite una tasa de transmisión de 20 Mbps. Debido a que ArcNet es una arquitectura de paso de testigo, para que un equipo en una red ArcNet pueda transmitir datos tiene que tener el testigo. El testigo se mueve de un equipo a otro de acuerdo con el orden en que estén conectados en el concentrador, independientemente de cómo estén situados físicamente. Esto significa que el testigo se mueve en orden del equipo 1 al equipo 2 (en las conexiones del hub), aunque el equipo 1 esté en un extremo del edificio y el equipo esté en el otro extremo del edificio.

1.4.4.2 Ethernet

Es la arquitectura de red más popular. Esta arquitectura de banda base utiliza una topología en bus, normalmente transmite a 10 Mbps y utiliza CSMA/CD para regular el segmento de cable principal.

El medio Ethernet es pasivo, lo que significa que no requiere una fuente de alimentación, por lo que no fallará a no ser que el medio esté cortado físicamente o no esté terminado correctamente.

1.4.4.3 Token Ring.

Cuando el primer equipo de Token Ring entra en línea, la red genera un testigo (estructura de datos tipo etiqueta). El anillo es una formación de bits predeterminada (una serie de datos) que permite a un equipo colocar datos en los cables. El testigo viaja a través de la red preguntando a cada equipo hasta que un equipo indica que quiere transmitir datos y se apodera del testigo y ningún equipo puede transmitir hasta que no tome el control del testigo.

Una vez que un equipo se apodera del testigo, envía una trama de datos a través de la red. La trama viaja por la red hasta que alcanza el equipo con una dirección que coincida con la dirección de destino de la trama. El equipo de destino copia la trama en su búfer de recepción y marca la trama en el campo de estado de la trama para indicar que se ha recibido la información.

La trama continúa por el anillo hasta que llegue al equipo que la envió, de forma que se valida la transmisión. A continuación, el equipo que envía retira la trama del anillo y transmite un testigo nuevo a éste.

En la red sólo puede haber un testigo activo y el testigo puede viajar sólo en una dirección del anillo.

El paso de testigos es determinante, lo que significa que un equipo no puede imponer su turno en la red, tal y como ocurre en un entorno CSMA/CD. Si el testigo está disponible, el equipo puede utilizarlo para enviar datos. Cada equipo actúa como un repetidor unidireccional, regenera el testigo y lo continúa pasando.

1.4.4.4 Token Bus (IEEE* 802.4)

Es una red en bus que utiliza un esquema de paso de testigo. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un testigo que viaja por la red determina quién es el equipo que tiene que informar. [10]

1.4.5 Clasificación según el medio de transmisión

1.4.5.1 Redes Inalámbricas

Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

1.4.5.2 Red cableada

Las redes cableadas son redes cuyos medios físicos son cables como cable coaxial y par trenzado. [5]

1.4.6 Clasificación según la propiedad

1.4.6.1 Redes públicas,

Aquellas cuyo moderador o gestor es un organismo o entidad pública, o aquellas cuya utilización está abierta a un público general.

1.4.6.2 Redes privadas

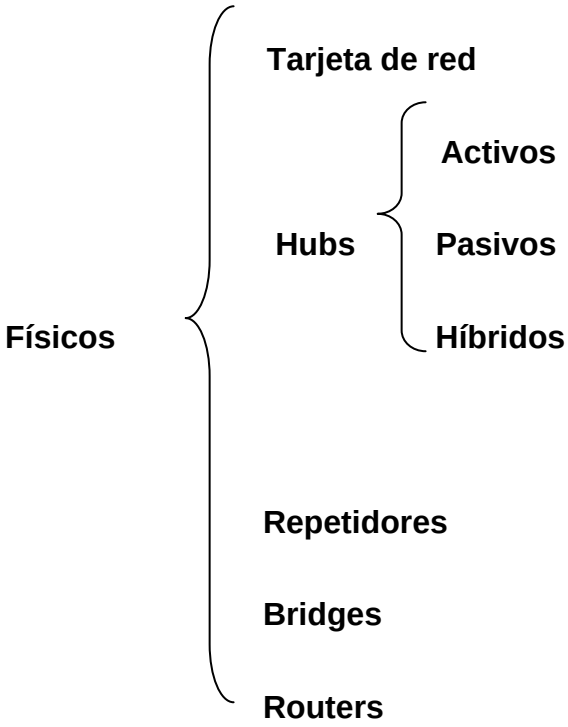
Aquellas cuyo moderador o gestor es una entidad corporativa y la emplea para fines propios. [8]

1.5 Componentes de las Redes

1.5.1 Lógicos

Lógicos (Software) — **Sistema Operativo***, **Software de Red***

1.5.2 Físicos



Los dispositivos utilizados para extender las LAN incluyen repetidores, puentes (bridges), ruteador (routers), y gateways (pasarelas). [13]

1.5.2.1 Tarjetas o placas de red

Se ha de conectar en una ranura del ordenador, dependiendo de cual sea la arquitectura así corresponderá un tipo de placa u otra, generalmente NIC (Network Interfece Card), o incluso PCMCIA (Personal Computer Memory Card International Association) para ordenadores portátiles, y es el dispositivo que hará de interfaz entre el equipo y la red. Teniendo en cuenta el cable a utilizar así llevará unas u otras conexiones, o en forma de T para coaxiales o de pinza muy similar a las de los teléfonos para los RJ 45, siendo lo normal que se incluyan ambas en la misma placa con independencia de que se utilice una u otra. [14]

1.5.2.2 Concentrador (Hub)

Es el componente hardware central de una topología en estrella. Además, se pueden utilizar para extender el tamaño de una LAN. Aunque la utilización de un concentrador no implica convertir una LAN en una WAN, la conexión o incorporación de concentrador a una LAN puede incrementar, de forma positiva, el número de estaciones. Este método de expansión de una LAN es bastante popular, pero supone muchas limitaciones de diseño. (Ver Figura 1.7)

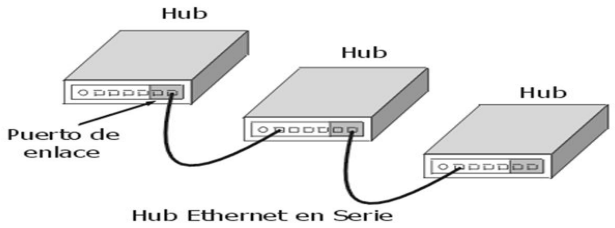


Figura1.7 Concentrador Ethernet en Serie [1]

Tipos

- **Activos.** La mayoría son activos; es decir, regeneran y retransmiten las señales del mismo modo que un repetidor. Como generalmente estos tienen de ocho a doce puertos para conexión de equipos de la red, a menudo se les llama repetidores multipuesto y requieren corriente eléctrica para su funcionamiento.
- **Pasivos**. Algunos son pasivos; como ejemplos están los paneles de conexión o los bloques de conexión (punch-down blocks). Actúan como puntos de conexión y no amplifican o regeneran la señal; la señal pasa a través del el y no necesitan corriente eléctrica para funcionar.
- **Híbridos.** Los híbridos, más avanzados que permiten conectar distintos tipos de cables.

1.5.2.3 Repetidores

Un repetidor funciona en el nivel físico del modelo de referencia OSI para regenerar las señales de la red y reenviarla a otros segmentos. El repetidor toma una señal débil de un segmento, la regenera y la pasa al siguiente segmento. Para

pasar los datos de un segmento a otro a través del repetidor, deben ser idénticos en cada segmento los paquetes y los protocolos Control lógico de enlace (LLC; Logical Link Control*).* (Ver Figura 1.8)

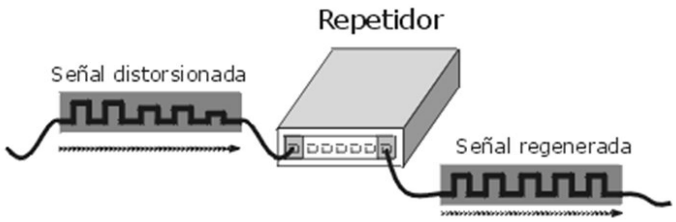


Figura 1.8 Funcionamiento de Repetidor [1]

Los repetidores no traducen o filtran señales. Un repetidor funciona cuando los segmentos que unen el repetidor utilizan el mismo método de acceso. Los dos métodos de acceso más habituales son acceso múltiple por detección de portadora con detección de colisión (CSMA/CD) y paso de testigo. Un repetidor no puede conectar un segmento que utiliza CSMA/CD con un segmento que utiliza el método de acceso por paso de testigo. Es decir, un repetidor no puede traducir un paquete Ethernet en un paquete Token Ring. Los repetidores pueden desplazar paquetes de un tipo de medio físico a otro. Pueden coger un paquete Ethernet que llega de un segmento con cable coaxial fino y pasarlo a un segmento de fibra óptica. Por tanto, el repetidor es capaz de aceptar las conexiones físicas.

1.5.2.4 Puentes (Bridges)

Trabajan a nivel de enlace de datos del modelo de referencia OSI y, por tanto, toda la información de los niveles superiores no está disponible para ellos. Más que distinguir entre un protocolo y otro, los puentes pasan todos los protocolos que aparecen en la red. Todos los protocolos se pasan a través de estos, de forma que aparecen en los equipos personales para determinar los protocolos que pueden reconocer.

Un puente funciona considerando que cada nodo de la red tiene su propia dirección. Además reenvía paquetes en función de la dirección del nodo destino.

Realmente, tienen algún grado de inteligencia puesto que aprenden a dónde enviar los datos. Cuando el tráfico pasa a través de el, la información sobre las direcciones de los equipos se almacenan en la RAM de este. Utiliza esta RAM para generar una tabla de encaminamiento en función de las direcciones de origen. (Ver Figura1.9)

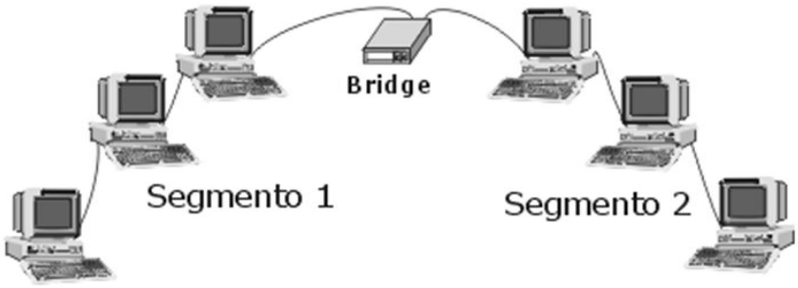


Figura1.9 Funcionamiento de un puente [1]

1.5.2.5 Ruteador (routers)

En un entorno que está formado por diferentes segmentos de red con distintos protocolos y arquitecturas, el puente podría resultar inadecuado para asegurar una comunicación rápida entre todos los segmentos. Una red de esta complejidad necesita un dispositivo que no sólo conozca la dirección de cada segmento, sino también, que sea capaz de determinar el camino más rápido para el envío de datos y filtrado del tráfico de difusión en el segmento local. Este dispositivo se conoce como ruteador.

Los ruteadores trabajan en el nivel de red del modelo de referencia OSI. Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Estos leen en el paquete la información de direccionamiento de

las redes complejas teniendo acceso a información adicional, puesto que trabajan a un nivel superior del modelo OSI en comparación con los puentes.

Los ruteadores pueden proporcionar las siguientes funciones de un bridge:

- Filtrado y aislamiento del tráfico.
- Conexión de segmentos de red.

Funcionamiento de los ruteadores

Los ruteadores mantienen sus propias tablas de encaminamiento, normalmente constituidas por direcciones de red; también se pueden incluir las direcciones de los hosts si la arquitectura de red lo requiere. Para determinar la dirección de destino de los datos de llegada, las tablas de encaminamiento incluyen:

- Todas las direcciones de red conocidas.
- Instrucciones para la conexión con otras redes.
- Los posibles caminos entre los ruteadores.
- El costo de enviar los datos a través de estos caminos.

Los ruteadores requieren direcciones específicas. Entienden sólo los números de red que les permiten comunicarse con otros ruteadores y direcciones NIC locales. Los ruteadores no conversan con equipos remotos.

Cuando los ruteadores reciben paquetes destinados a una red remota, los envían al ruteadores que gestiona la red de destino. En algunas ocasiones esto constituye una ventaja porque significa que los ruteadores pueden:

- Segmentar grandes redes en otras más pequeñas.
- Actuar como barrera de seguridad entre los diferentes segmentos. [10]

1.6 Medios de transmisión

El medio de transmisión, es el sistema físico por el que viaja la información transmitida (datos, voz y videos) a través de dos o mas puntos distantes entre si.

La tabla muestra la clasificación de los medios de transmisión:

Medios Guiados	Medios No Guiados
Cable par tranzado (UTP, STP)	Microondas
Fibra Óptica	Satélite
Cable Coaxial	Infrarrojos

Tabla 1.2 Clasificación de los medios de transmisión

1.6.1 Medios de transmisión guiados

Incluye alambre de metal (cobre, aluminio y otros) y cable de fibra óptica. El cable es normalmente instalado sobre los edificios o en conducit oculto. Los alambres de metal incluyen cable par trenzado y cable coaxial, donde el cobre es el material de transmisión preferido para la construcción de redes. La fibra óptica se encuentra disponible en filamentos sencillos o múltiples y en fibra de vidrio o plástico.

En el siguiente segmento se definen los diferentes medios guiados que existen:

1.6.1.1 Cable par trenzado

El cable de par trenzado consiste en un núcleo de hilos de cobre rodeados por un aislante, los cuales se encuentran trenzados por pares, de forma que cada par forma un circuito que puede transmitir datos. Un cable consta de un haz de uno o más pares trenzados rodeados por un aislante. [15]

Existen dos tipos de cable par trenzado:

- **STP** (Shielded Twister Pair/ Par Trenzado Blindado)

  En este tipo de cable, cada par va recubierto por una malla conductora que actúa de recubrimiento frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm.

El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más instalación. La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ 49.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

- **UTP** (Unshielded Twister Pair/ Par Trenzado sin Blindar)

El cable par trenzado más simple y empleado, sin ningún tipo de pantalla adicional y con una impedancia característica de 100 Ohmios. El conector más frecuente con el UTP es el RJ45, aunque también puede usarse otro (RJ11, DB25, DB11, etc.), dependiendo del adaptador de red.

Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesibilidad y fácil instalación. Sus dos alambres de cobre torcidos aislados con plástico PVC han demostrado un buen desempeño en las aplicaciones de hoy. Sin embargo, a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente. [14]

1.6.1.2 Fibra óptica

Las fibras ópticas son filamentos de vidrio de alta pureza, extremadamente compactos y flexibles (de 2 a 125 micrones); la fibra óptica es un conductor óptico de forma cilíndrica que consta del núcleo, un recubrimiento que tiene propiedades ópticas diferentes a las. Del núcleo y la cubierta exterior que absorbe los rayos ópticos, protege al conductor del medio ambiente y proporciona resistencia mecánica. En la figura 1.4 e ilustra físicamente lo que se conoce como fibra óptica.

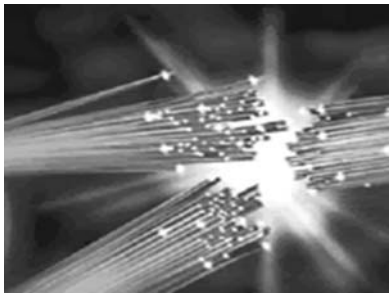


Figura 1.10 Fibra Óptica

La fibra óptica es fabricada a alta temperatura con base en silicio; su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones. Entre sus principales características se puede mencionar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad debido a que son inmunes a las interferencias electromagnéticas de radio-frecuencia.

Las fibras ópticas no conducen señales eléctricas, por lo tanto, son ideales para incorporarse en cables sin ningún componente conductivo, y pueden usarse en condiciones peligrosas de alta tensión. Tienen la capacidad de tolerar altas diferencias de potencial sin ningún circuito adicional de protección, y no hay problemas debido a los cortos circuitos..

Tienen un gran ancho de banda que puede ser utilizado para incrementar la capacidad de transmisión, con el fin de reducir el costo por canal. De ésta forma, es considerable el ahorro en volumen con relación a los cables de cobre.

Con un cable de seis fibras, se puede transportar la señal de más de cinco mil canales o líneas principales, mientras que se requiere de 10,000 pares de cable de cobre convencional para brindar servicio a ése mismo número de usuarios, con la desventaja que éste último medio ocupa un gran espacio en los ductos, y requiere de grandes volúmenes de material, lo que también eleva los costos.

Comparado con el sistema convencional de cables de cobre, donde la atenuación

de sus señales (decremento o reducción de la onda o frecuencia) es de tal magnitud, que requieren de repetidores cada dos kilómetros para regenerar la transmisión. En el sistema de fibra óptica se pueden instalar tramos de hasta 70 km, sin que halla necesidad de recurrir a repetidores, lo que también hace. Más económico y de fácil mantenimiento éste material.

En un sistema de transmisión por fibra óptica, existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o luminosa, por ello se le considera el componente activo de este proceso. Una vez que es transmitida la señal luminosa por las minúsculas fibras, en otro. Extremo del circuito se encuentra un tercer componente al que se le denomina detector óptico o receptor, cuya misión consiste en transformar .la señal luminosa en energía electromagnética, similar a la señal original.

El sistema básico de transmisión se compone en éste orden: señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo) empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida.

Ventajas importantes frente a los tradicionales cables eléctricos tales como:

- Mayor velocidad de transmisión: las señales recorren los cables de fibra óptica a la velocidad de la luz (c = 3x10^9 m/s*),* mientras que las señales eléctricas recorren los cables al 50% u 80% de esta velocidad, según el tipo de cable.
- Mayor capacidad de transmisión: pueden lograrse velocidades de varios Gbps a decenas de Km sin necesidad de repetidor. Cuanto mayor sea la longitud, de onda, mayor será la distancia y la velocidad de transmisión que podremos tener, reduciendo de éste modo la atenuación.
- Inmunidad total: frente a las interferencias electromagnéticas (incluidos los pulsos electromagnéticos nucleares resultado de explosiones nucleares).
- Se consiguen tasas de error mucho menores que en coaxiales, lo que permite aumentar la velocidad eficaz de transmisión de datos al reducir el

número de retransmisiones o cantidad de información redundante necesaria para detectar y corregir los errores de transmisión.

- Permite mayor distancia entre repetidores.
- Presenta una seguridad alta.
- Apropiados para una alta gama de temperaturas.
- Mayor resistencia a ambientes y líquidos corrosivos que los cables eléctricos.

Características técnicas de la fibra óptica

La fibra es un medio de transmisión de información analógica ó digital. [5]

La capacidad de transmisión de información que tiene una fibra óptica, depende. de tres características fundamentales:

- Del diseño geométrico de la fibra.
- De las propiedades de los materiales empleados en su elaboración (diseño óptico).
- De la anchura espectral' de la fuente de luz utilizada. Cuanto mayor sea esta anchura, menor será la capacidad de transmisión de información de esa fibra.

En función de cómo sea el cambio del valor del índice de refracción, las fibras se dividen en:

- Fibras ópticas de índice escalar *(stepped-index),* donde el cambio es muy abrupto.
- Fibras ópticas de modo gradual *(graded-index* o *gradex),* que experimentan un cambio gradual parabólico.

Se distinguen tres tipos de transmisión en la fibra óptica: monomodo, mu/timodo de índice gradual y multimodo de índice escalar.

En la propagación *monomodo,* la luz recorre una trayectoria única en el interior del

núcleo, proporcionando un gran ancho de banda. Para minimizar el número de reflexiones en la superficie entre el núcleo y el recubrimiento, el núcleo debe ser lo más estrecho posible, haciendo que su fabricación sea muy complicada. Debido a esto, surgieron las fibras *multimodo,* cuyo diámetro es mucho mayor. También es mayor el número de trayectorias de la luz resultantes de las distintas reflexiones, y esto da lugar a una dispersión de los componentes, disminuyendo la velocidad de propagación.

Tipos de fibra óptica

Hay tres tipos de fibras ópticas:

1.- Fibras monomodo de índice escalar: tienen un diámetro de entre 1 y 10 µm y un recubrimiento de 125 µm de diámetro. La dispersión es baja y se consiguen anchos de banda de varios GHz/Km. Se utiliza para redes *Backbone* (redes troncales). En la figura 1.5 se muestra como se propaga el haz de luz dentro de la fibra.

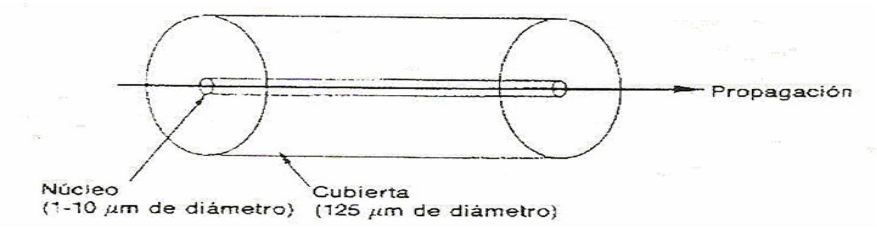


Figura 1.11 Propagación de luz en monomodo

2.- Fibras multimodo de índice escalar: el diámetro del núcleo está entre los 50 y los 60 µm, pero puede llegar a los 200 µm El diámetro del recubrimiento suele acercarse al tamaño estándar de los 125 µm; la dispersión es elevada. Sus aplicaciones se limitan a la transmisión de datos a baja velocidad o cables industriales de control. Ver la figura 1.6 que ilustra las trayectorias por las que viaja el haz de luz.

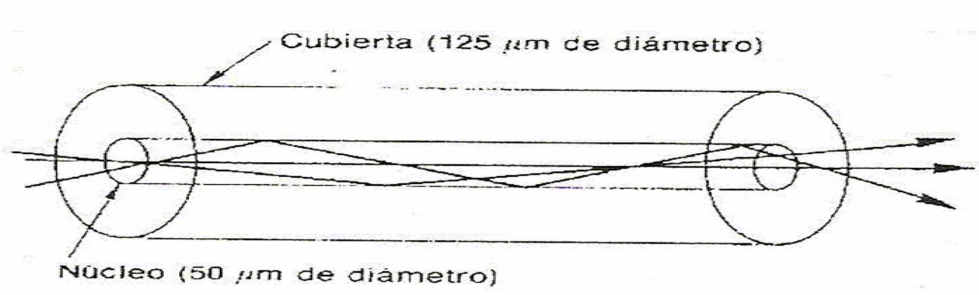


Figura 1.12 Fibras multimodo de índice escalar

3.- Fibras multimodo de índice gradual: el diámetro del núcleo está entre los 50 y los 60 µm, y el del recubrimiento es de 125 µm. Aunque existen muchos modos de propagación, la velocidad es mayor que en las fibras multimodo de índice escalar, reduciéndose así su dispersión, tal como se aprecia en la figura 1.7.

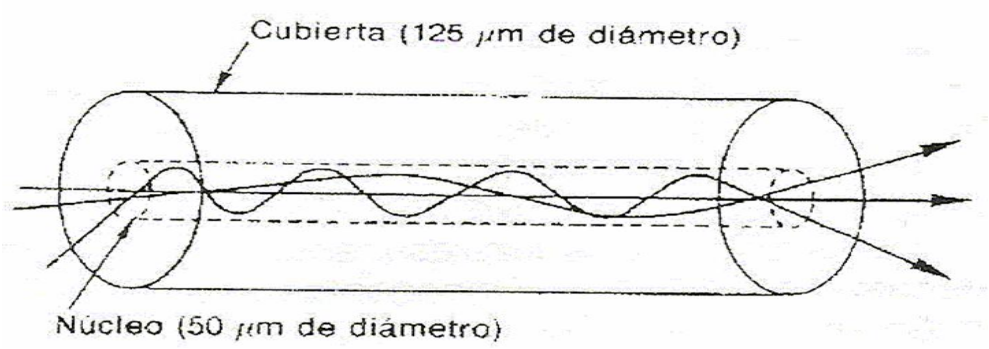


Figura 1.13 Fibras multimodo de índice gradual

Como transmisores (fuentes de luz), se emplean *diodos LEO* ó *diodos LASER* (éstos últimos se emplean para largas distancias y alta velocidad).

Destacan las siguientes aplicaciones:

- Transmisión a larga distancia. En telefonía, una fibra puede contener 60,000 canales.
- Transmisión metropolitana, para enlaces cortos de entornos de 10 Km sin necesidad de repetidores, y con capacidad de unas 100,000 conversaciones por cada fibra.
- Acceso a áreas rurales. Se usan para una longitud de 50 a 150 Km, con un

transporte del orden de 5,000 conversaciones por fibra. J!g Bucles de abonado.

- Redes de área local (LANs) de alta velocidad.

Características mecánicas de la fibra óptica

La fibra óptica, como elemento resistente dispuesto en el interior de un cable formado por agregación de varias de ellas, no tiene características adecuadas de tracción que permitan su utilización directa. Por otra parte, en la mayoría de los casos las instalaciones se encuentran a la intemperie o en ambientes agresivos que pueden afectar al núcleo.

La investigación sobre componentes optoelectrónicos y fibras ópticas, han traído consigo un sensible aumento de la calidad de funcionamiento de los sistemas. Es necesario disponer de cubiertas y protecciones de calidad capaces de proteger a la fibra. Para alcanzar tal objetivo, hay que tener en cuenta su sensibilidad a la curvatura y microcurvatura, la resistencia mecánica y las características de envejecimiento.

Las microcurvaturas y tensiones se determinan por medio de los ensayos de:

- **Tensión:** cuando se estira o contrae el cable se pueden causar fuerzas que rebasen el porcentaje de elasticidad de la fibra óptica y se rompa o formen microcurvaturas.
- **Compresión:** es el esfuerzo transversal
- **Impacto:** se debe principalmente a las protecciones del cable óptico.
- **Enrollamiento:** existe siempre un límite para el ángulo de curvatura, pero la existencia del forro impide que se sobrepase.
- **Torsión:** es el esfuerzo lateral y de tracción.
- **Limitaciones Térmicas**: estas limitaciones difieren en alto grado según se trate de fibras realizadas a partir del vidrio ó a partir de materiales sintéticos. [45]

1.6.1.3 Cable coaxial

El cable coaxial consta de un núcleo de cobre sólido rodeado por un aislante, una especie de combinación entre pantalla y cable de tierra y un revestimiento protector exterior. En el pasado, el cable coaxial permitió una transmisión más alta (10 Mbps) que el cable de par trenzado, aunque las recientes técnicas de transmisión sobre par trenzado igualan e incluso superan la velocidad de transmisión por cable coaxial. Sin embargo, los cables coaxiales pueden conectar los dispositivos de la red a distancias más largas que los de par trenzado. A pesar de ser el cable coaxial el medio tradicional de transmisión en redes basadas en Ethernet y ARCNET, la utilización de par trenzado y fibra óptica ya es muy común hoy en día sobre este tipo de redes. (Ver figura. 1.6). [15]

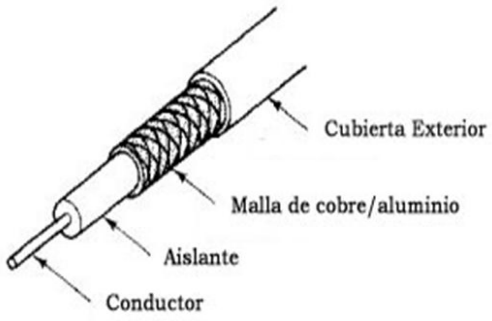


Figura 1.14 Cable Coaxial

Dependiendo del grosor tenemos:

- **Cable coaxial delgado (Thin coaxial):**

  El RG-58 es un cable coaxial delgado: a este tipo de cable se le denomina delgado porque es menos grueso que el otro tipo de cable coaxial, debido a esto es menos rígido que el otro tipo, y es más fácil de instalar.

- **Cable coaxial grueso (Thick coaxial):**

  Los RG8 y RG11 son cables coaxiales gruesos: estos cables coaxiales permiten una transmisión de datos de mucha distancia sin debilitarse la

señal, pero el problema es que, un metro de cable coaxial grueso pesa hasta medio kilogramo, y no puede doblarse fácilmente. Un enlace de coaxial grueso puede ser hasta 3 veces mas largo que un coaxial delgado. [14]

1.6.2 Medios De transmisión no guiados

Se refiere a las técnicas de transmisión de señales en el aire o espacio de transmisor a receptor. En esta categoría se encuentra microondas terrestre, satélites y el infrarrojo. [16]

1.6.2.1 Microondas terrestre.

Los sistemas de microondas terrestres han abierto una puerta a los problemas de transmisión de datos, sin importar cuales sean, aunque sus aplicaciones no estén restringidas a este campo solamente. Las microondas están definidas como un tipo de onda electromagnética situada en el intervalo del milímetro al metro y cuya propagación puede efectuarse por el interior de tubos metálicos. Es en si una onda de corta longitud.

Tiene como características que su ancho de banda varia entre 300 a 3.000 Mhz, aunque con algunos canales de banda superior, entre 3´5 Ghz y 26 Ghz. Es usado como enlace entre una empresa y un centro que funcione como centro de conmutación del operador, o como un enlace entre redes LAN. Para la comunicación de microondas terrestres se deben usar antenas parabólicas, las cuales deben estar alineadas o tener visión directa entre ellas, además entre mayor sea la altura mayor el alcance, sus problemas se dan perdidas de datos por atenuación e interferencias, y es muy sensible a las malas condiciones atmosféricas.

1.6.2.2 Satélites.

Conocidas como microondas por satélite, esta basado en la comunicación llevada a cabo a través de estos dispositivos, los cuales después de ser lanzados de la

tierra y ubicarse en la orbita terrestre siguiendo las leyes descubiertas por Kepler, realizan la transmisión de todo tipo de datos, imágenes, etc., según el fin con que se han creado. Las microondas por satélite manejan un ancho de banda entre los 3 y los 30 Ghz, y son usados para sistemas de televisión, transmisión telefónica a larga distancia y punto a punto y redes privadas punto a punto.

Las microondas por satélite, o mejor, el satélite en si no procesan información sino que actúa como un repetidor-amplificador y puede cubrir un amplio espacio de espectro terrestre. [17]

1.6.2.3 Infrarrojos

Los emisores y receptores de infrarrojos deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes . En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos (paredes por ejemplo). Tampoco es necesario permiso para su utilización (en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso). [18]

1.7 El modelo OSI

La arquitectura del modelo de referencia OSI divide la comunicación en red en siete niveles. Cada nivel cubre diferentes actividades, equipos o protocolos de red. El modelo OSI define cómo se comunica y trabaja cada nivel con los niveles inmediatamente superior e inferior. Por ejemplo, el nivel de sesión se comunica y trabaja con los niveles de presentación y de transporte.

Cada nivel proporciona algún servicio o acción que prepara los datos para entregarlos a través de la red a otro equipo. Los niveles inferiores (1 y 2) definen el medio físico de la red y las tareas relacionadas, como la colocación de los bits de datos sobre las placas de red (NIC, *Network Interface Cards*) y el cable. Los niveles superiores definen la forma en que las aplicaciones acceden a los servicios de comunicación. Cuanto más alto es el nivel, más compleja es su tarea.

Los niveles están separados entre sí por fronteras llamadas interfaces*. Todas las demandas se pasan desde un nivel, a través de esta interfaz, hacia el siguiente. Cada nivel se basa en los estándares y actividades del nivel inferior.

1.7.1 Definición de los 7 niveles de modelo OSI

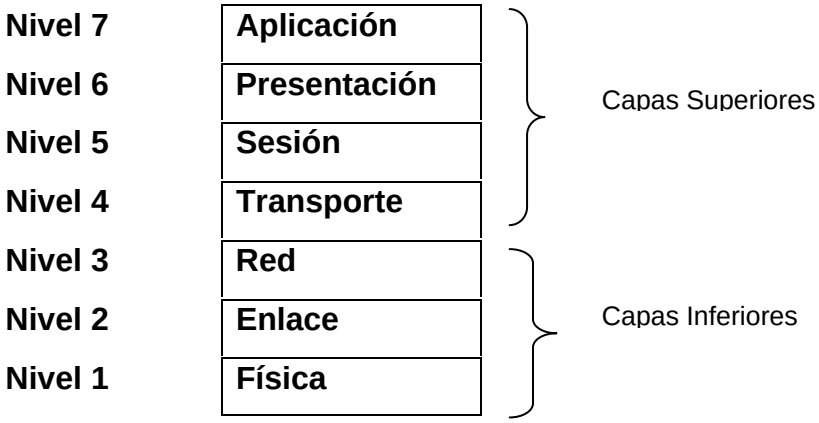


Tabla 1.3 Modelo OSI

Las capas de OSI:

Nivel 1 Capa física : se encarga de pasar bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

Nivel 2 Capa de enlace de datos: esta capa debe de encargarse de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.

Nivel 3 Capa de red: esta capa se encarga de enlazar con la red y encaminar los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos. Esta y las dos capas inferiores son las encargadas de todo el proceso externo al propio sistema y que están tanto en terminales como en enlaces o repetidores.

Nivel 4 Capa de transporte : esta capa se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos o circuitos virtuales) o no orientado a conexión (datagramas*).

Nivel 5 Capa de sesión: se encarga de proporcional diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones . Puede agrupar datos de diversas aplicaciones para enviarlos juntos o incluso detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.

Nivel 6 Capa de presentación: esta capa se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación.

Nivel 7 Capa de aplicación: esta capa acoge a todas las aplicaciones que requieren la red. Permite que varias aplicaciones compartan la red. [19]

1.8 Técnicas de Acceso al medio

Las técnicas de acceso al medio se describen, son empleadas en cada nodo para determinar de qué forma llevaran a cabo el acceso al medio.

1.8.1 Técnicas de contienda con escucha (CSMA)

Con esta técnica de acceso al medio, la transmisión esta condicionada al estado del canal o lo que es lo mismo, las estaciones tienen capacidad para escuchar ó determinar si el canal esta libre u ocupado.

Ahora, si la estación tiene datos que trasmitir y cree que el canal esta libre, comienza la transmisión, y si esta ocupado, espera hasta que se libere. En esta nueva situación, las colisiones se producirán cuando la estación crea que el canal esta libre cuando realmente no lo esta.

Dentro del protocolo CSMA, existen variantes que a continuación se presentan.

- **CSMA 1-persistente.** Si el canal esta ocupado, monitorizan el canal constantemente y esperan hasta que un instante libre en l que no se transmita para enviar sustraes. De esta manera, las colisiones ocurren cuando dos estaciones distintas quieren transmitir y el canal esta ocupado.

- **CSMA no persistente**. La estación no escucha constantemente el medio para evitar el problema anterior, ahora se espera un tiempo aleatorio para volver a mirar al canal. El inconveniente que se presenta, es que la última terminal en llegar sea la que trasmita primero (efecto LIFO).

- **CSMA p-persistente**. Para retrasar tanto el acceso al medio de una terminal (que es lo que ocurre en CSMA no persistente9, se propone la siguiente solución: enviar los datos con una probabilidad p si el canal esta libre, y esperar un tiempo t para volver a mirar al canal con una probabilidad 1-p.

1.8.2 Técnicas de contienda con escucha y detección de colisiones (CSMA/CD)

Es otra variante de CSMA capaz de detectar colisiones, esto es, que cuando se produce la colisión, la terminal deja de trasmitir deja de trasmitir la trama y no espera a que se acabe de enviar esta como ocurre en CSMA, y es asi como libera el canal lo antes posible. Posteriormente, se espera un tiempo aleatorio antes de volver as transmitir. Hay que tener en cuenta que ahora aparecerá en el bus fragmentos de colisión. [21]

Capitulo 2

Tecnologías utilizadas en las redes de alta velocidad

Reseña:

La finalidad de este capítulo es analizar las tecnologías para incrementar el ancho de banda en este capitulo se describen algunas de ellas tales como ATM, Fast Ethernet, FDDI, Frame Relay, Gigabit Ethernet entre otras

Las redes de alta velocidad, son redes digitales que utilizan tecnologías como Frame Relay, ATM, Ethernet, Gigabit Ethernet entre otras que se utilizan la tecnología de fibra óptica, por lo que ofrecen altas velo ciudades de conexión y transmisión de datos.

Las tecnologías de alta velocidad han reemplazado los paquetes por "**células".** Estas contienen una cantidad fija de datos formateados los cuales se transmiten a velocidades que van desde 155 Mbps, Hasta velocidades por encima de 1 Gbps, a diferencia de los datos formateados en un paquete que pueden alcanzar velocidades de transmisión que oscilan entre 1 y 100 Mbps, dependiendo del diseño de la red.

2.1 ATM (Modo de Transferencia Asíncrono)

ATM (Asynchronous Tranfer Mode / Modo de Transferencia Asíncrono), es una tecnología de conmutación orientada a conexión para redes locales y de largo alcance (LANs y WANs). ATM provee la capacidad de enviar audio, video, imágenes y datos sobre la misma red en aplicaciones tales como: multimedia y teleconferencía. [26]

ATM ha sido definida tanto por el ANSI como por el CCITT a través de sus respectivos comités ANSI T1, UIT SG XVIII como tecnología de transporte para la B-ISDN (Broad Band Integrated Services Digital Network). [37]

En ATM se usan pequeñas unidades de longitud fija para transferir los datos, llamadas células. Los paquetes de datos son segmentados en células antes de ser colocados en el medio de transmisión, y son reensamblados subsecuentemente en el destino; esto conlleva a que las células de paquetes de tiempo crítico pequeño (por ejemplo, las de tráfico de voz) sean intercaladas con aquellas de paquetes muy grandes (por ejemplo transferencia de archivos).

La cabecera contiene información para administrar la transmisión de la celda (5 Bytes), y la parte de información de la celda siempre tiene la misma longitud y

contiene los datos que se quieren transmitir (48 bytes) de datos. [27] Ver la distribución de una celda ATM en la Figura. 2.1

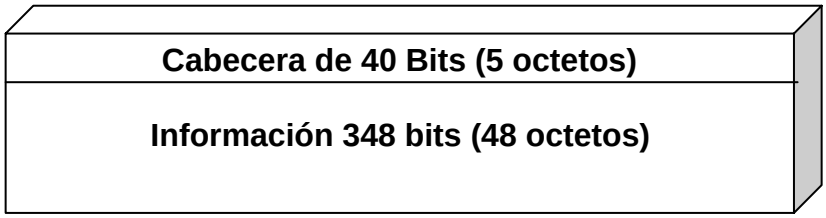


Figura 2.1 Cabecera de ATM

En resumen, las células* de longitud fija y pequeña producen un retardo mucho menor, y reducen el jitter* (variación de fase inaceptable) en la transmisión de datos en tiempo real a través de la red.

ATM combina la ventaja de poder tener un ancho de banda garantizado, ofrecida por los servicios de emulación de circuitos con la flexibilidad de la asignación de ancho de banda dinámico (bajo demanda) que ofrece la conmutación de paquetes. Antes de que la comunicación pueda tener lugar en una red ATM, se establece una conexión o circuito virtual entre el emisor y el receptor. El circuito virtual garantiza la disponibilidad en la red del ancho de banda solicitado, a diferencia de los sistemas tradicionales orientados a conexión, tal como el sistema telefónico, en el que el ancho de banda de cualquier conexión punto a punto es estadístico, el ancho de banda de un circuito virtual es dinámico y se establece cuando se crea este circuito.

En la red ATM, el medio físico no es compartido. En vez de esto, cada dispositivo conectado a la red ATM tiene su propio enlace dedicado que se conecta directamente el switch.

2.1.1 Características ATM

- ATM es considerado un modo de transferencia orientado a conexión, basado en la multiplexación asíncrona por división en el tiempo y el uso de las células de longitud fija. Cada célula contiene un campo de información y un encabezado, el cual es usado principalmente para identificar células

pertenecientes al mismo canal virtual dentro de la multiplexación asíncrona por división en el tiempo, y para realizar el direccionamiento apropiado. La integridad en la secuencia de las células es conservada para cada canal virtual.

- El tiempo de información de las células ATM, es llevado en forma transparente a través de la red, de modo que no se realiza ningún procesamiento tal como control de errores. Todos los servicios (voz, video, datos) pueden ser transportados vía ATM, incluyendo los servicios no orientados a conexión. Para acomodar varios servicios, se han definido varios tipos de Capas de Adaptación (AAL), dependiendo de la naturaleza del servicio, para ajustar la información dentro de las células ATM, y para proporcionar funciones específicas del servicio (tales como recuperación del reloj, recuperación de células perdidas). La información específica de la AAL está contenida dentro del campo de información de la célula ATM.

- En el direccionamiento, los valores del encabezado son asignados a cada sección de una conexión para la duración completa de la misa, y traslados cuando se conmuta de una sección a otra. La señalización y la información del usuario son transportadas en canales virtuales separados.

- Como ATM es orientado a conexión, las conexiones son establecidas, ya sea, en forma permanente o por la duración total de la conexión, en el caso de servicios conmutados. Este establecimiento incluye la asignación de un **VCI** (Virtual Circuit Identifier / identificador de Circuito Vitual) y/o un **VPI** (Virtual Path Identifier / Identificador de Trayecto Virtual), pero también, la asignación de los recursos empelados en el acceso de usuario y dentro de la red. Estos recursos determinarán el throughput y calidad de servicio (QoS). Pueden ser negociados entre el usuario y la red a través de **UNI** (User Network Interface), durante la fase de inicio de la llamada y posiblemente durante la llamada.

2.1.2 Arquitectura de ATM

El modelo OSI usa el concepto de planos separados para la segregación de funciones de usuario, gestión y control. Esta organización en planos fue también utilizada en la Integrated Services Digital Network/Red Digital de Servicios Integrados de Banda Estrecha (RDS/-BE) y está descrita en la recomendación 1.320 del CCITT.

El modelo de protocolo B-ISDN para ATM se muestra en la figura 2.2 Igual que el N-ISDN PRM (Protocol Reference Model) contiene 3 planos: un plano de usuario para transportar información del usuario, un plano de control, compuesto principalmente de información de señalización y un plano de gestión, usado para mantener la red y realizar funciones operativas. Adicionalmente, se ha añadido una tercera dimensión al PRM, llamada Plano de administración, que es responsable de la administración de los planos diferentes.

2.1.2.1 Capa física

Está compuesta por dos subcapas:

Subcapa del medio físico (PM Physical Médium).- Esta subcapa es responsable de la transmisión y recepción correcta de bits en el medio físico apropiado. En el más bajo nivel de esta capa, esta función es completamente dependiente del medio. Adicionalmente, esta subcapa debe garantizar una apropiada reconstrucción del bit timing en el receptor, por lo tanto, la entidad al punto de transmisión será responsable de insertar la información requerida de bit timing y codificación de línea.

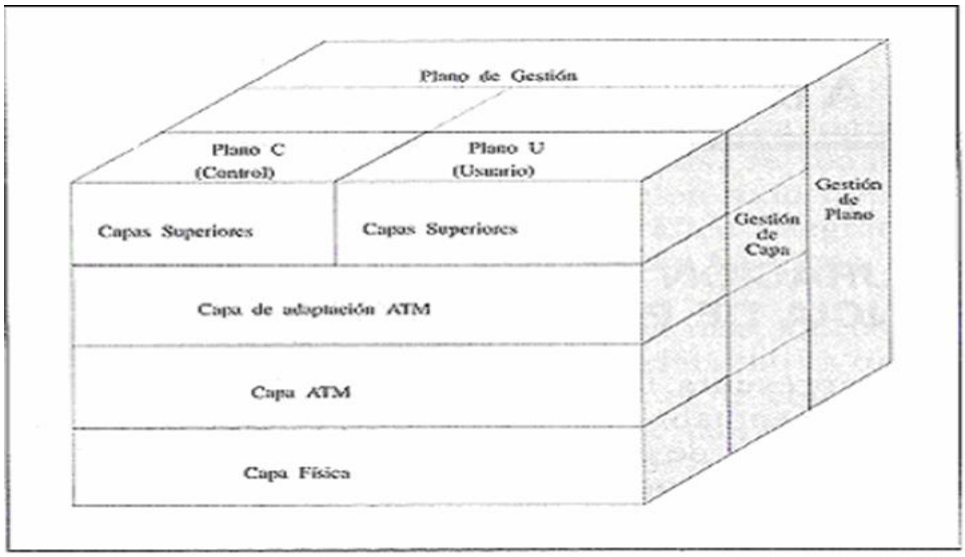


Figura 2.2 Protocolo de Modelo de Referencia para ATM Banda Ancha [14]

Subcapa de Convergencia de la Transmisión (TC Transmíssion Convergence), Aquí, los bits son ya reconocidos tal como vienen de la subcapa PM Physical Médium, realizándose básicamente 5 funciones:

1. Después de la reconstrucción de los bits, se hace la adaptación transmisión utilizado. Los sistemas pueden ser: SDH (Syncnronous Digital Hierarchy / Jerarquía Digital Síncrona). PDH (Plesiochronous Digital Hierarchy I Jerarquía Digital Pleosíncrona) o basada en células.

2. HEC (Header Error Check I Generación de la Comprobación de; Error en el Encabezado) para cada célula durante la transmisión y su verificación en el receptor.

3. Delineación de la célula, basado en el algoritmo delineador HEC, el cual asume que si el HEC es reconocido para un número consecutivo de células entonces se ha encontrado la frontera correcta de la célula.

4. Una vez que la delineación se ha localizado, se aplica un método adaptado que usando el HEC, detecta y corrige errores en el

encabezado
dependiendo de la situación.

5. Finalmente esta subcapa debe asegurar la inserción y supresión de células sin asignar, para adaptar el régimen utilizable a la carga útil del sistema de transmisión. Esta función se llama desacoplamiento del régimen de células.

2.1.2.2 La capa ATM

La capa ATM es completamente independiente del independiente de la Capa Física. Las siguientes realizadas por esta capa:

- Multiplexación y Demultiplexación de células de conexiones diferentes (identificadas por valores diferentes de VPI y VCI) dentro de un solo flujo de células de la capa física.
- Traducción del identificador. pues esta es requerida en la mayoría de los casos, cuando se conmuta una célula desde un enlace físico hacia otro dentro de un conmutador ATM o en una conexión cruzada. Esta traducción se puede realizar ya sea en el VPI o en el VCI por separado, o en ambos simultáneamente.
- Dar al usuario de un VCC o VPC una clase de QoS, de las clases soportadas por la red. Algunos servicios pueden requerir de una determinada QoS para una parte del flujo de células de una conexión, y un QoS menor para el resto.
- Funciones de Gestión. Estas funciones incluyen la supervisión, el diagnóstico y el mantenimiento de todos los dispositivos empleados en la red.
- Extracción o Adición del encabezado de célula antes o después de que la célula se entregada a (/desde) la Capa de Adaptación.
- Implementación de un mecanismo de control de flujo en la interfaz de red del usuario.

2.1.2.3 La capa de adaptación de ATM (AAL)

La capa de Adaptación de ATM, amplía el servicio proporcionado por la Capa ATM hacia un nivel requerido por la capa superior más próxima. Esta capa realiza funciones para los planos de usuario, control y de gestión, así como el soporte de mapeo entre la capa ATM y la capa superior mas próxima. Las funciones realizadas por la AAL dependen de los requerimientos de la capa superior.

La capa AAL está subdividida en dos subcapas: la de segmentación y reensamblado (SAR) y la subcapa de convergencia (CS).

El propósito principal de la SAR, es la segmentación de la información de la capa superior, en un tamaño adecuado a la carga útil de las células ATM de una conexión virtual y la operación inversa; reensamblando el contenido de las células de una conexión virtual, en unidades de datos que se entregarán al nivel superior.

La CS realiza funciones tales como: la identificación de mensaje, recuperación de reloj, etc. Para algunos tipos de AAL que soportan el transporte de datos sobre ATM, la subcapa de convergencia ha sido subdividida en: CPCS (Common Parí Convergence Sublayer I Subcapa de Convergencia de Parte Común) y SSCS (Service Specifíc Convergence Sublayer I Subcapa de Convergencia de Servicio Específico).

Algunos usuarios del servicio de AAL podrían encontrar el servicio ATM suficiente para sus requerimientos. En ese caso, el protocolo AAL podría estar vacío.

Las SDU (Service Data Units I Unidades de Servicios de Datos) del AAL son transportadas de un SAP (Service Access Point / Punto de Acceso al Servicio) de la AAL hacia uno o algunos otros a través de la red A TM. Los usuarios de AAL tendrán la capacidad de seleccionar un AAL-SAP dado que este asociado con el QoS requerido para transportar las SDU- AAL. [42]

2.2 FDDI (Interfaz de Datos Distribuidos por Fibra)

La FDDI o Interfaz de Datos Distribuidos por Fibra (Fiber Distributed Data Interface), es una interfaz de red en configuración de simple o doble anillo, con paso de testigo, que puede ser implementada con fibra óptica, cable de par trenzado apantallado (STP-Shielded Twisted Pair), o cable de par trenzado sin apantallar (UTP-Unshielded Twisted Pair).

Esta norma fue definida, originalmente, en 1982, para redes de hasta 7 nodos y 1 Km. de longitud, denominada como LDDI (Locally Distributed Data Interface). Sin embargo, en 1986 fue modificada y publicada como borrador de la norma actual, e inmediatamente aprobada, apareciendo los primeros productos comerciales en 1990.

La tecnología FDDI permite la transmisión de los datos a 100 Mbps., según la norma ANSI X3T9.5, con un esquema tolerante a fallos, flexible y escalable.

Una FDDI viaja por el anillo de la red desde un nodo hasta otro. Si un nodo no necesita transmitir datos, toma el testigo y lo envía al nodo siguiente. Si el nodo que posee el testigo necesita transmitir, puede enviar todas las tramas que desee durante un tiempo, llamado tiempo de retención de testigo. Es posible que varias tramas de varios nodos estén en la red en un tiempo determinado, proporcionando comunicaciones de gran capacidad, por que FDDI utiliza un método de liberación temprana de testigo.

Una vez que un nodo transmite una trama, esta se desplaza hasta el próximo nodo del anillo, cada uno de los nodos determina si la trama esta destinada a el y si existen errores en la trama. Si el nodo es el que tiene que recibir la trama, este lo marca como leído, si algún nodo detecta un error, marca un bit de estado para indicar una condición de error. Cuando la trama vuelve al nodo que origino la transmisión, se lee de nuevo para determinar si el nodo dstino lo recibió. También se comprueban los errores de la trama, de manera que si se detecta un error, se

retransmitirá la trama. Si no se encuentran errores, el nodo que origino la transmisión sacara esa trama del anillo. [28]

2.2.1 Características de FDDI

- FDDI ofrece 100 Mbps con hasta 500 estaciones conectadas, distanciadas en un máximo de 2 km y conectadas por medio de fibra óptica, en una circunferencia máxima de 100 Km. La capacidad de comunicación es de 450,000 paquetes por segundo y es determinada por la codificación empleada, denominada 4B/5B, con una frecuencia de reloj de 125mhz siendo por lo tanto la eficacia del 80 %.
- FDDI se utiliza para proporcionar conexiones de alta velocidad a varios tipos de red. FDDI se puede utilizar para redes de área metropolitana (MAN) que permiten conectar redes en la misma ciudad con una conexión de fibra óptica de alta velocidad.
- FDDI especifica el uso de anillos duales. El tráfico en estos anillos viaja en direcciones opuestas. Físicamente, los anillos consisten de dos o más conexiones punto-a-punto entre estaciones adyacentes. Uno de los dos anillos FDDI es llamado el *anillo primario* y el otro es llamado el *anillo secundario*. El anillo primario es usado para transmisión de datos mientras el secundario es usado como un respaldo.

  Los nodos clase A, que son los equipos de red, y se conectan a los dos anillos de la red. Estos nodos tienen la posibilidad de reconfigurar wl anillo para permitir que los dos anillos se conecten en el caso de que se produzca una falla en la red, y puede ser DAS.

  Los nodos de clase B, que se conectan ala red FDDI a través de los dispositivos de clase A y se conectan únicamente a anillo primario, y pueden ser SAS:

  SAS: (single attach station / estaciones de asignación simple) se conectan a un anillo **DAS**: (dual attach station / *estaciones de asignación dual*) se

conectan a ambos anillos. SAS son conectados al anillo primario a través de un concentrador, el cual provee conexiones para múltiples SAS. El concentrador asegura que cuando falle o se apague cualquiera de los nodos SAS no se interrumpa al anillo. Esto es una particularidad usada cuando PCs, o dispositivos similares que frecuentemente son encendidos y apagados, se conectan al anillo. Ver figura 2.2 [30]

Una típica configuración FDDI con DAS y SAS se muestra en la Figura.

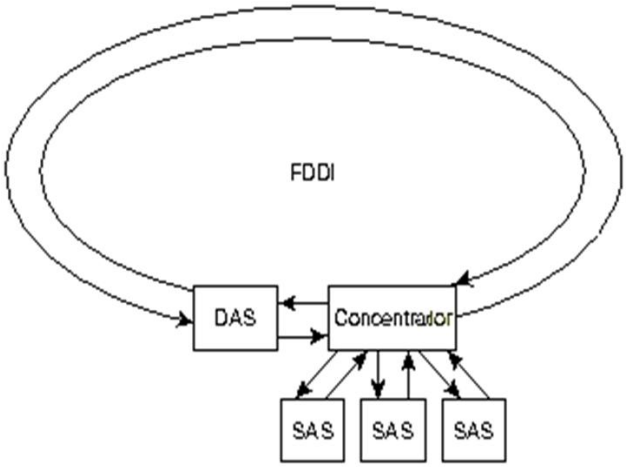


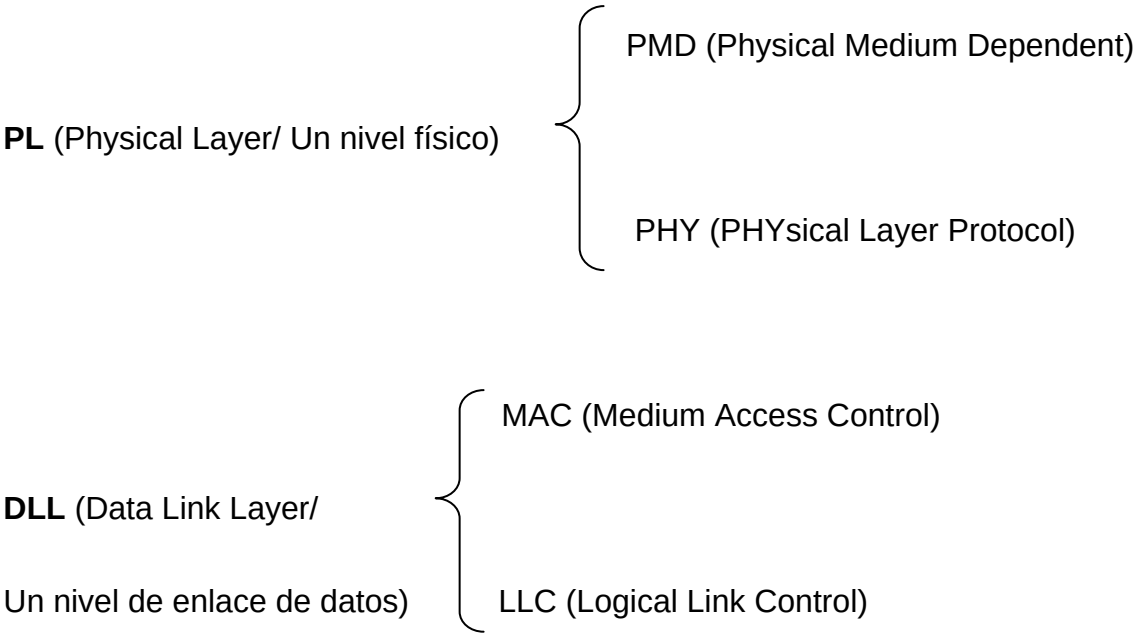
Figura 2.3 Nodos FDDI: DAS, SAS, y Concentrador

2.2.2 Arquitectura de FDDI

El estándar FDDI especifica un troncal de fibra óptica multimodo, que permite transportar datos a altas velocidades con un esquema de conmutación de paquetes y paso de testigo en intervalos limitados.

En una red FDDI, pueden coexistir un máximo de 500 estaciones, distanciadas en un máximo de 2 Km. y conectadas por medio de fibra óptica 62,5/125 mm, en una circunferencia máxima de 100 Km. El error máximo es de 10^{-9} bits. [28]

La norma FDDI se descompone en:



SMT (Station Management/ estándar de gestión de estación), que suministra el control necesario, a nivel de la estación, para gestionar los procesos situados en los diversos niveles de FDDI.

2.2.3.1 Nivel físico

El nivel físico PL (Physical Layer) está constituido por dos subniveles:

1.- El subnivel PMD (Physical Medium Dependent), que ofrece todos los servicios necesarios para las comunicaciones digitales punto a punto entre las estaciones de una red FDDI, es decir, para la transmisión de oleadas de bits codificadas de una estación a otra. El PMD define y caracteriza los emisores y receptores ópticos, los inconvenientes de código impuestos por el soporte, los cables, los conectores, el balance energético, los repetidores ópticos y otras características físicas.

2.- El subnivel PHY (PHYsical Layer Protocol), que es objeto de la norma ISO 9313.1. Permite la conexión entre el PMD y el DDL. El nivel PHY es responsable de la sincronización y de la codificación y descodificación. Se utilizan dos niveles

de codificación: el PHY convierte los símbolos procedentes del MAC en bits codificados en NRZ, el código utilizado es un código de grupo de tipo 4B/5B, un grupo de 4 bits de datos está codificado en un grupo de 5 bits codificados en NRZ, que a su vez están codificados en una secuencia de 5 bits codificados en NRZI. [29]

2.2.3.2 El nivel de enlace de datos

MAC o Media Access Control (control de acceso al medio). Su función es la programación y transferencia de datos hacia y desde el anillo FDDI, así como la estructuración de los paquetes, reconocimiento de direcciones de estaciones, transmisión del testigo, y generación y verificación de secuencias de control de tramas (FCS o Frame Check Sequences).[28]

Este subnivel está destinado a ser utilizado sobre una red de altas prestaciones. Este protocolo está pensado para ser operativo a 100 Mbits/s sobre un bucle en anillo basado en testigo y un soporte de fibra óptica, pudiendo cubrir distancias de varias decenas de kilómetros. El acceso al soporte está controlado por un testigo; una estación que haya capturado el testigo lo retransmite inmediatamente por el soporte una vez que haya terminado su transmisión. Se han diferenciado dos clases de servicios sobre una red FDDI.

MAC aporta las mayores novedades de FDDI y soporta dos tipos de tráfico:

- Tráfico síncrono: voz, imágenes, información que debe ser transmitida antes de un determinado tiempo. Podría decirse que es tráfico de datos en tiempo real.

- Tráfico asíncrono: e-mail, Ftp, información para la cual el tiempo que tarde en llagar al destino no es el factor decisivo.

La filosofía que persigue FDDI es atender primero el tráfico síncrono y después el tráfico asíncrono. Para ello, cada estación tiene varios temporizadores:

- Token Rotation Time (TRT): tiempo transcurrido desde que llegó el último testigo.

- Token Hold Time (THT): tiempo máximo que una estación puede poseer el testigo. [29]

2.2.3.3 El subnivel SMT

SMT (Station Management/gestión de estaciones). Se encarga de la configuración inicial del anillo FDDI, y monitorización y recuperación de errores. Incluye los servicios y funciones basados en tramas, así como la gestión de conexión (CMT o Connection Management), y la gestión del anillo (RMT o Ring Management). Se solapa con las otras 3 subcapas FDDI, y por tanto fue la de más complicada aprobación por parte de ANSI, que se realizó en 1993. [28]

La siguiente figura 2.4 muestra la arquitectura de FDDI

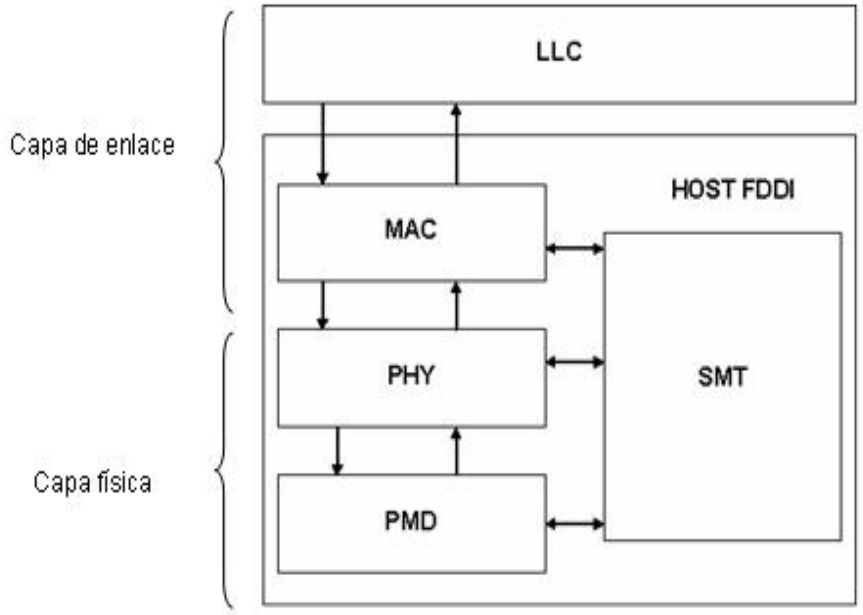


Figura 2.4 Arquitectura de FDDI

2.3 FDDI II

En 1985 surgió la necesidad de una red local capaz de soportar simultáneamente voz y datos. El protocolo FDDI se revelo inadecuando para este tipo de aplicación, principalmente en redes con gran numero de nodos. Así pues se propuso un nueva versión del bucle FDDI, principalmente a iniciativa de especialistas en telecomunicaciones, también basada sobre bucles de fibra óptica, a fin de ofrecer una calidad de servicio adecuada para la voz. El protocolo FDDI II utiliza una técnica de conmutación híbrida. De esta forma, la norma FDDI II ofrece procedimientos de conmutación de circuitos para tráficos de voz y video, y de conmutación de paquetes para los datos. [31]

FDDI II es una propuesta de la norma americana ANSI (Comité X3T9.5), para una red local de 100 Mbps, con una longitud de más de 50 Km. Se trata de un doble bucle de control de acceso por testigo.

FDDI II es una expansión de la norma FDDI, que añade una trama sincronía. La banda de paso esta constituida por la trama asíncrona y 16 canales sincronos, que contienen 96 “cycle groups” de 16 bytes cada uno. Los canales isócronos, pueden ser asignados y no asignados dinámicamente en tiempo real, con lo que la capacidad no asignada queda disponible para el canal de paso de testigo. [28]

2.3.1 Arquitectura de FDDI II

La capa Física y la capa de enlace son las mismas que FDDI. En el nivel MAC, hay dos nuevos componentes que son: IMAC Y HMUX.

IMAC (Media Access Control isócrono) especifica las reglas para compartir los canales asignados para la conmutación de circuito.

HMUX (multiplexor híbrido) combina la forma packet-switched y con conmutador de circuito del tráfico la estación para la transmisión encendido al medio. Las especificaciones para HMUX e IMAC se combinan en un documento estándar nombrado HRC (control híbrido del anillo).

2.3.1.1 EL modo híbrido

- En modo híbrido, los servicios del paquete y del circuito están disponibles. Una red de FDDI-II comienza típicamente hacia fuera en modo básico a instalar los contadores de tiempo y los parámetros necesarios para el protocolo simbólico sincronizado, entonces cambian al modo híbrido.
- La conmutación de circuito se alcanza por medio de un formato del ciclo creado por una estación conocida como el ciclo maestro. El ciclo maestro es responsable de crear los ciclos en un índice de 8 khz. e inserta el estado latente requerido para mantener un número integral de ciclos síncronos en el anillo. Los ciclos son repetidos por el resto de las estaciones en el anillo. Mientras que cada ciclo termina su circuito del anillo, es anulado por el el ciclo maestro.
- La subcapa de IMAC dentro del HRC (control híbrido del anillo) controla los canales de ancho de banda (wideband WBCs) que se utilizan para el tráfico con conmutador de circuito. Cada WBC puede apoyar un solo canal isócrono. Alternativamente, en WBC puede ser subdividido por IMAC en un número de subcanales. Estos subcanales separados permiten diálogos simultáneos, independientes, isócronos entre diversos pares de estaciones de FDDI-II.
- Durante la operación normal, la actividad en una red de FDDI-II consiste en una secuencia de los ciclos generados por el ciclo maestro. Las estaciones se comunican con la conmutación de circuito compartiendo el uso de un canal isócrono dedicado. Las estaciones se comunican con conmutación de conjunto de bits sobre el canal de los datos del paquete.
- **La Inicialización**. El anillo será configurado para inicializarse en modo básico. Una vez que se establezca el modo básico y operación, unas o más estaciones pueden procurar mover la red al modo híbrido publicando un ciclo.
- **EL Mantenimiento de programación de la plantilla**. El ciclo maestro mantiene la plantilla de programación. La asignación de la capacidad entre

el paquete y la transmisión del circuito se puede modificar dinámicamente por medio de peticiones de SMT al ciclo maestro. [32]

2.3.2 Diferencia entre el FDDI y FDDI-II

El FDDI y FDDI-II funciona en 100 M bits/seg.4 en la fibra. El FDDI puede transportar tipos asincrónicos y sincronos de bastidores. FDDI-II tiene un nuevo modo de operación llamado Hybrid Mode. El modo híbrido utiliza una estructura del ciclo 125useg para transportar tráfico isócrono, además de marcos de synchronous/asynchronous. FDDI-II apoya la voz integrada, vídeo, y las capacidades de los datos y por lo tanto amplían la gama de usos del FDDI. Las estaciones del FDDI y de FDDI-II se pueden funcionar en el mismo anillo solamente en modo básico. [32]

2.4 DQDB (Cola Distribuida en Doble Bus).

DQDB (Distributed Queue Dual Bus) es una arquitectura para las redes de área local metropolitana desarrollada por el IEEE (la Subred MAN IEEE 802.6), basada en unos trabajos realizados en la University Western Australia en 1988, que adopto inicialmente el nombre de QPSX (Queue Packet and Synchronous Switch). El objetivo marco de DQDB es la interconexión de redes de área local redes de área extensa a través de un red de area metropolitana con un perímetro máximo de 160 Km. De esta forma, se diferencia su planteamiento del establecido para FDDI, el cual era básicamente interconectar recintos o campus a través de una red de 100 Km. de perímetro. Por estar concebida para conectarse a redes de área extensa, DQDB debía apoyarse en los conceptos de transferencia emergentes, particularmente la tecnología ATM. Por ello la unidad de transferencia en DQDB es también una célula con 48 octetos de carga útil y 5 octetos de cabecera.[22]

Durante la deliberación dentro de la IEEE rápidamente se dieron cuenta que la tecnología era capas de manejar velocidades de mas de 20Mbps. Esto implicaba que debían consultar conjuntamente con la ANSI (Instituto de Estándares Nacionales Americanos). Cuando esto no paso los americanos se sintieron indispuestos. Lo que paso después fue que las empresas europeas Alcatel N.V.

(Paris) y Siemenx Aktiengesellschaft (Munich) monopolizaron en una gran área geográfica la distribución de productos basados en QPSX. Los americanos, que ahora si se sintieron completamente marginalizados deciden tomar otros rumbos para el diseño de redes MAN, en 1990 Telecom comienza a hacer experimentos comerciales con DQDB y desde 1992 comienza a ofrecer amplio servicio comercial.

2.4.1 Características de DQDB

- DQDB actualmente proporciona tecnologías de empaquetamiento rápido para la interconexión transparente de redes LAN y de servicios de datagrama a 2Mbps. DQDB además es capaz de proveer transmisión a alta velocidad, servicios de circuitos virtuales y servicio de transmisión de datos en isócrono. Así mismo DQDB garantiza una trama fija de datos para distribución en aplicaciones CAD/CAM, Teleconferencia e imágenes médicas.

- Las configuraciones en doble bus abierto o doble bus cerrado son posibles para DQDB. Donde las aplicaciones de datos son críticas es recomendable usar la configuración de doble bus cerrado para minimizar las fallas de tolerancia. Si el bus esta severamente accidentado la red deberá ser reconfigurada hasta que el punto roto en el bus sea desviado. Incluso en una configuración de bus abierto existe un alto nivel de falta de tolerancia incluso desde nodos que estén lógicamente adyacentes en el bus y puedan ser desviados en el momento que una falla se presente en uno de los nodos. Los nodos adyacentes no deben ser afectados si tienen capacidad de conservar su cabecera de bus.
- DQDB tiene muchas ventajas, este a sido aprobado como un estándar internacional (IEEE 802.6), que ofrece alta velocidad (de 2Mbps a 300 Mbps), que permite correr en diferentes medios, permite la interconexión entre redes MAN a MAN, ofrece servicios de conmutación de paquetes y

conmutación de circuitos y alto rendimiento independiente del numero de estaciones encadenados a la red.

2.4.2 Arquitectura de DQDB

2.4.2.1 Capa física

El procedimiento de proporcionar las distintas funciones de la capa física depende del medio y del sistema de transferencia utilizado, si bien todos los PLCP (protocolo de convergencia de nivel físico) deben seguir ciertos principios generales.

La Capa Física, en general, realiza las siguientes funciones:

- Delimitación de células.
- Transporte de las células sobre la estructura de transporte.
- Reconocimiento de células con información de gestión.
- Propagación de a información de sincronización de la capa DQDB.
- Control de los deslizamientos de tiempo (jitter) a valores aceptables.

Cada PLCP debe especificar una función de puente (bypass) en cada nodo, de modo que se pueda aislar a cada nodo de la red dejando a ésta en funcionamiento. Esta función permite mantener la red operativa en las siguientes situaciones:

- Cuando el nodo no está conectado a la alimentación.
- El nodo está conectado a la alimentación, si bien aún no está sincronizado con la red.
- La Capa Física determina que las funciones de acceso de este nodo están dañando a la red.
- La Entidad de Gestión de la Capa Física indica que el nodo debe aislarse.

La Capa Física debe monitorizar el porcentaje de errores de transmisión para proporcionar una calidad de servicios aceptable. El umbral de errores dependerá del sistema de transferencia y del medio. En caso de que un nodo que no sea

cabecera de bus detecte la caída de un enlace, debe notificarlo a la capa DQDB y al próximo nodo en el bus. [35]

2.4.2.2 La Capa DQDB

La capa DQDB provee la interfaz entre la capa física y los servicios de datos de las subredes DQDB. Y es responsable de funciones típicas LAN de enlace de datos incluyendo direccionamiento, secuenciación, detección de errores y control de acceso a medio. Esto corresponde a la subcapa MAC de la capa enlace de un modelo OSI. La capa DQDB soporta tres tipos de servicio de datos:

- Servicios MAC al control de enlace lógico. Provee un servicio de paquetes no orientado a conexión, a la subcapa de control de enlace lógico, entre dos sistemas abiertos que soporten el estándar IEEE 802.2*.
- Servicios de datos orientados a conexión. Transfiere paquetes de datos entre dos sistemas a través de un circuito virtual. Este servicio es asìncrono es decir no hay garantía de un constante intercambio de tiempo para estas unidades de datos.
- Servicio de bytes isócrono soportando servicio de switcheo de circuitos para aplicaciones sensitivas al tiempo. [34]

Estructura de un bus DQDB

En esta figura 2.5 se ilustra el sistema de bus abierto. Hay dos buses de fibra óptica que cargan los datos en direcciones opuestas des su cabecera de bus (HOB) hasta el terminador. Los HOB (head of bus) actúan como un slot* generador de señal, así que el bus nunca esta quieto. Los nodos están localizados adyacente en el bus y son lectores promiscuos. Pueden leer de todos los slot que vengan al bus pero no necesariamente alterar los datos. Los nodos pueden ser lectores activos o pasivos en el sistema, pueden actuar como repetidores para contrarrestar la atenuación. Si el nodo 2 desea enviar datos al nodo N, deberá usar el bus B.

Cuando un nodo escribe sobre un slot, la unidad de acceso primero lee el slot, luego escribe la localización dentro del slot y después cuando pasa el slot de regreso, éste atraviesa una compuerta lógica OR. Esto implica que es posible pasar de 0 a 1 pero no pasar de 1 a 0.

Esto es por que la verdadera función de una compuerta lógica OR es retornan un valor 0 si y solo si ambas afirmaciones son falsas, de otra manera retornará un valor de 1.

En una configuración de bus abierto, un nodo puede ejecutar o no las funciones de cabecera de bus (HOB). En un bus cerrado, un nodo actuará como el HOB para ambos buses. [35]

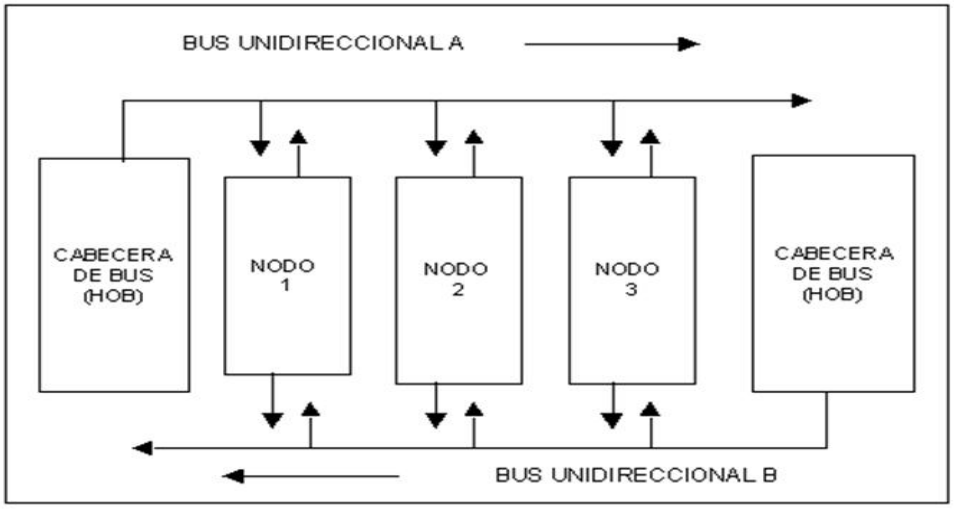


Figura 2.5 Estructura De un Bus DQDB [41]

2.5 Fast Ethernet

En la década de los 90´s, un grupo de compañías de redes se juntaron para formar la alianza de Fast Ethernet. El objetivo de este grupo fue promover la estandarización de Fast Ethernet, a lo que llamaron 802.3u 100BaseT de la IEEE, y aceleró la aceptación de dicha especificación en el mercado. La especificación final del 802.3u fue aprobada en Junio de 1995.

Dentro de otros objetivos de esta alianza se tiene:

- Mantener el CSMA/CD (Ethernet Transmission Protocol Carrier Sense Múltiple Access Collision Detection).
- Soportar los esquemas populares de cableado. (10BaseT).
- Asegurar que la tecnología Fast Ethernet no requerirá cambios en los protocolos de las capas superiores, ni en el software que corre en las estaciones de trabajo LAN. (no se necesita realizar cambios para el software de SNMP (Simple Network Managment Protocol) ni para las Management Information Bases (MIBs)).

2.5.1 Arquitectura de Fast Ethernet

El estándar 100Base-T (IEEE 802.3u9, esta compuesto de cinco especificaciones de componentes. Estos definen la subcapa MAC (Media Acces Control), el MII (Medio Independent Interfece) y tres Capas Físicas (100Base-T4, 100Base-TX y 100Base-FX).

2.5.1.1 SubCapa MAC

La subcapa 100BaseT MAC está basada en el protocolo CSMA/CD (carrier sense multiple access with collision detection) como lo está 10 Mbps Ethernet. Sólo se transmite cuando el medio está libre. Si múltiples estaciones comienzan a mandar datos al mismo tiempo, porque todas sensaron libre el medio, se detecta una colisión. En este caso, cada participante CSMA/CD tiene un retrazo máximo de 50 microsegundos y tamaño mínimo de trama de 512 bits, las longitudes cortas de cable para Fast Ethernet pueden alcanzar rangos de datos de 100 Mbps. La razón de tiempo de propagación a tiempo de transmisión se mantiene.

Fast Ethernet reduce el tiempo de duración de cada bit que es transmitido en un factor de 10, permitiendo que la velocidad del paquete se incremente de 10 Mbps a 100 Mbps; el formato de trama y longitud es como el 10BaseT. El intervalo interframe es de 0.96 microsegundos. Además mantiene las funciones de control

de errores de Ethernet y no se requiere traducción de protocolo para moverse entre Ethernet y Fast Ethernet.

2.5.1.2 MII Media Independent Interface

MII es una especificación nueva que define una interfase estándar entre la subcapa MAC y cualquiera de las tres capas físicas (100BaseTX, 100BaseT4, y 100BaseFX). Su función principal es ayudar a la subcapa convergente hacer uso del rango de bits más alto y diferentes tipos de medios transparentes a la subcapa MAC. Es capaz de soportar 10Mbps y 100 Mbps. Puede ser implementado en un dispositivo de red tanto interna como externamente. Internamente conecta la supcapa MAC directamente a la capa física. Usualmente con adaptadores (NICs).

MII también define un conector de 40 pins que puede soportar transceptores externos. Un uso de transceptores adecuados puede conectar estaciones de trabajo a cualquier tipo de cables instalados, muy parecido a un conector AUI para 10 Mbps Ethernet.

2.5.1.3 Capa física

Fast Ethernet puede correr a través de la misma variedad de medios que 10BaseT (UTP,STP y Fibra Optica), pero no soporta cable coaxial. La especificación define 3 tipos de medios con una subcapa física separada para cada tipo de medio:

Capa Física para 100BaseT4 Esta capa física define la especificación para 100BaseT para 4 pares de categoría 3, 4 o 5 UTP. 100BaseT4 es half-duplex que usa tres pares para transmisión 100 Mbps y el cuarto par para detección de colisiones y recibir.

Capa física 100BaseTX . Esta posee un sistema similar de 100Base-T, donde un par es usado para transmitir (con frecuencia de operación de 125Mhz al 80% de eficiencia para permitir codificación 4B/5B) y el otro par lo usa para detección de colisiones y recibir 4B/5B o codificación cuatro binario/cinco binario en códigos, es

un esquema que usa 5 bits de la señal para cargar 4 bits de datos. Tiene 16 valores de datos, 4 códigos de control y un código ocioso que no usa.

Capa física 100BaseFX Define la especificación para 100BaseT Ethernet a través de dos hilos de fibra; utilizando una fibra para la transmisión y la otra fibra para detección de colisiones y recibir. Su canal de señalización está basado en las capas físicas de FDDI.

Dentro del estándar 100Base-T existen dos tipos de repetidores de acuerdo a su clase:

Clase I: Solo un repetidor de esta clase puede estar entre dos DTE (Equipo Terminal de Datos o Estación) dentro de un dominio de colisión.

Clase II: Dentro de un dominio de colisión uniendo dos estaciones (DTE) pueden estar conectados en cascada dos repetidores de esta clase como máximo, no más. [33]

2.6 Frame-Relay

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI: el CCITT (Comité de Consulta Internacional en Telegrafía y telefonía). Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores en cada “salto” de la red.

Frame Relay es un servicio público que proporciona conexiones entre usuarios, a través de redes de alta velocidad (64 kbit/s a 2 Mbit/s) y bajo retraso, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un solo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores y las tramas deben de llegar ordenadas al destinario, ya que todas siguen el mismo camino a través de la red. [36]

Frame Relay es un servicio orientado a conexión (“connetion oriented”), dichas conexiones son totalmente equivalentes y coincidentes, e incluso más apropiadas que los circuitos basados en redes de routers y, por tanto, que las proporcionadas por SMDS.

Frame Relay se define como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps, aunque nada le impide superarlas.

Frame Relay es un servicio de transmisión de datos especialmente diseñado para cubrir las necesidades de uso e interconexión de LANs, con el fin de eliminar distancias geográficas y aumentar considerablemente el volumen de datos a transmitir.

2.6.1 Características de Frame Relay

- El servicio Frame Relay permite que diferentes canales compartan una sola línea de transmisión. La capacidad de enviar en ciertos periodos breves de tiempo un gran volumen de tráfico (“tráfico a ráfagas”), aumenta la eficiencia de las redes basadas en Frame Relay, a ello debemos su alta velocidad y bajos retardos.
- Se trata de un servicio de transporte que opera en la capa 2 del modelo OSI, transmite la información estructurada en tramas y es capaz de soportar múltiples protocolos y aplicaciones correspondientes a diversos entornos de comunicaciones de clientes. El carácter multiprotocolo del servicio Frame Relay se ha visto ampliado por el desarrollo de estándares para la transmisión de voz sobre Frame Relay.
- El servicio Frame Relay, se plasma en la red cliente como un conjunto integrado de conexiones de acceso, circuitos virtuales, y en general, recursos de red que constituyen el servicio entregado al cliente. La red cliente se soporta sobre la red UNO, que proporcional la interconexión con otras redes internacionales.

- Frame Relay maneja circuitos virtuales permanentes (PVC) y circuitos virtuales conmutados (SVC) y, por la manera en que estos han sido diseñados, la probabilidad de que las tramas se envíen en orden es muy alta. Los circuitos virtuales pueden ser del tipo punto a punto, punto a multipunto y multipunto a multipunto. [37]
- Para los clientes del Servicio Frame Relay, existe la posibilidad de contratar el servicio nodo de red, que permite introducir un Nodo de RED gestionado en el propio domicilio del cliente. Brindándoles los siguientes servicios:

    - Optimización de los costes de telecomunicaciones
    - Solución personalizada de Red.
    - Servicio gestionado extremo a extremo: Transmisión Telefónica de Datos que se ocupa de la configuración, administración, mantenimiento, supervisión y control permanente durante las 24 horas del día, los 365 días del año de los elementos de red.
    - Tecnología de punta y altas prestaciones: Frame Relay proporciona alta capacidad de transmisión de datos, ya que utiliza nodos de red de alta tecnología y bajos retardos como consecuencia de la construcción de la red backbone sobre enlaces a 34 Mbps y de los criterios de encaminamiento de la RED UNO.
    - Flexibilidad del servicio: Frame Relay es una solución adaptable a las necesidades cambiantes del cliente, basada en PVC. Sobre una interfaz de acceso a la red, se pueden establecer simultáneamente múltiples PVC distintos, lo que permite un fácil incorporación de nuevas sedes a la Red de Cliente.
    - Servicio Normalizado: Frame Relay es un servicio normalizado según los estándares y recomendaciones de ITU-T y ANSI, con lo que queda garantizada la interoperatividad con cualquier otro producto Frame Relay asimismo normalizado.
    - Se distingue tres frases en la provisión del servicio: de oferta o preventa de instalación y de prestación o post-venta.

- Frame Relay es un servicio de tarifa plana que incluye una cuota de alta inicial y cuotas mensuales fijas independientes del trafico cursado.

2.6.2 Arquitectura para Frame Relay

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario, que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión a través de la ruta establecida para la conexión en la red. [36]

Este equipo se denomina FRAD (Frame Relay Assembler/Disassembler/ Ensamblador/Desensamblador Frame Relay) y el nodo de red se denomina **FRND** (Frame Relay Network Device / Dispositivo de Red Frame Relay).

La trama y cabecera de Frame Relay puede tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico.

La información transmitida en una trama frame relay, puede oscilar entre 1 y 8,250 bytes, aunque por defecto es de 1,600 bytes.

Lo más increíble de todo, es que a pesar del gran número de formas y tamaños, Frame Relay funciona perfectamente, y ha demostrado un muy alto grado de interoperatibilidad entre diferentes fabricantes de equipos y redes; ello es debido a que sean las que sean las opciones empleadas por una determinada implementación de red o equipamiento, siempre existe la posibilidad de “convertir” los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

En Frame Relay, por tanto, los dispositivos del usuario se interrelacionan con la red de comunicaciones, haciendo que sean aquellos mismo los responsables del

control de flujo y de errores. La red sólo se encargar de la transmisión y conmutación de los datos, así como de indicar cuál es el estado de sus recursos.

En el caso de errores o de saturación de los nodos de la red, los equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas, y si es preciso, reducirán la velocidad de transmisión para evitar la congestión.

Las redes Frame Relay son orientadas a conexión, su principio básico, es dividir el nivel de enlace en dos subniveles, con el fin de incrementar el desempeño y la velocidad de la red, partiendo del supuesto de que los medios de transmisión utilizados a nivel físico son altamente confiables.

El identificador de conexión es la concatenación de dos campos de HDLC (High-level Data Link Control) en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Por ello, el “identificador de conexión de enlace de datos” o DLCI (Data Link Connection Identifier / Identificación de Conexión de Enlace de Datos), esta interrumpido por algunos bits de control.

Otros bits de la cabecera tienen funciones muy especiales en las rede Frame Relay. Dado que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red, y que estas funciones son imprescindibles, para ello, algunos bits de la cabecera. [37]

Los tres campos más esenciales son:

- **DE** (Discard Eligibility / Elegible para ser Rechazada), que es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión.
- **FECN** (Forward Explicit Congestion Notification / Notificación de Congestión Explicita de Envió), que es usado con protocolos de sistema final que controlan el flujo de datos entre el emisor y el receptor, como el

mecanismo “windowing” de TCP/IP, en teoría, el receptor puede ajustar su tamaño de “ventana” en respuesta a las tramas que llegan con el bit FECN activado.

- **BECN** (Backward Explicit Congestion Notification / Notificación de Congestión Explicita de Reenvio). Como es lógico, puede ser usado con protocolos que controlan el flujo de los datos extremo a extremo en el propio emisor.

Según esto, la red es capaz de detectar errores, pero no de corregirlos (en algunos casos podría llegar tan solo a eliminar tramas).

No se ha normalizado la implementación de las acciones de los nodos de la red ni del emisor / receptor, para generar y/o interpretar estos tres bits. Por ejemplo, TCP/IP no tiene ningún mecanismo que le permita ser alertado de que la red Frame Relay está generando bits FECN, ni de cómo actuar para responder a dicha situación.

Frame Relay También ha sido denominado FPT (Fast Packet Technology / Tecnología de Paquetes Rápidos) o “X.25” para los 90’s.

El protocolo X.25 opera en la capa 3 e inferiores del modelo OSI, mediante la conmutación de paquetes a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red, X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 no envié paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesar. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos, no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador

de paquetes X.25, y la combina con las funciones de trama. Así, la trama contiene al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una “conmutación de paquetes”.

Lógicamente, todo el control de errores en el contenido de la trama y el control de flujo, debe ser realizado en los extremos de la comunicación (nodo origen y nodo destino). La conmutación de paquetes en X.25, un proceso de 10 pasos, se convierte en uno de 2 pasos, a través de la transmisión de tramas.[37]

2.7 Gigabit Ethernet (1000BASE-T)

Gigabit Ethernet es una extensión a las normas de 10 Mbps y 100 Mbps IEEE 802.3.Ofreciendo un ancho de banda de 1000 Mbps, Gigabit Ethernet mantiene compatibilidad completa con la base instalada de nodos Ethernet.

Gigabit Ethernet soporta nuevos modos de operación full duplex para conexiones conmutador-conmutador y conexiones conmutador-estación y modos de operación half-duplex para conexiones compartidas que usan repetidores y los métodos de acceso CSMA/CD. Inicialmente operando sobre fibra óptica, Gigabit Ethernet también podrá usar cableados UTP y coaxiales de categoría 5 y 6.

Las implementaciones iniciales de Gigabit Ethernet emplearan cableados de fibra de gran velocidad, los componentes ópticos para la señalización sobre la fibra óptica serán 780 nm (Longitud de onda corta) y se usara el esquema 8B/10B para la señalización y deseñalizacion. Esta reforzándose la tecnología de fibra actual que opera a 1.063 Gbps para correr a 1.250 Gbps, proporcionando así los 1000 Mbps completos. Para enlaces a mas largas distancias, por encima de al menos 2 Km. Usando fibra monomodo y por encima de 550 metros con fibra multimodo de 62.5; también se especificaran ópticas, de 1300nm (longitud de onda larga)

2.7.1 Arquitectura del protocolo Gigabit Ethernet

Para acelerar la velocidad de Fast Ethernet de 100 Mbps a Gbps, se necesitaron grandes cambios en la interfaz física. Se decidió que Gigabit Ethernet pareciera idéntico a Ethernet en el nivel de enlace de datos.

El reto para superar la aceleración a 1 Gbps, fue resuelto aprovechando la alta velocidad de la tecnología de Fiber Channel manteniendo el formato de frame, de IEEE 802.3 y de Ethernet, la compatibilidad con los medios instalados, y el uso de full o half duplex (vía CSMA/CD)

Sus capas son:

2.7.1.1 Interface física

La especificación de Gigabit Ethernet necesitara en principio 3 medios de transmisión: onda larga (LW) láser en modo simple, fibra multimodo (conocido como 1000-base-LX) y onda corta (SW) láser en fibra multimodo (100-Base- SX). El 1000-Base-CX permite las transmisiones sobre cable de cobre apantallado de 150 ohms.

Se soportaran dos estándares de láser sobre fibra óptica 1000-Base-SX y 1000-Base-LX. Los láser de onda corta y onda larga utilizaran fibra multimodo.

La primera se ha usado para Ethernet, Fast Ethernet y tráfico de backbone FDDI: sin embargo, esta tipo de fibra tiene un ancho de banda menor, especialmente con láser de onda corta. Esto significa que el láser de onda corta sobre 62.5 milímetros podrán atravesar distancias mas cortas que los láser de onda larga. Las fibras de 50 mm tienen características muy superiores de ancho de banda y serán capaces de atravesar distancias mas largas en comparación a las fibras de 62.5mm.

Para recorridos cortos Gigabit Ethernet permitirá la transmisión sobre un cable especial de 150 ohms. Este es un nuevo tipo de cable apantallado; no es UTP ni tipo 1 o 2 IBM. Para minimizar cuestiones de seguridad e interferencias causadas por las diferencias de voltaje, tanto transmisores como receptores compartirán un

espacio común. La perdida de retorno para cada conector es limitada a 20 db para minimizar las distorsiones de la transmisión.

La especificación PMD (Physical Médium Dependent) de fiber channel actualmente permite la transmisión de 1.062 baudios en half duplex. Gigabit Ethernet incrementara esta tasa de transmisión a 1.25 Gbps. [38]

La interfase de GBIC le permite a los administradores de red configurar cada puerto Gigabit sobre bases puerto a puerto para láser de onda corta y onda larga, así como para intereses físicas de cobre. Tal como se muestra en la figura 2.6

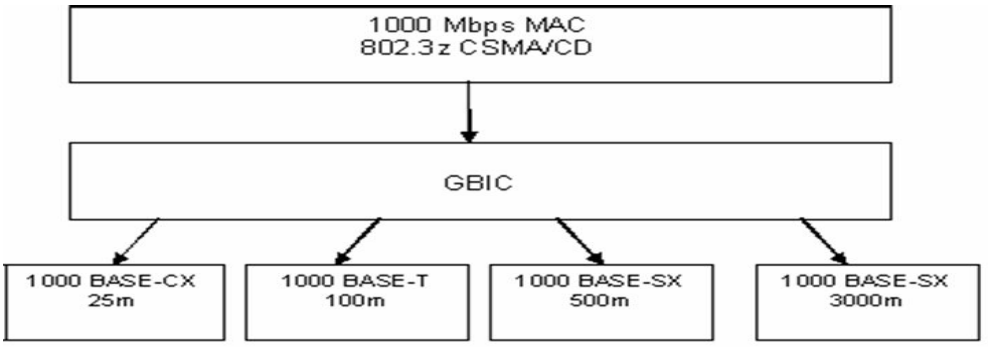


Figura 2.6 Interface GBIC

2.7.1.2 Nivel MAC

El nivel MAC de Gigabit Ethernet es similar ale estándar Ethernet y al Fast Ethernet. Soportara tanto transmisión Full-duplex como Half-duplex.

Las características de Ethernet, tales como detección de colisiones, máximo diámetro de red, reglas de repetición y otras, serán las mismas para Gigabit Ethernet.

El soporte para half-duplex, se utilizara CSMA/CD para asegurar que las estaciones se pueden comunicar por un solo cable y que se puede llevar a cabo la recuperación de colisiones.

La implementación de CSMA/CD para Gigabit Ethernet será la misma que para Fast Ethernet, permitirá la creación de Gigabit Ethernet compartidos vía bus o conexiones half-duplex punto a punto.

La limitación actual de Gigabit Ethernet será de 50 metros como máximo para cableados con cobre entre estaciones con un solo repetidor en el medio. La meta del comité de estandarizaciones es incrementar dicha distancia a 200 metros.

La aceleración de Ethernet a velocidades Gigabit, a creado algunos desafíos en términos de implementación de CSMA/CD. A velocidades mayores de 100 Mbps los tamaños mas chicos de paquetes son menores que el largo de spot time (bits). Slot time se define como la unidad de tiempo que utiliza Ethernet MAC para manejar colisiones. Para solucionar el problema de slot time, se agrego una extensión que agrega bits al frame relay hasta que este alcanza el mínimo slot-time requerido.

Full-duplex provee los medios para transmitir y recibir simultáneamente por un mismo cable. full-duplex es tipicamente usado entre endpoints, tales como entre switches, switches y servidores, switches y routers, etc. La transmisión full-duplex sera utilizada en Gigabit Ethernet para incrementar wl ancho de banda de 1Gbps a 2 Gbps para enlaces punto a punto, asi como para incrementar distancias posibles.

El uso de Ethernet full-duplex elimina colisiones en el cable, por lo tanto; CSMA/CD no necesita ser utilizado como control de flujo. EL estándar IEEE 802.3 formaliza la tecnología full-duplex y se espera que sea soportada por futuros productos de Gigabit Ethernet.

2.7.1.3 El nivel LLC

Define los servicios de acceso para protocolos que adhieren al modelo OSI. Desafortunadamente, muchos protocolos no obedecen las reglas de estos niveles. Por lo tanto se debe añadir información adicional al LLC para proveer la información relativa a estos protocolos. [39]

2.8 SMDS (Servicio de Conmutación de Datos de Megabits)

SMDS (Switched Multi-megabit Data Service, o "servicio de conmutación de datos de megabits"), es, más que una tecnología, un servicio completo.

SMDS permite una comunicación eficiente entre redes LAN, y al mismo tiempo es un servicio público, como las redes de área metropolitana (MAN), que podría sustituir al embrollo de redes privadas intercomunicadas con líneas punto a punto conectando routers remotos.

SMDS es una red WAN pública, que extiende los servicios de las redes LAN y MAN. Su objetivo primordial es el de proporcionar conectividad para MAN's, subredes FDDI, y redes LAN privadas, de modo que compartir los datos sea tan fácil como realizar una llamada telefónica, y soportando tanto datos como voz y vídeo.

2.8.1 Arquitectura de SMDS

Las primeras implementaciones de SMDS requerirán un acceso CPE (Customer Premise Equipment o Equipamiento Local de Usuario), por cada LAN del usuario, sustituto de los actuales routers. Posteriormente, se ofrecerá soporte de múltiples CPE, posiblemente mediante algún tipo de bus DQDB 802.6 (especificaciones MAN).

Las canales de entrada y salida SMDS, tendrán velocidades de 4, 10, 16, 25 y 34 Mbps., de modo que las velocidades SMDS se alinen con las velocidades de las LAN actuales (Token Ring, Ethernet y otras), eliminando así los cuellos de botella de los routers.

Se soportan paquetes de longitudes de hasta 9.188 bytes, así como direccionamiento de grupos y multicast.

Un elemento crucial de SMDS es la validación y "ocultación" de direcciones. Es decir, tienen que existir métodos válidos para autorizar y desautorizar las direcciones fuentes y destino. De este modo, se logra crear redes virtuales

privadas o VPN (Virtual Private Network), que facilitan enormemente el trabajo de usuarios y gestores de redes actuales.

SMDS esta distribuida en capas, igual que ATM. Las capas SMDS son denominadas Protocolo de Interfaz SMDS o SIP (SMDS Interface Protocol), y tienen funciones equivalentes a las de las capas ATM. Las capas SIP y sus PDU o Unidades de Datos de Protocolo (Protocol Data Unit) asociados, se alinean totalmente con sus equivalentes ATM. Asimismo, las diferentes capas del modelo OSI. [40]

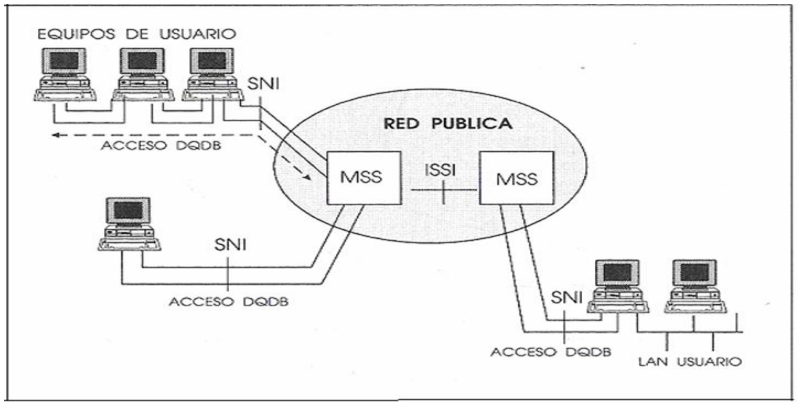


Figura 2.7 Red para servicios SMDS [41]

Los usuarios se conectan a la red con la interfaz SIN; (Subscriber Network Interface. El protocolo se denomina SIP, SMDS Interfese Protocol, que se basa en DQDB IEEE 802.6. Los demás elementos de la figura son MSS, MAN switching System e ISSI; Inter.-System Interface. [41]

Los servicios SMDS pueden ser proporcionados por un nodo de la red que incorpore ambas pilas de protocolos, los de la red local, y los SIP. Los servicios SMDS también pueden ser incorporados en routers o dispositivos similares.

SMDS es un servicio sin conexión, igual que las redes locales, que permitirá a cualquiera obtener servicios de interconexión entre red LAN, fácil y eficientemente a través de redes públicas.

Lo más importante es que, dado que SMDS es un servicio, los detalles de la red pueden ser desconocidos por el usuario, y ser proporcionados por una red de tecnología ATM o Frame Relay.

Algunos de los atributos requeridos a los servicios SMDS, para ser considerados como eficaces son: disponibilidad del 99,7% (menos de 26,3 horas de "down time" por año); recuperación en caso de caídas en menos de 3,5 horas; retraso en la red menor de 20 milisegundos para el 95% de los paquetes a velocidades DS-3; deben de producirse menos de 5 paquetes erróneos, cada 1013 paquetes transmitidos; y por último, menos de 1 paquete cada 104 no podrá ser entregado.[40]

Capítulo 3

Tendencias de protocolos en las redes de alta velocidad

Reseña:

En este capítulo se hace referencia al protocolo en especial como es IPv6 con su anterior versión de IPv4; también se describen algunas diferencias importantes entre estos como pueden ser formato de cabecera, seguridad entre otras.

El protocolo IP constituye el soporte vital de Internet. La versión anterior IPv4 ha sobrevivido sin apenas cambiar durante casi dos décadas; sin embargo, hace pocos años comenzaron a surgir problemas que no era capaz de gestionar adecuadamente, por lo que comenzó al trabajo hacia la próxima generación: IP Next Generation, hoy IPv6.

En los últimos años, Internet ha pasado de ser una red académica, a una red comercial. Esto, junto a la aparición y demanda de nuevos servicios, ha demostrado que el clásico IPv4 debía ser renovado para dar paso a un protocolo de nuestra generación, que ha resultado ser IPv6.

El crecimiento de la red de Internet es la principal causa que provoco la necesidad de una nueva generación IP. Si algo se aprendió de la utilización de IPv4, es que el direccionamiento y el encaminamiento deberán de ser capaces de manipulaciones razonables en escenarios de crecimiento futuro. [23]

3.1 IPv4 (Internet Protocol Versión 4)

El IP es un protocolo que pertenece al nivel de red, por lo que es utilizado por los protocolos de nivel de transporte como TCP para encaminar los datos hacia su destino. IP tiene la misión de encaminar el datagrama sin comprobar la integridad que contiene. Para ello se utiliza una nueva cabecera, que se antepone al datagrama que esta tratando. Suponiendo que ese protocolo TCP a sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructuras del mensaje una vez tratado quedaría así:

Cabecera IP (20 bytes)	**Cabecera TCP (20 bytes)**	**Datos**

La cabecera IP tiene un tamaño de 160 bits y esta formado por varios campos de distinto significado. Estos campos se ilustran en la figura 3.1 y son:

Versión	IHL	Tipo de servicio	Longitud total
Identificación		Flags	Fragmentación
Limite de existencia		Protocolo	Comprobación
Dirección de origen			
Dirección de destino			

Figura 3.1 Organización de la cabecera.

Versión: numero de versión del protocolo Ip utilizado. Tamaño: 4 bits**.**

Longitud de la cabecera:(Internet Header Length, IHL) especificas la longitud de la cabecera expresada en el numero de grupos de 32 bits y contiene. Tamaño: 4 bits.

Tipo de servicio: el tipo o QoS* se utiliza para indicar la prioridad o importancia de los datos que se envía, lo que condicionara la forma en que estos serán tratados durante la transmisión. Tamaño: 8 bits.

Longitud total: Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bits, el tamaño máximo del datagrama no podrá superar los 65.535 bytes; aunque en la práctica este valor será mucho más pequeño. Tamaño 16 bits.

Identificación: valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 bits.

Flags : Indicadores utilizados en la fragmentación. Tamaño: 3 bits.

Fragmentación: contiene un valor (offset) para poder ensamblar los datagramas que se hallan fragmentado. Esta expresado en numero de grupos de 8 bites (64 bits), comenzando con el valor 0 para el primer fragmento. Tamaño: 16 bits.

Limite de existencia: contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no deba descuidarse esta posibilidad. Tamaño: 8 bits.

Protocolo: el número utilizado en este campo, sirve para indicar a que protocolo pertenece al datagrama que se encuentra a continuación en la cabecera IP,
De manera que puede ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bits.

Comprobación: el campo de comprobación (check sum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia esta ampo no puede utilizarse para comprobar los datos incluidos a continuación, sino estos datos de usuario se comprobaran posteriormente a partir del campo de comprobación de la cabecera siguiente y que corresponden al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de cabecera, como puede ser el límite de existencia. Tamaño 16 bits.

Dirección de origen: contiene la dirección del host que envía el paquete. Tamaño: 32 bits.

Dirección de destinos: esta dirección es la del host que recibirá la información. Los routers o gateway intermedios deben conocerla para dirigir correctamente el paquete. Tamaño 32 bits.

3.1.1 Tipos de direccionamiento en IPv4

El protocolo IP identifica a cada maquina que se encuentra conectada a la red mediante su correspondiente dirección. Esta dirección, es un número de 32 bits que debe ser único para cada Host, y normalmente suele representarse como 4 cifras de 8 bits separadas por puntos.

La dirección de Internet (IP Adress) se utiliza para identificar tanto a la maquina en concreto, como a la red a la que pertenece, de manera que sea posible distinguir a las maquinas que se encuentran conectadas a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron 3 clases diferentes de direcciones:

Clase A: son la que en su primer byte tienen un valor comprendo entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para dada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir mas de dieciséis millones de maquinas en cada uno de las redes de esta clase.

Este tipo de direcciones son usadas por redes muy extensas, pero hay que tener en cuenta que solo puede haber 126 redes de este tamaño.

Clase B: Estas direcciones se utilizan su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso, el identificador de la red se obtiene de los primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254(no es posible utilizar los valores 0 y 255 por tener un significado especial. Los dos últimos bytes de la dirección constituyen el identificador del hots, permitiendo un numero máximo de 64516 maquinas en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el numero de maquinas que se necesiten conectar fuese mayor seria posible obtener mas de una dirección de “clase B” evitando de estas forma el uso de una de “clase A”.

Clase C: En este caso, El valor del primer Byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes por el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera, queda libre un byte para el host, lo que permite que se conecten un máximo de 254 maquinas en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas.

En al siguiente tabla se describen los campos de una dirección IP, así como también indica los números de redes y host que pueden existir en la red dependiendo en el tipo de clase a la que pertenezcan.

Clase	Primer Byte	Identificación De red	Identificación De hosts	Num. de redes	Num. de host
A	1-126	1 byte	3 byte	126	16,387,064
B	128-191	2 byte	2 byte	16,256	64,516
C	192-223	3 byte	1 byte	2,064,512	254

Tabla 3.1 Direcciones IP de Internet

El número de 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast, es cuando se quiere convertir el nombre por domino de una maquina a su correspondiente numero IP y no se conoce la dirección del servidor de nombres de domino mas cercano.

Lo usual, es que cuando se quiere hacer uso de broadcast, se utiliza una dirección compuesta por el identificador normal de la red y por el número 255 en binario para cada byte que identifique al host. Sin embargo, por conveniencia también se

permite el uso del numero 255. 255. 255.255. con la misma finalidad, de forma que resulte mas simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de diferentes formas, y por lo tanto, no siempre se encuentra disponible en las líneas punto a punto, no es posible enviar broadcast, pero si es posible hacerlo en las redes Ethernet, donde se supone que todas las maquinas prestaran atención a este tipo de mensajes.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (subredes). Como ejemplo podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bits. En este caso seria posible utilizar el tercer byte para indicar en que red Ethernet se encuentra un host en concreto. Esta división no tendrá ningún significado para cualquier otra maquina que este conectad a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho mas cómodo el acceso que si se tratar de varias direcciones de clase C independientes. [23]

3.1.2 Problemas de IPv4

A continuación se hace mención de algunos de los problemas que presenta el IPv4:

- **Escala:** Cada maquina presente en la red dispone de una dirección IP de 35 bits ello supone mas de cuatro mil millones de maquinas diferentes esta cifra es muy engañosa. El numero asignado a una maquina no es arbitrario sino que depende de una estructura mas o menos jerárquica, lo cual ocasiona que se desperdicie un enorme cantidad de direcciones.
- **Crecimiento de Internet:** es la capacidad de almacenamiento necesaria en las pasarelas y el tráfico de gestión precisa para mantener sus tablas de

encaminamiento. Existe un limite tecnológico al numero de rutas que un nodo puede manejar, y como dado que Internet crece mucho mas rápidamente que la tecnología que la mantiene, se observo que las pasarelas pronto alcanzaría su capacidad máxima y empezarían a desechar rutas, con lo que la red comenzaría a fragmentarse en subredes sin acceso entre si. Dado lo grave de la situación, se definió el CIDR* (Classless Inter-Domain Routing), con el que las pasarelas reducían el tamaño de sus tablas colapsando varias subredes con el mismo prefijo. Gracias a ello se ha ganado el tiempo, aunque solo sea postergado un problema inevitable.

- **Multiprotocolo:** Cada vez resulta mas necesaria la convivencia de diversa familias de protocolos como: IP, IPX; etc.; se necesitan mecanismos que permitan abstraer al usuario que la tecnología subyacente para permitir que concentre su atención en los aspectos realmente importantes de su trabajo. Se entiende hacia una red orientada a aplicaciones, que es con lo que el usuario interacciona; mas que a una red orientada a protocolos.
- **Seguridad:** es urgente definir unos mecanismos de seguridad en el nivel de red. Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en si, como la misma integridad de la red ante ataques mal intencionado o errores.
- **Tiempo real:** define una red pura orientada a datagramas y como tal, no existe el concepto de reserva de recursos. Cada datagrama debe compartir con los demás, el tiempo de transito en la red es muy variable y sujeto a congestión. A pesar de que en la cabecera IP hay un campo destinado a fijar, la prioridad del datagrama, en la práctica ello no supone ninguna garantía. Se necesita una extensión que posibilite el envió de tráfico en tiempo real, y así poder hacer frente a las nuevas demandas en esta campo.
- **Turificación:** Con una red cada día mas orientada hacia el mundo comercial, hace falta dotar al sistema de mecanismos que posibiliten el

análisis detallado del tráfico, tanto por motivos de facturación como para poder dimensionar los recursos que forma apropiada.

- **Comunicaciones móviles:** esta en auge y aun lo estará mas en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios.
- **La asignación de direcciones:** comenzó hacerse de manera centralizada por un único centro de registro (NIC) satisfaciendo casi todas las solicitudes sin necesidad de mayor trámite.

  Este modelo de asignación de direcciones, cuando Internet comenzó a crecer de forma espectacular, trajo algunas consecuencias:

  - **Mal aprovechamiento del espacio de direcciones**. Cada centro tendía a pedir una clase superior a la requerida, normalmente una clase B en vez de una o varia clases C, por puro optimismo en el crecimiento propio o por siempre vanidad.
  - **Peligro de agotamiento de las direcciones de clase B**. Las mas solicitadas debido a la escasez de posibilidades de elección. La alerta sonó cuando se había agotado el 30% de esta clase y la demanda crecía exponencial mente.
  - **Síntomas de saturación en los routers de los backbone**. Al imponerse restricciones severas en la asignación de clase B, las peticiones múltiples de clase C se hicieron masivas, lo que hizo que aumentara de forma explosiva el número de prefijos que los routers habían de mantener en sus tablas, llegándose a alcanzar los límites físicos impuestos por la capacidad de memoria y de proceso.
- **Políticas de enrutado:** Tradicionalmente los datagramas se han encaminado atendiendo a criterios técnicos tales como el minimizar el numero de saltos a efectuar, el tiempo de permanencia en la red, etc.

Cuando la red pertenece a una única organización, eso es ideal. Pero en el nuevo entorno económico en el que diferentes proveedores compiten por el mercado, las

cosas no son tan simples. Es imprescindible que la fuente pueda definir por que redes desean que pasen sus datagramas, atendiendo criterios de fiabilidad, costo, retardo, privacidad, etc. [23]

3.2 IPv6 (internet Protocol Versión 6)

La nueva versión de protocolo IP recibe el nombre de IPv6 aunque es también conocido comúnmente como IPng (Intenet Protocol Next Generation).Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión 4 no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior y además ofrece soporte a las nuevas redes de alto rendimiento (como ATM, Gigabyte, Ethernet, etc.).

Los criterio que se han seguido a los largo del desarrollo de IPv6 han sido fundamentales para obtener un protocolo sencillo y al mismo tiempo extremadamente consistente y escalable. Son de destacar entre estos criterios, la especial aptitud para ser soportado por plataformas existentes y una evolución que permite su uso concurrente con IPv4; no es necesario realizar un cambio instantáneo en una fecha determinada, sino que el cambio es transparente.

Estos criterios se han alcanzado en gran medida por la flexibilidad y simplificación de la cabecera de longitud fija, lo que redunda en la eficacia en su encaminamiento, tanto en pequeños routers como en los más grandes, con soportes de ancho de banda muy superiores a los 100 Gb con los dispositivos actuales.

IPv6 conserva varias de las características que contribuyen al éxito del IPv4, de hecho, los diseñadores han caracterizado al IPv6 como si fuera básicamente el mismo que el IPv4 con una cuantas modificaciones. Algo muy importante, es que IPv6 revisa completamente el formato de los datagramas, remplazando el campo de opción de longitud variable del IPv4 por una serie de encabezados de formato fijo.

Los cambios introducidos para el IPv6 pueden agruparse en cinco categorías:

1.- Direcciones mas largas

2.- Formato de encabezados flexibles

3.- Opciones mejoradas

5.- Soporte para asignación de recursos.

6.- Provisión para extinción de protocolo.

La característica más llamativa, es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bits, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituya uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal. [23]

3.2.1 Formato de la cabecera para IPv6

La única cabecera obligatoria es conocida como la cabecera IPv6. Tiene una longitud fija de 40 octetos, comparados con los 20 octetos de la parte obligatoria de la cabecera IPv4, sin embargo, la cabecera IPv6 tiene 8 campos, frente a los 13 campos de la cabecera de IPv4, con lo que el proceso en los encaminadotes es menor.

El tamaño de la cabecera que el protocolo IPv6 añade a los datos, es de 320 bits, el doble que IPv4. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado de la misma, debido a la innecesaria redundancia, mientras que otros, se han convertido en opcionales por medio de las extensiones. De esta manera, los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar del rendimiento en la transmisión. IPv6 puede contar con las siguientes cabeceras opcionales. De esta manera, los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar del rendimiento en la transmisión. IPv6 puede contar con las siguientes cabeceras opcionales

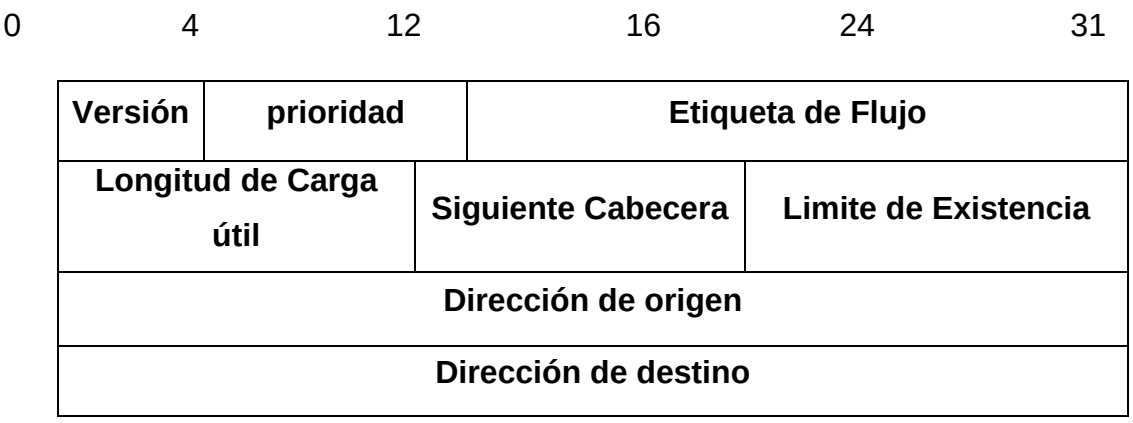


Figura 3.2 Formato de Cabecera de IPv6

En la figura 3.2 se representa la cabecera fija de IPv6, que consta de los siguientes campos:

Versión: tiene una longitud de 4 bits. Indica el número de la versión del Ip (valor 6).

Clase de tráfico: Tiene una longitud de 8 bits. Indica prioridad. Equivale al campo DS de Servicios Diferenciados. Permite diferenciación de tráfico posibilidad de descarte en caso de congestión.

Etiqueta de flujo. Tiene una longitud de 20 bits, puede ser utilizado por un nodo para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red.

Longitud de la carga útil. Tiene una longitud de 16 bits. Indica la longitud del resto del paquete IPv6 excluida la cabecera, en octetos. Representa la longitud total de todas las cabeceras adicionales mas la PUD (unidad de datos de protocolo) de la capa de transporte.

Próxima cabecera. Tiene una longitud de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.

Limite de saltos. Tiene una longitud de 8 bits. Indica el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado. Se decrementa en 1 de cada nodo que reenvía el paquete.

Dirección fuente. Tiene una longitud de 128 bits. Indica la dirección del productor del paquete.

Dirección destino. Tiene una longitud de 128 bits .indica la dirección de destino deseado del paquete. Puede que este no sea en realidad el ultimo destino deseado si esta presente la cabecera de encaminamiento.

3.2.2 Direcciones en IPv6

Las direcciones de IPv6 tienen una longitud de 128 bits. Las direcciones se asignan a interfaces individuales en los nodos, no a los nodos mismos. Una única interfaz puede tener múltiples direcciones monodestino. Cualquiera de las direcciones monodestrino asociadas a alas interfaces de los nodos se puede utilizar para identificar de forma univoca al nodo.
El primer campo de cualquier dirección IPv6 es el “prefijo de formato” de longitud variable, que identifica diferentes categorías de direcciones.

IPv6 permite tres tipos de direcciones:

Undistribucion (unicast)

Un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.

Monodistribucion (anycast)

Un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodistribucion se entregan una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia del protocolo de encaminamiento).

Multidistribición (multicast)

Un identificador para un conjunto de interfaces (normalmente pertenece a diferentes nodos). Un paquete enviado a una dirección multidistribucion se entrega a todas las interfaces identificadas por esa dirección.

3.2.3 Cabeceras adicionales de IPv6

En la nueva versión, ciertas informaciones complementarias se codifican en cabeceras que deben colocarse en el paquete entre la cabecera IPv6 y la cabecera del nivel de transporte. Hay un pequeño número de extensiones a la cabecera IPv6 (cada una de ellas identificada por un valor Próxima cabecera distinto). Un paquete IPv6 puede contener ninguna, una o varias cabeceras suplementarias.

Salvo excepciones, las cabeceras suplementarias apenas son examinadas o manipuladas por los nodos alcanzados por el paquete a lo largo de su camino hasta que este llega al nodo (o a cada grupo de nodos en el caso del *multicast)* identificados por el campo dirección de destino de la cabecera *IPv6.* En este momento se trata la primera cabecera suplementaria, o la cabecera de transporte en el caso de no haber cabeceras suplementarias. El contenido de cada cabecera determinará si es necesario tratar la cabecera siguiente.

La única excepción es la cabecera nodo por nodo *(Hop-by-Hop),* que lleva información que deberá ser examinada por los nodos de la red. Cuando está presente, tiene que seguir inmediatamente a la cabecera *IPv6.*

Cada cabecera suplementaria es de una longitud de un múltiplo de 8 octetos, para conservar una alineación de 8 *bytes* en las cabeceras suplementarias.

Cuando hay más de una cabecera suplementaria en un mismo paquete, las cabeceras deben aparecer en el orden siguiente:

Cabecera *IPv6* **(IPv6 Header).**
Cabecera nodo por nodo (**Hop-by-Hop Header).**
Cabecera de encaminamiento **(Routing Header).**
Cabecera de fragmentación **(Fragrnent Header).**
Cabecera de autentificación **(Authentication Header).**
Cabecera de confidencialidad **(Privacy Header).**
Cabecera de extremo a extremo **(End-to-End Header).**
Cada tipo de cabecera debe aparecer una sola vez en el paquete (excepto en el caso de un encapsulado *IPv6* en *IPv6,* donde cada cabecera *IPv6* encapsulada debe estar seguida por su propia cabecera suplementaria).

Cabecera nodo por nodo

La cabecera nodo por nodo contiene informaciones analizadas por los distintos nodos del camino seguido por el paquete. Se identifica por el valor del campo Próxima cabecera igual a 0, y tiene el formato siguiente:

next header	hdr ext len	options

- Next Header (8 *bits).* Identifica el tipo de cabecera que sigue inmediatamente a ésta.

- Hdr Ext Len. Indica la longitud de la cabecera nodo por nodo en múltiplos de 8 octetos (sin contar los ocho primeros).

- Options. Este campo contiene una o varias opciones codificadas en TLV (Type Length Value). Es de longitud variable en múltiplos de 8 octetos.

Cabecera de encaminamiento

La cabecera de encaminamiento es utilizada por el emisor *IP* para establecer una lista de nodo(s) intermedio(s) (o topología de *clusters)* que deberá seguir el paquete para llegar a su destino. Esta forma particular de cabecera de encaminamiento está diseñada para soportar el protocolo de encaminamiento a petición del emisor (Source Demand Routing Protocol, SDRP).

<table>
<tr><td>next header</td><td>routing type</td><td>mre</td><td>f</td><td>reserved</td><td>source route length</td></tr>
<tr><td>next hop pointer</td><td colspan="5">strict/loose bit mask</td></tr>
<tr><td colspan="6">source route</td></tr>
</table>

- Next Header. Identifica el tipo de cabecera que sigue inmediatamente a ésta.

- Routing Type. Indica el tipo de encaminamiento soportado por esta cabecera. Su valor es 1.

- MRE (Must Report Errors). Si este *bit* está a 1 y un encaminador no puede emitir correctamente la lista *Source Route,* el encaminador genera un mensaje de error *ICMP.* En el caso de que el *bit* esté a 0, no generara este mensaje de error.

- F (Failure of Source Route Behavior). Si este *bit* está a 1, indicará que si un encaminador no puede enviar más lejos un paquete, como se especifica en el *Source Route,* el encaminador fijará el valor del campo *Next Hop Pointer* con el valor del campo *Source Route Length.* De esa forma, el destino siguiente del paquete estará basado únicamente en la dirección del campo *Destination Address* (en el caso de que el bit estuviera a 0, el encaminador destruirá el paquete).

- Reserved. Inicializado a 0 por el emisor, es ignorado por el receptor.

- Source Route Length. Es el número de elementos o nodos que hay en una cabecera de encaminamiento *SDRP.* La longitud de esta cabecera puede calcularse a partir de este valor *(Iongitud=SrcRouteLen* 16+8).* Este campo no debe exceder el valor 24.

- Next Hop Pointer. Apunta a los elementos o nodos que hay que alcanzar. Se inicia a 0 para apuntar al primer elemento o nodo del *Source Route.* Cuando es igual al campo *Source Route Length,* significa que el *Source Route* está terminado.

- StricT/Loose Bit Mask. Este campo se utiliza para que un nodo opte por un camino. Si el valor de *Next Hop Pointer* es *N,* significa que el *N-ésimo bit* del *Strict/Loose Bit Mask* está a 1 (indica que el siguiente nodo es un nodo *Strict Source Route Hop),* mientras que si está a 0, el siguiente nodo es un *Loose Route Hop.*

- Source Route. Es una lista de direcciones *IPv6* que indica el camino que debe seguir el paquete. Puede contener un conjunto de direcciones de tipo *unicast* y *cluster.*

Cabecera de fragmentación

La cabecera de fragmentación es utilizada por el emisor *IP* para mandar paquetes de un tamaño superior a la que se puede enviar a los destinatarios. A diferencia de *IPv4,* la fragmentación es ejecutada únicamente por los nodos origen y no por los encaminadores que intervengan en el recorrido. La cabecera de fragmentación se distingue por un valor del campo *Next Header* igual a 44, el cual se encuentra justo después de la cabecera anterior.

next header	reserved	fragment offset	reserved	m
identification				

- Next Header. Identifica el tipo de la cabecera que sigue inmediatamente a ésta.

- Reserved. Inicializado a 0 por el emisor, es ignorado por el receptor.

- Fragmentation Offset. Indica la posición del primer octeto del datagrama total (es decir, de todo el datagrama, sin fragmentar). El primer fragmento estará en el lugar número 0. El valor de este campo es un múltiplo de 8 octetos.

- Reserved. Inicializado a 0 por el emisor, es ignorado por el receptor.

- M. Si este *bit* está a 1, significa que quedan uno o más fragmentos. En caso contrario, indica que no queda ninguno.

- Identification. Es un valor asignado al paquete de origen que es diferente de los demás paquetes fragmentados recientemente con la misma dirección fuente, la misma dirección destino y el mismo valor del campo *Next Header.* Permite identificar el datagrama para asegurar el reensamblaje de los paquetes. El número de identificación está contenido en la cabecera de todos los fragmentos.

Cabecera de autentificación.

La cabecera de autentificación es utilizada para autentificar y asegurar la integridad de los paquetes. La cabecera de autentificación viene determinada por el valor 51 del campo *Next Header.*

next header	authentication data length	reserved
security association id		
authentication data		

- Next Header. Identifica el tipo de cabecera que sigue inmediatamente a ésta. Los valores son idénticos a los del campo Protocol de *IPv4.*

- Authentication Data Length. Es la longitud del *Authentication Data* en múltiplos de 8 octetos.

- Reserved. Inicializado a 0 por el emisor, es ignorado por el receptor.

- Security Association ID. Se combina con la dirección fuente para identificar al (o a los) destinatario(s) el tipo de seguridad establecido.

- Authentication Data. Muestra información sobre el algoritmo que se ha de utilizar para autentificar el origen del paquete y para asegurar su integridad con respecto al tipo de seguridad asociado. La longitud de este campo es variable y múltiplo de 8 octetos.

Cabecera de confidencialidad.

La cabecera de confidencialidad se utiliza para evitar el acceso no autorizado al paquete, encriptando los datos y colocándolos en la parte correspondiente de la cabecera de confidencialidad. Dependiendo de las exigencias de seguridad del usuario.

Se podría encriptar la trama del nivel de transporte *(UDP* o *TCP)* o el datagrama entero. Este enfoque con encapsulado es necesario para asegurar una confidencialidad completa del datagrama original. Si está presente, la cabecera de confidencialidad es siempre el último campo no encriptado de un paquete. Esta cabecera funciona entre estaciones, entre una estación y *un* firewall o entre *dos* firewalls*.*

security association identifier		
initialization vector		
next header	length	reserved
protected data		
trailer		

- Security Association Identifier (SAID). Identifica el tipo de seguridad del datagrama. Si no se ha establecido ninguna asociación de seguridad, el valor de este campo será 0x0000. Una asociación de seguridad es unilateral, por ello, una comunicación confidencial entre dos estaciones debe tener normalmente dos *SAID* (uno para cada uno de los sentidos). La estación de destino utiliza la combinación del valor del *SAID* y de la dirección fuente para distinguir la asociación correcta.

- Initialization Vector. Este campo es opcional, y su valor depende del *SAID* utilizado.

- Next Header. Va encriptado e identifica el tipo de la cabecera que sigue inmediatamente a ésta. Los valores son idénticos a los del campo Protocol de *IPv4.*

- Reserved. Va encriptado y es ignorado por el receptor.

- LENGTH. Va encriptado e indica la longitud de la cabecera codificada (es un múltiplo de 8 octetos) y no incluye los 8 primeros octetos.

- Protected Data. Va encriptado y puede contener encapsulado un datagrama *IPv6* completo, una secuencia de opciones *IPv6* y, por último, el paquete del nivel de transporte.

- Trailer. Va encriptado y se utiliza para hacer de relleno (necesario en algunos algoritmos) o para registrar datos de autentificación utilizados en un algoritmo de criptografía que proporcione confidencialidad sin autentificación. Este campo está presente únicamente si el algoritmo lo necesita.

Cabecera de extremo a extremo

La cabecera de extremo a extremo da una información opcional que debe ser controlada por el (o los) nodo(s) destinatario(s) del paquete*. Es identificada por un valor del campo *Next Header* del *TBD,* que sigue inmediatamente a la cabecera previa y tiene el mismo formato que la cabecera de opciones nodo por nodo, a excepción de la capacidad de excluir una opción de cálculo de la integridad de autentificación.[22]

3.3 Diferencias más importantes entre el formato IPv6 y el IPv4

IPv4 presenta algunas limitaciones en en las redes actuales: Saturación de direcciones ip, Limita el crecimiento de Internet, Obstaculiza el uso de Internet a nuevos usuarios, No fue diseñado para ser seguro, Las nuevas aplicaciones son mas demandantes

Las cabeceras de los paquetes han sido simplificadas en IPv6, eliminando los campos no utilizados, y añadiendo el concepto de cabeceras de extensión. Estas permiten seleccionar facilidades especiales de encaminamiento, fragmentación y seguridad. Así como el manejo de opciones, que han sido eliminadas de la cabecera IPv6. Cada cabecera incluye un campo que define el tipo de cabecera que le sigue a continuación, hasta llegar a la de transporte, con lo que se agiliza el proceso de los paquetes.

En IPv6, la fragmentación / ensamblado de paquetes, es una tarea de los sistemas finales, con lo que de nuevo se facilita la vida a los routers para que se entreguen a su misión primordial: encaminar paquetes. La unidad máxima de transmisión (MTU) de un enlace, es ahora como mínimo de 576 octetos (64 en IPv4).

El encaminamiento propuesto por IPv6 permitirá seleccionar en el origen, los nodos intermedios por los que van pasando los paquetes mediante el empleo de cabeceras de extensión (routing header). En ésta cabecera, se especificará un cambio que será recorrido a la inversa al regreso, mediante direcciones unicast o anycast.

La transmisión de información en tiempo real, se podrá realizar mediante el empleo de dos campos en la cabecera IPv6.

La prioridad o flor label, que distingue los diferentes tipos de datagramas según la clase de servicio, la etiquita de flujo y la clase de tráfico, que permite diferenciar y asignar distintos estados a distintos flujos originados por la misma fuente.

La seguridad en el nivel será una realidad mediante el empleo de cabeceras de extensión de autentificación, que proporciona servicios de verificación de identidad e integridad y de encapsulado de seguridad que proporciona servicios de confiabilidad. Estas dos extensiones de cabecera son:

- **AH.** Autentication Header , protege de encaminamiento incorrecto de fuente y de ataque a la maquina central. No existe problema de exportación de tecnología por tratarse de un procedimiento de verificación (se cifra una función del contenido, pero no del contenido en si).

- **ESP.** Encapsulation Security Payload. DES: Data Encryption Standard. En éste caso, si existen problemas de exportación con lo algoritmos de encriptación. [22]

Capítulo 4

Caso práctico: red de alta velocidad de ciudad universitaria de la UAEH

Reseña:

En este capítulo analizaremos algunos de los componentes y tecnologías relacionados con redes de alta velocidad, aplicados en la red de ciudad universitaria de la UAEH.

4.1 Servicio de Internet en ciudad universitaria

La red de telecomunicaciones de la Ciudad Universitaria se basa Internet de alta velocidad (Internet 2). El Internet de alta velocidad es una necesidad hoy día, debido al crecimiento explosivo de usuarios en los últimos años, así como a la necesidad creciente de transmitir información de audio y video. El Internet de alta velocidad utiliza un tipo de transmisión de gran ancho de banda llamado Broadband y es capaz de combinar voz, datos y video. Algunas tecnologías que permiten la conexión a Internet de alta velocidad son: la conexión por sistema de cable, el servicio DSL*, conexión por fibra óptica y vía satélite. Las velocidades de transmisión en estas tecnologías van desde 2 hasta más de 27 veces la velocidad actual de Internet. Este Internet es suministrado por Avantel en un enlace dedicado E3 [43]

4.2 Tipo de Red (VLAN) en ciudad universitaria

El tipo de la red de telecomunicaciones de la Ciudad Universitaria es una Red de Área Local Virtual (VLAN). Las virtual LAN están estrechamente relacionadas con el trabajo en grupo. Las VLAN unen lógicamente usuarios separados físicamente para formar parte de uno o múltiples grupos de trabajo, eliminando las limitaciones físicas y en un único entorno propio al grupo. Además, proporcionan seguridad y protección en los envíos de información entre los miembros de cada grupo de trabajo dentro de cada red virtual. De este modo, los empleados de los diferentes departamentos consiguen un óptimo tiempo de respuesta dentro de su grupo o con otros departamentos de la corporación, evitando problemas de inseguridad.

La formación de grupos lógicos consigue también solventar los problemas de tramos de red congestionados por exceso de tráfico ajeno al grupo *(broadcast* de toda la organización, tramos no aislados que pueden ser filtrados, etc.) permitiendo aprovechar el ancho de banda. El administrador de la red también obtendrá ventajas, ya que la red puede ser transformada de una forma más sencilla, se reducen los costos de añadir, cambiar o eliminar usuarios y podrá

controlar y optimizar el ancho de banda. [22]

Los objetivos de la VLAN de Cuidad Universitaria es conseguir que:

- Integren usuarios remotos móviles.
- Den seguridad y flexibilidad a los grupos virtuales de trabajo.
- Permitan el más alto rendimiento en todos los nodos de la red corporativa.
- Logren organizaciones más flexibles.
- Eliminen limitaciones geográficas al 'crear grupos virtuales de trabajo en toda la red.
- Permitan añadir, eliminar o cambiar usuarios vía software.

4.2.1 Funcionamiento de la VLAN de ciudad universitaria

La VLAN de Ciudad Universitaria se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de switch se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten broadcasts. Los puertos que no pertenecen a esa VLAN no comparten esos broadcasts. Esto mejora el desempeño de la red porque se reducen los broadcasts innecesarios. Las VLAN de asociación estática se denominan VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

Los usuarios conectados al mismo segmento compartido comparten el ancho de banda de ese segmento. Cada usuario adicional conectado al medio compartido significa que el ancho de banda es menor y que se deteriora el desempeño de la red. La VLAN por defecto para cada puerto del switch es la VLAN de administración. La VLAN de administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el switch. Todos los demás puertos en el switch pueden reasignarse a VLAN alternadas.

En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema

conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN. Ver Figura 4.1

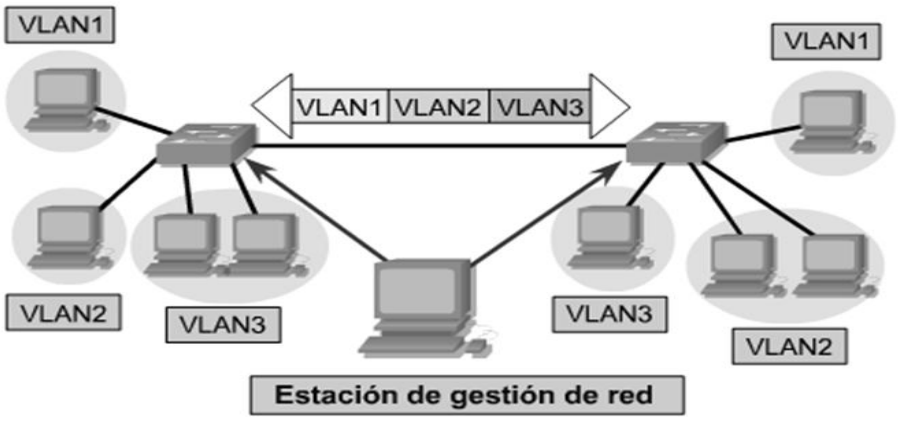


Figura 4.1 Segmentación de una VLAN

Los administradores de red son responsables por configurar las VLAN de forma estática y dinámica. En nuestro caso de estudio ocuparemos la estática.

- **Estáticamente.** Los administradores de la VLAN de cuidad universitaria configuran puerto por puerto. Cada puerto esta asociado a un VLAN especifica el administrador de red es responsable de escribir las asignaciones entre lo puertos y las VLAN
- **Dinámicamente.** Los puertos pueden calcular su configuración de VLAN. Se usa una base de datos de software que contiene un mapeo de direcciones MAC a VLAN, que el administrador de red tiene que configurar de nuevo.

Los puentes filtran el tráfico que no necesita ir a los segmentos, salvo el segmento destino. Si una trama necesita atravesar un puente y la dirección MAC destino es conocida, el puente sólo envía la trama al puerto de puente correcto. Si la dirección MAC es desconocida, inunda la trama a todos los puertos en el dominio

de broadcast, o la VLAN, salvo el puerto origen donde se recibió la trama. Los switches se consideran como puentes multipuerto.

- Existen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete y la de nuestro caso de estudio ocupa la basada en puerto:
- VLAN basadas en puerto

    - Método de configuración mas común
    - Los puertos se asignan individualmente, en grupos, en filas o en dos o mas switches
    - Uso sencillo
    - Se implementa a menudo donde el Protocolo de Control de Host Dinámico se usa para asignar direcciones IP a los Host de red.

4.2.2 Ventajas de la VLAN de ciudad universitaria

La VLAN de ciudad universitaria permite que los administradores organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores realicen varias tareas:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

4.2.3 Algunos problemas de la VLAN de ciudad universitaria

Algunos problemas recurrentes en la VLAN de ciudad universitaria se deben un crecimiento de la demanda de servicios por parte de puertos de estación de trabajo que excede los recursos de configuración, enlace troncal o capacidad para acceder a los recursos de servidor. Por ejemplo, el uso de tecnologías de Web y aplicaciones tradicionales, como la transferencia de archivos y correo electrónico,

provoca un crecimiento en el tráfico de red que las redes de las empresas deben manejar.

Muchas LAN de campus se enfrentan a patrones de tráfico de red impredecibles resultantes de la combinación de tráfico de intranet, menos ubicaciones de servidor de campus centralizadas y el uso creciente de aplicaciones multicast. La exploración de Web interna ahora permite que los usuarios localicen y accedan a la información desde cualquier lugar en la intranet corporativa. Los patrones de tráfico están determinados por la ubicación de los servidores y no por las configuraciones del grupo de trabajo físico con el que se agrupan. Si una red presenta con frecuencia síntomas de cuello de botella, como desbordes excesivos, tramas descartadas y retransmisiones, es posible que haya demasiados puertos en un solo enlace troncal* o demasiados requerimientos de recursos globales y acceso a los servidores de intranet.

Los síntomas de cuello de botella también pueden producirse porque la mayor parte del tráfico se ve obligado a atravesar el backbone. Otra causa puede ser que el acceso de "cualquiera a cualquiera" es común, cuando los usuarios utilizan los recursos corporativos basados en Web y aplicaciones multimedia. En este caso, puede resultar necesario tener en cuenta el aumento de los recursos de la red para satisfacer la demanda creciente. [44]

4.3 Protocolos que utilizan en ciudad universitaria

La red de telecomunicaciones de Cuidad universitaria utiliza el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas.

TCP. El TCP es el responsable de la transmisión fiable de datos desde un nodo a otro.

IP. El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento.

Entre otros protocolos escritos específicamente para el conjunto TCP/IP y que son muy utilizados para la VALN de cuidad universitaria se incluyen:

- **SMTP** (Protocolo básico de transferencia de correo). Correo electrónico.
- **FTP** (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.
- **SNMP** (Protocolo básico de gestión de red). Para la gestión de redes.

Además de los anteriores tenemos algunos otros para realizar tareas especificas dentro de la VLAN de cuidad universitaria.

Protocolo de resolución de direcciones (ARP)

Este protocolo en especial lo tiene configurado todos los componentes de cisco que se ocupan en la VLAN de cuidad universitaria como son ruteadores, switchs etc. Antes de enviar un paquete IP a otro host se tiene que conocer la dirección hardware de la máquina receptora. El ARP determina la dirección hardware (dirección MAC) que corresponde a una dirección IP. Si ARP no contiene la dirección en su propia caché, envía una petición por toda la red solicitando la dirección. Todos los hosts de la red procesan la petición y, si contienen un valor para esa dirección, lo devuelven al solicitante. A continuación se envía el paquete a su destino y se guarda la información de la nueva dirección en la caché del router.

Protocolo de mensajes de control de Internet (ICMP)

Este protocolo permite a los administradores de red de la VALN de cuidad universitaria el reconocimiento de una estación para saber si esta activa o no y

esto se realiza mediante el comando ping. El ICMP es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo. Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Si el flujo de datos es demasiado rápido para un router, pide a los otros routers que reduzcan la velocidad de transmisión.

Los dos tipos básicos de mensajes ICMP son el de informar de errores y el de enviar preguntas.

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo no orientado a la conexión y es el responsable de la comunicación de datos extremo a extremo. En cambio, a diferencia de TCP, UDP no establece una conexión. Intenta enviar los datos e intenta comprobar que el host de destino recibe los datos. UDP se utiliza para enviar pequeñas cantidades de datos que no necesitan una entrega garantizada. Aunque UDP utiliza puertos, son distintos de los puertos TCP; así pues, pueden utilizar los mismos números sin interferirse. [1]

4.4 Tecnologías de transmisión de ciudad universitaria

La red de telecomunicaciones de la Ciudad Universitaria se basa en un backbone de fibra óptica con tecnología Gigabit Ethernet, así como equipos terminales Fast Ethernet que conectan a los usuarios distribuidos en todas las escuelas e institutos de la universidad que a continuación se desglosan cada una de ellas:

4.4.1 Envío de datos en ciudad universitaria

En la red Ethernet de ciudad universitaria, cuando un dispositivo envía datos, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC destino. El dispositivo origen adjunta un encabezado con la dirección MAC del destino y envía los datos a la red. A medida que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección destino física que transporta la trama

de datos. Si no hay concordancia, la NIC descarta la trama de datos. Cuando los datos llegan al nodo destino, la NIC hace una copia y pasa la trama hacia las capas superiores del modelo OSI. En una red Ethernet, todos los nodos deben examinar el encabezado MAC aunque los nodos que están comunicando estén lado a lado.

La NIC utiliza la dirección MAC para evaluar si el mensaje se debe pasar o no a las capas superiores del modelo OSI. La NIC realiza esta evaluación sin utilizar tiempo de procesamiento de la CPU permitiendo mejores tiempos de comunicación en una red Ethernet.

Todos los dispositivos conectados a la LAN de Ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, routers y switches

Todos los estándares son básicamente compatibles con el estándar original de Ethernet. Una trama de Ethernet puede partir desde una antigua NIC de 10 Mbps de cable coaxial de un PC, subir a un enlace de fibra de Ethernet de 10 Gbps y terminar en una NIC de 100 Mbps. Siempre que permanezca en redes de Ethernet, el paquete no cambia. Por este motivo, se considera que Ethernet es muy escalable.

¿Porque se utiliza Ethernet en la red de Cuidad Universitaria?

- Sencillez y facilidad de mantenimiento.
- Capacidad para incorporar nuevas tecnologías.
- Confiabilidad
- Bajo costo de instalación y de actualización.
- Con la llegada de Gigabit Ethernet, lo que comenzó como una tecnología LAN ahora se extiende a distancias que hacen de Ethernet un estándar de red de área metropolitana (MAN) y red de área amplia (WAN).

4.4.1.1 La tecnología Ethernet de cuidad universitaria donde opera en el modelo OSI

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física. Ver figura 4.6

Figura 4.2 Ethernet y el Modelo OSI

Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y comunicación con el computador. La subcapa MAC trata los componentes físicos que se utilizarán para comunicar la información. La subcapa de Control de Enlace Lógico (LLC) sigue siendo relativamente independiente del equipo físico que se utiliza en el proceso de comunicación.

4.4.1.2 Control de acceso al medio (MAC) de ciudad universitaria

MAC se refiere a los protocolos que determinan cuál de los computadores de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la Capa 2 del modelo OSI. Tanto MAC como LLC son subcapas de la Capa 2. Hay dos categorías amplias de Control de acceso al medio: determinística (por turnos) y la no determinística (el que primero llega, primero se sirve).

Los protocolos MAC no determinísticos utilizan el enfoque de "el primero que llega, el primero que se sirve". CSMA/CD es un sistema sencillo. La NIC espera la ausencia de señal en el medio y comienza a transmitir. Si dos nodos transmiten al mismo tiempo, se produce una colisión y ningún nodo podrá transmitir.

Las tecnologías específicas para cada una son las siguientes:

Ethernet: topología de bus lógica (el flujo de información tiene lugar en un bus lineal) y en estrella o en estrella extendida física (cableada en forma de estrella) como la de Cuidad Universitaria.

Como funciona CSMA/CD en ciudad universitaria

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

- Transmitir y recibir paquetes de datos
- Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI
- Detectar errores dentro de los paquetes de datos o en la red

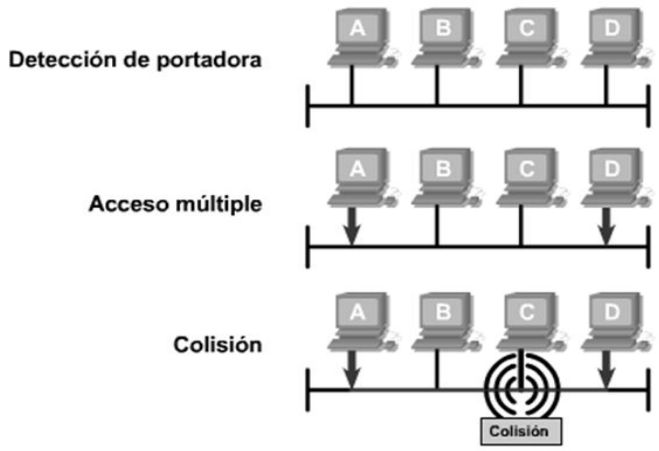


Figura 4.3 Funciones de CSMA/CD

En el método de acceso **CSMA/CD**, los dispositivos de networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo determinado al azar antes de reintentar. Si el nodo determina que el medio de networking no está ocupado, comenzará a

transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar.

Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo. Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de networking. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

4.4.1.3 Arquitectura ocupada en ciudad universitaria de Fast Ethernet

Los enlaces de Fast Ethernet generalmente consisten en una conexión entre la estación y el concentrador o switch. Los concentradores se consideran repetidores multipuerto y los switches, puentes multipuerto. Estos están sujetos a la limitación de 100 m de distancia de los medios UTP. La tabla 4.1 muestra las distancias de cable de la configuración arquitectónica. Los enlaces de 100BASE-TX pueden tener distancias sin repetición de hasta 100 m. El amplio uso de switches ha hecho que las limitaciones de distancia sean menos importantes. Como la mayoría de Fast Ethernet está conmutada, estos representan los límites prácticos entre los dispositivos.

Arquitectura	**100BASE-TX**	**100BASE-FX**	**100BASE-TX Y FX**
Estación a estación Estación a switch, Switch a switch (Half ó full duplex)	**100 m**	**412 m**	**N/A**

Tabla 4.1 Distancia de cable en Ethernet

4.4.2 Arquitectura ocupada en ciudad universitaria de Gigabit Ethernet

Las limitaciones de distancia de los enlaces full-duplex están restringidas sólo por el medio y no por el retardo de ida y vuelta. Como la mayor parte de Gigabit Ethernet está conmutada, los valores de las tablas y son los límites prácticos entre los dispositivos. Las topologías de cadena de margaritas, de estrella y de estrella extendida están todas permitidas. El problema entonces yace en la topología lógica y el flujo de datos y no en las limitaciones de temporización o distancia.

DISTANCIAS DE CABLE MAXIMAS 1000 BASE- SX

MEDIO	Ancho de banda modal	Distancia máxima
Fibra multimodo 62.5 µm	160 Mbps	220 m
Fibra multimodo 62.5 µm	200	275 m
Fibra multimodo 50 µm	400	500 m
Fibra multimodo 50 µm	500	500 m

Tabla 4.2 Distancia de cable máximas 1000 BASE-SX

DISTANCIAS DE CABLE MAXIMAS 1000 BASE-LX

MEDIO	Ancho de banda modal	Distancia máxima
Fibra multimodo 62.5 µm	500 Mbps	550 m
Fibra multimodo 50 µm	400	550 m
Fibra multimodo 50 µm	500	550 m
Fibra multimodo 10 µm	N/A	5000 m

Tabla 4.3 Distancia de cable máximas 1000 BASE-LX

Un cable UTP de 1000BASE-T es igual que un cable de una 10BASE-T o 100BASE-TX, excepto que el rendimiento del enlace debe cumplir con los requisitos de mayor calidad de ISO Clase D (2000) o de la Categoría 5e.

No es recomendable modificar las reglas de arquitectura de 1000BASE-T. A los 100 metros, 1000BASE-T opera cerca del límite de la capacidad de su hardware para recuperar la señal transmitida. Cualquier problema de cableado o de ruido ambiental podría dejar un cable, que en los demás aspectos cumple con los

estándares, inoperable inclusive a distancias que se encuentran dentro de la especificación.

Se recomienda que todos los enlaces existentes entre una estación y un hub o switch estén configurados para Auto-Negociación para así permitir el mayor rendimiento conjunto. Esto evitará errores accidentales en la configuración de otros parámetros necesarios para una adecuada operación de Gigabit Ethernet. [44]

4.5 Cableado estructurado de ciudad universitaria

Un sistema de cableado da soporte físico para la transmisión de las señales asociadas a los sistemas de voz, telemáticos y de control existentes en un edificio o conjunto de edificios.

El sistema de cableado estructurado de la red de ciudad universitaria, es un sistema de cableado diseñado en una jerarquía lógica, que adapta todo el cableado existente y el futuro en un único sistema. Exige una topología en estrella que permite una administración sencilla y una capacidad de crecimiento flexible.

Este sistema permite identificar, reubicar, cambiar de forma racional los diversos equipos interconectados, basarse en normas de identificación de cables y componentes, además del empleo de conectores de las mismas características que tienen los equipos. Proporciona el medio físico para llevar al puesto de trabajo los servicios telemáticos y de comunicaciones (voz, datos y video), incorpora nuevos servicios sobre la red de distribución ya existentes y posibilita modificaciones internas sin que se pierda la eficacia. Permite utilizar una infraestructura común entre todos los sistemas de telecomunicaciones y planificar el cableado, ya que su vida útil ha de ser alrededor de los 10 años.

Una solución de cableado estructurado se divide en una serie de subsistemas, cada subsistema tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada para cada caso. Los distintos elementos que lo componen son:

- Repartidor de campus
- Cable de distribución de campus *(Backbone)*
- Repartidor principal o del edificio
- Cable de distribución de edificio *(Backbone)*
- Subrepartidor de planta
- Cable horizontal
- Punto de transición opcional
- Toma ofimática
- Punto de acceso o conexión

Las normas más comunes son las siguientes:

- **ANSI/EIA/TIA** (Instituto Nacional Americano para la Estandarización, Asociación de Industrias Electrónicas, .Asociación de Industrias de Telecomunicación).
- **ISO/IECO** (Organización Internacional de. Normas/Comisión Internacional de Electrónica)

En la siguiente tabla se muestran algunos estándares con su respectiva descripción:

ESTANDAR	DESCRIPCION
EIA/TIA568	Cableado Para edificios
EIA/TIA569	Canalización para equipos de telecomunicación
EIA/TIA570	Cableado para edificios residenciales
EIA/TIA606	Administración de infraestructura de telecomunicaciones
PN-2416	Cableado troncal de edificios residenciales
PN-3012	Cableado con fibra óptica
IS-11801	cableado estructurado de propósito general
EN-50098-3	Instalación de cable
EN-50098-4	Cableado estructurado de propósito general

Tabla 4.4 Estándares

Un estándar, es una colección de criterios, principios y guías que juntos forman un modelo base para construir y comparar sistemas.

Los estándares de red proporcionan la base para la transmisión de los datos, para la fabricación de los equipos de red compatibles, y para el diseño de sistemas operativos que se utilizan en una red, también definen el tiempo máximo que un paquete debe de tardar en viajar de un nodo a otro antes de determinar que el paquete no ha encontrado su destino, definen que hacer cuando un paquete se envía con falta de información y establecen cómo prevenir la confusión cuando se envían demasiados paquetes al mismo tiempo.

Las organizaciones más importantes que realizan los estándares para interconectar computadoras son: el Instituto Nacional Americano para la Estandarización *(ANSI),* el Instituto de Ingenieros Eléctricos y Electrónicos *(IEEE),* el Comité Consultivo sobre Telegrafía y Telefonía *(CCITT)* y la Organización Internacional de Estándares *(ISO).*

4.5.1 Ventajas del cableado estructurado en ciudad universitaria

Un sistema de cableado abierto, es un sistema de cableado estructurado que está diseñado para ser independiente del proveedor y de la aplicación a la vez.

Las características claves de un sistema de cableado estructurado abierto son:

- Todos los *outlets* (salidas para conexión) del área de trabajo son idéntica mente conectados en estrella a algún punto de distribución central.
- Puede aceptar cualquier necesidad de aplicación que pueda ocurrir a lo largo de la vida del cableado.

Éstas características del cableado estructurado abierto ofrecen principalmente tres ventajas:

- Como el. cableado es independiente del proveedor y de la aplicación, los cambios en la red y en el equipamiento pueden realizarse con los mismos

cables existentes.

- Debido a que los *outlets** están cableados de igual forma, los movimientos de personal pueden hacerse sin modificar la base de cableado.
- Un closet de telecomunicaciones, el cual permite que los problemas de cableado o de red sean detectados y aislados fácilmente sin tener que parar el resto de la red.

Para establecer un cableado estructurado, será necesario hacer hincapié en los siguientes puntos:

Definir un cableado horizontal en ciudad universitaria

- El cableado horizontal es siempre de cable par trenzado con conectores *RJ-45.*
- Definir los puestos de trabajo; de no existir ubicación, calcular un puesto de trabajo cada 10m² (2.5 m * 4 m).
- Definir el accesorio a utilizar (Caja, roseta).
- Definir la cantidad de conectores *RJ-45* por puesto de trabajo previsto (típico 2 conectores).
- Definir la canalización a usar en la llegada al área de trabajo.
- Definir la ubicación del armario de piso.
- Definir la cantidad de *UTP* por piso.
- Definir él panel de parcheo a utilizar (Número, de conectores ± del 15 - 20% de vacantes).
- Repetir por cada piso.

Definir un Backbone en ciudad universitaria

- Definir la cantidad de servicios (datos, control de alarmas, etc.).
- Definir el vínculo físico del backbone: UTP, coaxial, fibra óptica más vacantes, y la terminación del backbone..
- Definir el distribuidor de piso, el panel de parcheo tanto del piso como del panel para el backbone, los organizadores verticales y los organizadores

horizontales, sin olvidar el espacio libre para equipos, incluyendo el espacio vacante.

- Repetir para cada piso.

Definir el distribuidor de edificio

- Cuantificar la cantidad y el tipo de *Backbone.*
- Definir la terminación.
- Definir la construcción del distribuidor.
- Definir la conexión de tierra.

Definir el plan de la numeración

- Los cables deben identificarse en sus dos extremos como mínimo, de preferencia números romanos.
- Los conectores RJ 45 de puestos de trabajo deben numerarse e identificarse también en el panel de parcheo.
- Los cables de parcheo deben identificarse en ambos extremos.
- Se aconseja dejar junto a cada distribuidor toda la información posible (croquis de planta con la distribución de los puestos de trabajo, circulación de los tendidos de cables, cajas de paso, croquis del distribuidor con el destino de cada componente, etc.).

Recomendaciones que se utilizan para canalizaciones y ductos en ciudad universitaria

- Los cables *UTP,* no deben circular junto a cables de energía dentro de la misma canalización por muy corto que sea el trayecto; de igual modo, deberá evitarse el cruce de cables *UTP* con cables de energía.
- Los cables *UTP* pueden circular por bandeja compartida con cables de energía, respetando el paralelismo a una distancia mínima de 10 cm. En el caso de existir una división metálica puesta a tierra, ésta distancia se reduce a 7 cm.

- En el caso de pisoductos o caños metálicos, la circulación puede ser en conductos contiguos.
- Sí es inevitable cruzar un gabinete de distribución con energía, no debe circularse paralelamente a más de un lateral.
- De usarse canalizaciones plásticas; lubricar los cables para reducir la fricción entre éstos y las paredes de las canalizaciones, ya que ésta genera un incremento de la temperatura que aumenta la adherencia.
- El radio de las curvas no debe ser inferior a 2".
- Las canalizaciones no deben superar los 20 metros o tener más de 2 cambios de dirección sin cajas de paso.
- En tendido vertical, se deben fijar los cables a intervalos regulares para evitar el efecto del eco en el acceso superior.
- Al utilizar fijaciones (grapas, precintos o cinchos); no excederse en la presión aplicada (no arrugar la cubierta), ya que se puede afectar a los conductores internos. [46]

4.5.2 Componentes del cableado estructurado en ciudad universitaria

Cable de parcheo *(Patch Cord)* Están construidos con cable *UTP,* y tienen 1 conector en cada una de sus puntas. Es muy importante utilizar *PC* certificados puesto que al hacerlos en obra, no garantiza en modo alguno la certificación.

Canaleta (*Hinged Raceways)* Se utiliza para cubrir el cableado y de éste modo evitar que se dañe. Ver figura. 4.4

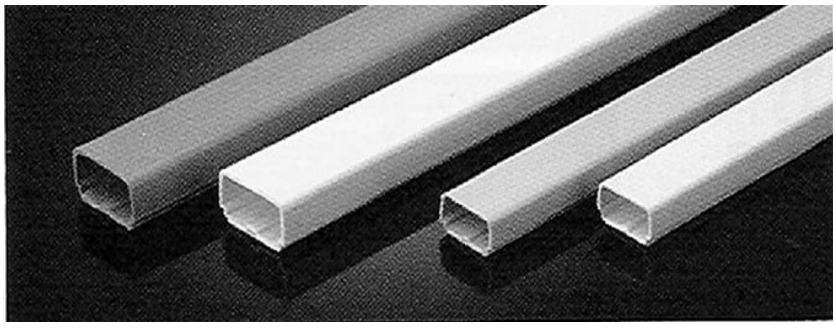


Figura 4.4 Canaleta

Conector *(jack)* Usualmente de dos conectores, aunque existe también la versión reducida de 1 boca. Posee un circuito impreso que soporta conectores *RJ-45*. Ver figura 4.5

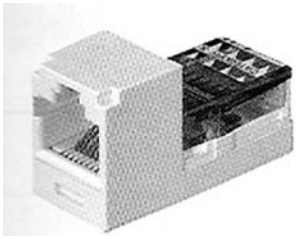


Figura 4.5 Jack

Conector *RJ-45* Va al inicio y al final del cable; se conecta directamente a la roseta y equipo. Ver figura 4.6

Figura 4.6 RJ 45

Herramienta de impacto Posee un resorte que se puede graduar para dar distintas presiones de trabajo y sus puntas pueden ser cambiadas para permitir la conexión de otros bloques, tal como los 88 y 66. En el caso del bloque de 110, la herramienta es de doble acción inserta y corta el cable. Ver figura 4.7

Figura 4.7 Herramienta de impacto

Panel de Parcheo *(Patch Panel)* Están formados por un soporte, usualmente metálico y de medidas compatibles con rack de 19", que sostiene placas de circuito impreso sobre la que se montan de un lado los conectores *RJ-45,* del otro lado los conectores *IDC* para bloc tipo 110. Se proveen en capacidades de 12 a 96 puertos (múltiplos de 12). Ver figura. 4.8 y figura 4.9

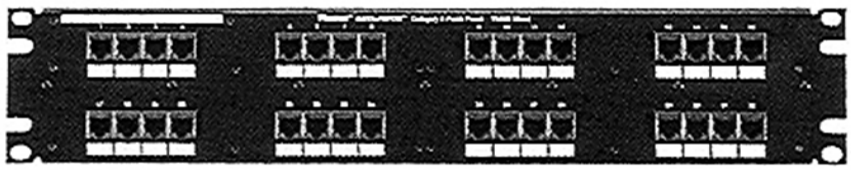


Figura 4.8 Panel frontal

Figura 4.9 Panel exterior

Pelador y cortador de cables Permite agilizar notablemente la tarea de pelado de vainas de los cables *UTP,* tanto sólidos como flexibles, así como el emparejado de los pares internos del mismo.

Pinzas Ponchadoras Permite cortar el cable, pelarlo y apretar el conectar para fijar los hilos del cable a los contactos. Ver figura 4.10

Figura 4.10 Pinzas Ponchadoras

Conectores para fibra óptica. Va al inicio y al final del cable; se conecta directamente a la roseta y equipo.

Figura 4.11 Conector de fibra óptica

Rack En la siguiente imagen se puede ver un racks utilizado por la red LAN de la ciudad universitaria. Figura. 4.12

Figura. 4.12 Rack

Roseta para conectores Pieza plástica de soporte que se amura a la pared y permite encastrar hasta dos conectores. Ver figura. 4.13. [48]

Figura. 4.13 Roseta

En el apéndice A muestra el plano de cuidad universitaria del cableado estructurado.

4.6 Equipos Ethernet y Gigabit Ethernet de ciudad universitaria

4.6.1 Switches de ciudad universitaria

Los switches de ciudad universitaria operan en la Capa 2 del modelo OSI y ofrecen servicios como el de asociación de VLAN. El principal propósito de un switch de capa de acceso es permitir a los usuarios finales el acceso a la red. Un switch de capa de acceso debe proporcionar esta funcionalidad con bajo costo y una alta densidad de puerto.

Los siguientes switches Cisco se utilizan comúnmente en la capa de acceso y rn ciuda universitaria:

- Serie Catalyst 2950
- Serie Catalyst 3550
- Serie Catalyst 4000

El switch serie Catalyst 2950 ofrece acceso efectivo para servidores y usuarios que requieren un alto ancho de banda. Esto se logra con puertos de switch adaptados para Fast Ethernet. El switch serie Catalyst 4000 incluye puertos Gigabit Ethernet y son dispositivos de acceso efectivos para una mayor cantidad de usuarios en redes de campus más grandes. En la siguiente tabla se muestra algunas diferencias de estos modelos:

Catalyst	Capas OSI admitidas	Puertos Ethernet	Puertos Fast Ethernet	Puertos Gigabit
Serie 2950	Capa 2	Ninguno	12 ó 24 puertos con velocidad configurable	0 ó 2
Serie 4000	Capa 2 y 3	Puertos configurables-Hasta 240	Puertos configurables-hasta 240	Puertos configurables-hasta 240

Tabla 4.5 Diferencias entre switches

La siguiente imagen muestra en switch modelo catalyst 4000 como el que se usa en la red de Cuidad universitaria:

Figura 4.14 Switch Catalyst 4000 de Cisco

4.6.2 Ruteador de ciudad universitaria

Un ruteador es un dispositivo de Capa 3 que se considera como uno de los dispositivos más poderosos en la topología de red. El router utilizado en la red de Cuidad Universitaria es un Cisco 7000.

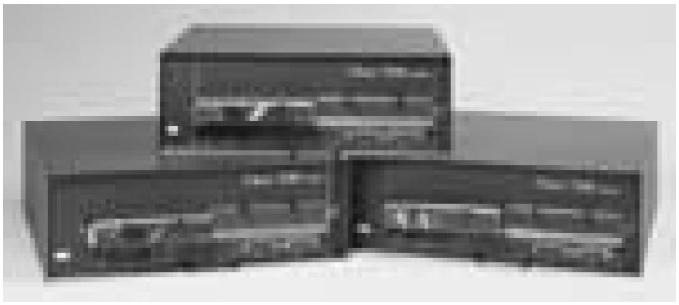


Figura 4.15 Ruteador serie 7000 de Cisco

Los dispositivos de la Capa 3 se pueden utilizar para crear segmentos LAN únicos. Los dispositivos de Capa 3 permiten la comunicación entre los segmentos basados en las direcciones de Capa 3, como por ejemplo direcciones IP. La implementación de los dispositivos de Capa 3 permite la segmentación de la LAN en redes lógicas y físicas exclusivas. Los routers también permiten la conectividad a las WAN como, por ejemplo, Internet.

El enrutamiento de Capa 3 determina el flujo de tráfico entre los segmentos de red física exclusivos basados en direcciones de Capa 3. Un router envía paquetes de datos basados en direcciones destino. Un router no envía broadcasts basados en

LAN, tales como las peticiones ARP. Por lo tanto, la interfaz del router se considera como el punto de entrada y salida de un dominio de broadcast y evita que los broadcasts lleguen hasta los otros segmentos LAN.

4.6.3 Sistema operativo de internetworking (IOS) que ocupan los dispositivos de ciudad universitaria

Al igual que un computador, un ruteador o switch no puede funcionar sin un sistema operativo. Cisco ha denominado a su sistema operativo el Sistema operativo de internetworking Cisco, o Cisco IOS. Es la arquitectura de software incorporada en todos los routers Cisco y también es el sistema operativo de los switches Catalyst. Sin un sistema operativo, el hardware no puede hacer ninguna función. El Cisco IOS brinda los siguientes servicios de red:

- Funciones básicas de enrutamiento y conmutación
- Acceso confiable y seguro a los recursos de la red
- Escalabilidad de la red. [44]

4.7 Redes inalámbricas en ciudad universitaria

Las redes inalámbricas, utilizan el estándar 802.11 de la IEEE que se despliega en el espectro de 2.4 Gigahertz sin licencia, reservado para las redes inalámbricas de datos. Para conectar una red LAN inalámbrica se necesita un equipo Access Point que se conecta a la red cableada, además se requiere instalar en cada PC una Station Adapter y una tarjeta Ethernet que proveerán la conexión inalámbrica con los Access Point.

Las velocidades de transmisión de una red LAN inalámbrica varían desde 1 hasta 11 Megabits por segundo.

Actualmente compañías como Nortel, Lucent y Cisco Systems han lanzado ya productos con este estándar y se espera que antes de que finalice el año 2001 los equipos sean capaces de alcanzar velocidades de hasta 26 Megabits por segundo. Cada Access Point en este tipo de redes tiene un límite de 140 usuarios.

Esta tecnología está implementada ya en nuestra institución, utilizando equipos de acceso inalámbrico AP1000 de Lucent Tecnologies, que se encuentran situados en puntos estratégicos en Ciudad. [43]

4.8 Servidores de ciudad universitaria

Un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.
Los servidores de la red de cuidad universitaria son:

1.- Servidores DNS *(name servers)*, que contestan las peticiones de los clientes, los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada;

2.- Servidores de Correo (Mail Servers) Casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

3.- Servidores web (Web Servers) Básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

4.9 Monitoreo y Seguridad en la VLAN de ciudad universitaria

El monitoreo se lleva a cabo con un dispositivo electrónico que permite verificar todos los accesos que tengan los usuarios. Este dispositivo funciona segmentando el ancho de banda de la red para poder monitorear todas las gestiones de los usuarios.

La seguridad se lleva a cabo con un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet).

Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un

programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes. [47]

Nota: los modelos de estos dispositivos no pueden ser revelados por los administradores de la red por motivos de seguridad.

En la figura 4.16 se muestra la distribución de equipos de ciudad universitaria.

Como podemos apreciar en la figura 4.16 tenemos dos enlaces dedicados* E3* que distribuyen el Internet, uno por parte de Telmex y otro por parte de Avantel que es el que proporciona el Internet 2, también como ya vimos en los temas anteriores podemos apreciar un Router de cisco 7000 que funciona sobre la capa 3 del modelo OSI estos funcionan como conexiones de segmentos de la red VLAN cabe mencionar que existen alrededor de 30 de estas redes en Ciudad Universitaria, además de que gestionan el trafico. Existen en la red dos firrewall uno que sirve para monitorear la red y otro para proteger la red.

Pasando a otro segmento de la red tenemos el switch cisco 3500 que conecta a los tres servidores existentes en la red y esto permite el funcionamiento de las capas superiores del modelo OSI.

La ultima parte de la figura donde se encuentra el switch 2950 que son los encargados de dar servicio a los usuarios finales y a los acces points.

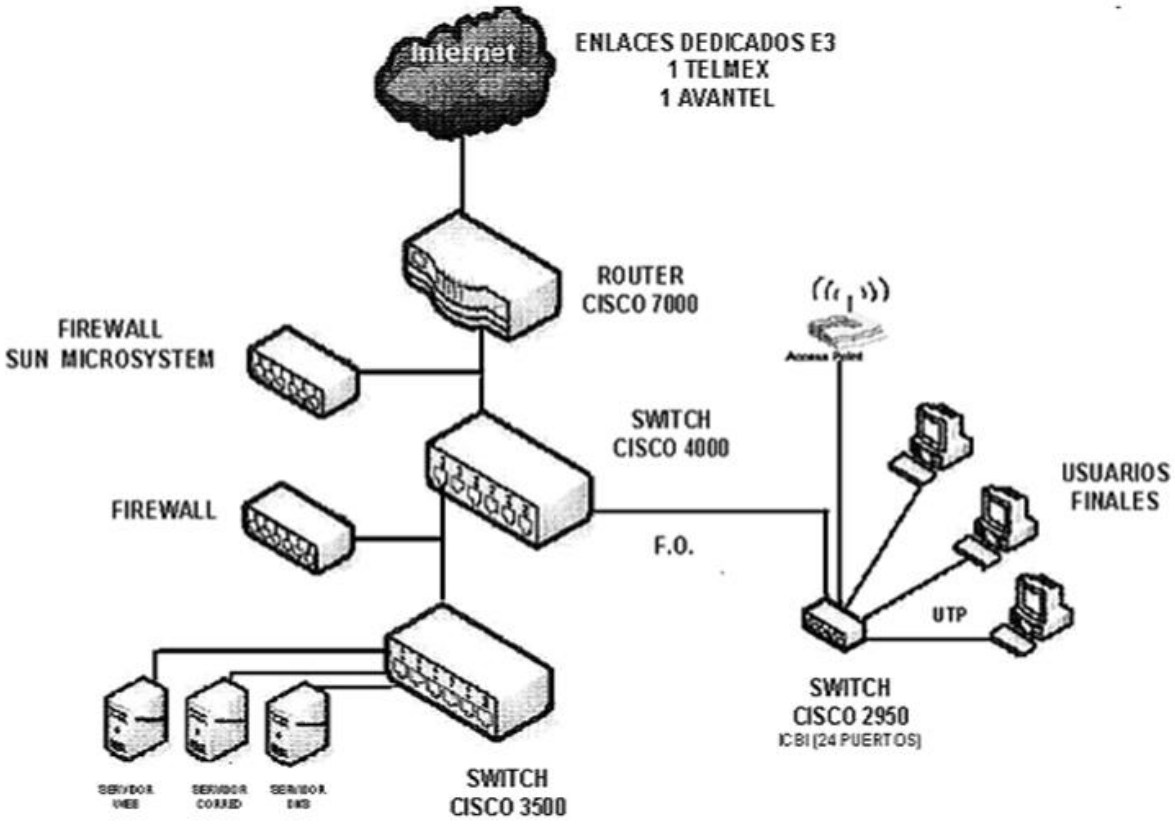


Figura 4.16 Arquitectura de la red de ciudad universitaria

Conclusiones

Las tecnologías como Ethernet y GigabitEthernet son el punto de atención para los diseñadores de redes, son tecnologías con una gran sencillez de manejo desde su administración hasta su instalación de usuario final; sobre todo brindan una gran confiabilidad en este caso para la Universidad Autónoma del Estado de Hidalgo además de que no solo cumplen con características muy interesantes como las anteriores sino que aun mejor son de bajo costo en la instalación y actualización. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

Por otra parte Ethernet seguirá dando de que hablar ya que la IEEE y la Alianza de Ethernet de 10 Gigabits se encuentran trabajando en estándares para 40, 100 e inclusive 160 Gbps. Esto nos indica que Ethernet seguirá evolucionando mientras que otras tecnologías de transmisión desaparecerán.

Las tecnologías innovadoras como Ethernet seguirán haciendo a las redes más rápidas y sobre todo muy fáciles de administrar mientras Ethernet siga evolucionando tendremos en un futuro muy prometedor para las redes de alta velocidad.

En otro orden de ideas la presente monografía aporta a la comunidad universitaria información sobre una red real de alta velocidad, entre lo mas destacado de la información se encuentra un plano de la distribución de cables de toda la ciudad universitaria proporcionado por la Dirección general de obras y proyectos y además una arquitectura general de cómo estas conectados los diferentes dispositivos de red que se ocupan en dicha red.

Glosario

A

AAL. ATM. Adaptación Layer. Niveles de adaptación utilizados en ATM que permiten transportar tráficos clásicos (voz, video, datos) sobre redes ATM. Están definidos diferentes niveles, el AAL1 para trafico de voz, AAL 2 para video, AAL ¾ para datos y el AAL 5 también para datos.

Aislante. Recubierta que tiene dos finalidades: proteger de la humedad al cable y apartar los cables eléctricamente unos de otros.

Ancho de banda. Margen de frecuencias capaz de transmitirse por una red de Telecomunicaciones.

ANSI (American National Standards Institute / Instituto Nacional Americano para la Estandarización). Organismo oficial dedicado a fomentar la adopción de normativas en materia de informática, comunicaciones, etc.

Apantallamiento Recubrimiento de un cable por el que se transmite información en forma de señal electromagnética, con el fin de evitar las interferencias que pudiesen alterar la información.

Arquitectura. Especificación que define como debe organizarse la red, definiendo los niveles funcionales, protocolos, formatos de datos, procedimientos e interfaces para permitir la comunicación entre distintos elementos. Una buena arquitectura debe definir que se conecta con que y como se conecta. De no haber una definición arquitectónica, habrá dificultad constante al tratar de establecer y mantener las conexiones, la integridad (asegurarse de que funcione todo como debería funcionar), y la disponibilidad.

Asíncrono Transmisión no sincronizada en la que el sincronismo entre el emisor y el receptor se establece de nuevo en el terminal para cada carácter transmitido.

Atenuación. La energía de la señal es inversamente proporcional a la distancia, de manera que disminuye con ésta. En medios guiados la atenuación es

logarítmica, por lo que se suele expresar en dB / Km. En medios no guiados su dependencia no es sólo de la distancia, sino también de las condiciones atmosféricas.

ATM (Asynchronous Transfer Mode I Modo de Transferencia Asíncrona). Técnica de conmutación por paquetes de alta velocidad adecuada para redes de área metropolitana (MAN).

B

Backbone. En una WAN, como Internet, un medio de alta velocidad y alta capacidad diseñado para transferir datos a cientos o miles de kms. Se utilizan varios medios físicos para los servicios de columna vertebral, incluyendo los relevadores de microondas, los satélites y las líneas telefónicas dedicadas.

Banda ancha. Técnica de comunicaciones en la que las señales digitales se transmiten moduladas, pudiendo enviarse por un solo canal múltiples señales simultáneas. La UIT- T define también como banda ancha a las comunicaciones digitales a más de 2 Mbps.

Bit (Bínary Digit/Dígito binario). Unidad mínima de información con la que trabajan los ordenadores. Es un dígito del sistema binario que puede tener el valor O o 1.

Bps (Bíts por second I Bits por segundo). Unidad de velocidad de transmisión de datos.

Broadcast. Mensaje que se nevia por un dispositivo a todos los de mas en una red

Bus Conjunto de líneas que transportan información binaria entre la CPU, la memoria principal y la unidad de entrada/salida. Facilitan la transmisión de datos entre dispositivos situados en dos puntos terminales, pudiendo, únicamente, transmitir uno de ellos en un momento dado.

Bucle. La palabra bucle define la telefonia clasica el par de hilos de cobre, alimentados por corriente continua, que unen la central telefonica con el equipo de abonado.

Byte Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

C

Cabecera (Header).Parte inicial de un paquete que precede a los datos propiamente dichos y que contiene las direcciones del remitente y del destinatario, control de errores y otros campos. Porción de un mensaje de correo electrónico que precede al mensaje propiamente dicho y contiene, entre otras cosas, el remitente del mensaje, la fecha y la hora.

CCITT (Comité Consultatif International Téléphonique el Télégraphique / Comité Consultivo Internacional de Telefonía y Telegrafía). Una organización internacional extinta que diseñaba estándares para la comunicación analógica y digital que implica a los módems, redes de computadoras y maquinas de fax. Para los usuarios de computadoras, el papel más importante del CGITT recae en el establecimiento de estándares internacionales para la conectividad mediante módems, los famosos estándares "V punto". El GGITT ha sido reemplazado por la Unión Internacional de Telecomunicaciones-Sección de Normas de Telecomunicaciones (1 TU- TSS).

Células. Contiene información con un tamaño fijo para su conmutación.

Codificación Conversión de un valor analógico en una señal digital según un código prefijado.

Código Cada una de las secuencias de caracteres que transforman los elementos de un repertorio en otro.

Código detector de errores. Código que permite mediante una estructura definida redundante de los datos, la detección de cualquier error ocurrido durante la transmisión o la grabación de los datos.

Colisión Se produce cuando más de un nodo intenta transmitir al mismo tiempo.

CSMA/CD (Carner Sense Multiple Access with Collision Detection). Protocolo de comunicaciones para una red de área local que utiliza una estructura en bus. Define los niveles físico y de enlace en el modelo OS I para el método de acceso

a la red por el cual una estación obtiene el uso del medio físico para enviar un mensaje a través de la red. La especificación de este protocolo se describe en las normas IEEE 802.3 e ISO 8802.3, ambas basadas en el estándar Ethernet.

D

Datagrama. Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Decodificación. Conversión de un valor digital en una señal analógica. Proceso de reconversión de un mensaje codificado al mensaje que dio lugar a la codificación.

DQDB *(Distributed Queued Dual Bus).* Mecanismo de control de acceso al medio empleado por las redes metropolitanas normalizadas *IEEE 802.6.*

Dirección MAC: Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

DTE (Data Terminal Equipment I Equipo Terminal de Datos). El término utilizado. por la especificación que define al puerto serial estándar para describir la computadora que está conectada a un módem o a un módem para fax.

DSL. Digital suscribe line, Permite la transmisión full duplex de 192 kbps al bucle de abonado.

E

Enlace dedicado. Son los enlaces que contratan las empresas para servicio de Internet

E3. Línea de transmisión de 34 Mbps.

F

FDDI *(Fiber Distributed Data Interface).* Especificación de una red de área local con topología en anillo, método de acceso por paso de testigo cuya estructura se implementa sobre un cable de fibra óptica. Esta norma fue desarrollada por el *ANSI.*

Full-duplex . Protocolo de comunicaciones asincrónicas que permite al canal de comunicaciones enviar y recibir señales al mismo tiempo.

FTP (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.

Frame Re/ay Sistema de transporte para la transmisión de datos (paquetes) a alta velocidad (hasta 45 Mbits/s) mediante celdas de longitud variable.

Frecuencia El número de ciclos por segundo de una onda. Se mide en Hertzios (Hz), que indican el número de cambios por segundo.

G

Gigahertzio GHz. Unidad de medida de la velocidad de reloj de un ordenador que equivale a mil Megahercios.

H

Halt-duplex .Protocolo de comunicaciones asincrónicas en el que el canal de comunicaciones manipula una sola señal a la vez. Las dos estaciones alternan sus transmisiones.

Host En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red.

I

IEEE (instítute of Electrical and Electronícs Engíneers I Instituto de Ingenieros

Eléctricos y Electrónicos). Organismo normalizador de métodos de acceso y control para LANs. Es miembro de ANSI e ISO. La *IEEE* cuenta con sus estándares 802 sobre cableado físico y la transmisión de datos en redes de área local y son:

- 802.1: una introducción a los estándares 802.
- 802.2: estándares para el control lógico de enlace *(LLC, Logícal Link Control)* y otros estándares sobre la conexión básica de redes.
- 802.3: estándares para el *CSMAlCD*
- 802.4: estándares para el acceso al bus mediante el paso de testigo (token bus).
- 802.5: estándares para el acceso al anillo mediante testigo *(token ring)* y para las comunicaciones entre redes *LAN* y *MAN.*
- 802.6: estándares para redes *LAN* y *MAN,* incluyendo interconexión de alta velocidad y sin conexiones.
- 802.7: estándares para tecnología de banda ancha.
- 802.8: estándares para tecnología de fibra óptica.
- 802.9: estándares para servicios de red integrados, tales como voz y datos.
- 802.10: estándares para la seguridad de redes *LAN* y *MAN.*
- 802.11: estándares para la conexión inalámbrica.
- 802.12: estándares para el método de acceso con petición de prioridad.

Infrarrojo Radiaciones del espectro solar no visibles.

IOS. Sistema operativo de internetworking

IP (Intemet Protocol). Un número binario de 32 bits que identifica de manera única y precisa la posición de una computadora particular en Internet. Toda computadora que esté conectada de manera directa a Internet debe tener una dirección IP. Debido a que los números binarios son difíciles de leer, las direcciones IP están dadas en números decimales de cuatro partes, donde cada parte representa 8 bits de la dirección de 32 bits (por ejemplo, 128.143.7.226).

ISO (Intematíonal Organízatíon for Standardízatíon / Organización Internacional

de Normalización). Es el máximo organismo de normalización a nivel internacional con sede en Ginebra. Su Technícal Committe 97 (TC97), es responsable del modelo de referencia OSI. Edita propuestas de normas internacionales "Draft Intemational Standard (OIS)" que juntamente con el lEC, son los 2 organismos competentes para emitir normas internacionales.

ITU- T (Telecommunication Standardization Sector / Unión Internacional de Telecomunicaciones). Es una de los 3 sectores de la ITU (Intemational Telecomunicatíon Uníon), creado para reemplazar al CCITT. Organización internacional que diseña estándares para la comunicación analógica y digital.

J

Jitter (Fluctuación). Tendencia a perder la sincronizaron a causa de cambios mecánicos o eléctricos. En las señales de datos es la desviación que se produce respecto a la señal original de sincronización en las transmisiones correspondientes al sincronismo o defectos producidos en las señales de datos por el propio proceso de transmisión sobre los medios físicos.

K

Kbps. Kilobits por segundo. Medida de velocidad de transmisión

L

LAN (Local Area Network / Red de Área Local) Computadoras personales y de otros tipos enlazadas, dentro de un área limitada, mediante cables de alto desempeño para que los usuarios puedan intercambiar información, compartir periféricos y extraer programas y datos almacenados en una computadora dedicada, llamada servidor de archivos.

Láser (Ught Amplíficatíon by Estimulated Emission of Radiation / Amplificación de la Luz mediante Emisión Estimulada de Radiación). Dispositivo para la emisión de luz estimulada con una radiación coherente.

LLC (Logical Unk Control/Control de enlace lógico). Protocolo de nivel de enlace del modelo OSI definido para LANs.

M

MAC: Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

MAN Metropolitan Area Networks / Redes de Área Metropolitana.

MAU (Multistation Access Unit / Unidad de acceso multíestación).Concentrador de dispositivos en estrella para redes TokenRing.

Mbps Megabits por segundo. Medida de velocidad de transmisión.1 Mbps = 10 bps (bits por segundo).

Multiplexación. En redes LAN, la transmisión simultánea de varios mensajes en un canal. Una red con capacidad de multiplexión, permite que varias computadoras accedan a la red de manera simultánea. Sin embargo, la multiplexión eleva el costo de una red, ya que deben incluirse dispositivos multiplexores que permiten mezclar las señales para transmitir/as en un solo canal.

N

NIC. Tarjeta de Interfece de red que se ocupa para conectar las Pc´s a las redes.

O

OSI (Open Systems Interconnection I Interconexión de Sistemas Abiertos). Estándar ISO para comunicaciones a nivel mundial que define una estructura con el fin de implementar protocolos en 7 estratos o capas. El control se transfiere de un estrato al siguiente comenzando en el estrato de aplicación en una estación, llegando hasta el estrato inferior, por el canal hasta la próxima estación y subiendo nuevamente la jerarquía. Las 7 capas son: Nivel Físico, de Enlace de datos, de Red, de Transporte, de Sesión, de Presentación y de Aplicación. El. OSI requiere una enorme cooperación para que sea un estándar universal como el sistema telefónico.

P

Paquete. Secuencia de dígitos binarios, incluyendo datos y señales de control, que se transmite y conmuta como un todo.

PBX. Private Branch Exchange. Equipo de conmutación telefónica que se dedica a un cliente y se conecta a la red conmutada publica.

Protocolo. Conjunto formal de convenciones que gobiernan el formato y control de datos. Conjunto de procedimientos o reglas para establecer y controlar transmisiones desde un dispositivo o proceso fuente a un dispositivo o proceso objeto.

Puerto: Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo tamaño, como un jack RJ-45. En estos puertos se usan los cables de conmutación para interconectar computadores conectados al panel de conmutación.

PVC (Permanent Virtual Circuit /Circuitos Virtuales Permanentes). Son conexiones "permanentes" entre dos nodos de la red y operan como una línea física dedicada.

Q

Q&S. Quality of services, el ATM proporciona diveros servicios según las necesidades de comunicación definiendo mediante perametros de calidad y servicio

Q&S. Quality of services, el ATM proporciona diveros servicios según las necesidades de comunicación definiendo mediante perametros de calidad y servicio

R

Red Uno Empresa líder en el mercado mexicano de telecomunicaciones, dedicada al diseño e integración de soluciones corporativas de comunicación de voz, datos y video.

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

Network). Red que evoluciona a partir de la red telefónica; permite la conectividad digital de usuario a usuario, proporcionando. servicios telefónicos y no-telefónicos.

S

Señalización. Es el intercambio de información o mensajes dentro de una red de telecomunicación para controlar, establecer, conmutar, encaminar, supervisar y gestionar sus comunicaciones.

Servidor (informática), computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos. Internet es en último término un conjunto de servidores que proporcionan servicios de transferencia de ficheros, correo electrónico o páginas WEB, entre otros. En ocasiones se utiliza el término servidor para referirse al software que permite que se pueda compartir la información

SMDS (Switched Multimegabit Data Services / Servicios de datos conmutados a multimegabits). Conmutación de datos entre LANs mediante MANs.

Slot. Ranura de tiempo. Mecanismo de acceso para comparición del medio físico utilizado en algunos sistemas de comunicaciones.

Sistema operativo: software básico que controla una computadora. El sistema operativo tiene tres grandes funciones: coordina y manipula el hardware del ordenador o computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el mouse; organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, discos duros, discos compactos o cintas magnéticas, y gestiona los errores de hardware y la pérdida de datos.

Software de red: Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún sistema operativo de red, los equipos no pueden compartir recursos y los usuarios no pueden utilizar estos recursos.

SMTP (Protocolo básico de transferencia de correo). Correo electrónico.

SNMP (Protocolo básico de gestión de red). Para la gestión de redes.

SVC (Switched *Virtual Circuit I* Circuitos Virtuales Conmutados). Son circuitos creados dinámicamente para cada transmisión

T

Token Bus. Protocolo para transmisión de datos en una LAN, utilizando una estructura en anillo. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.4 del IEEE y en la norma 8802.4 de la ISO.

Token Ring Protocolo para transmisión de datos en una LAN, utilizando una estructura en bus. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma /EEE 802.5 del IEEE y en la norma 8802.5 del ISO.

Topología. Es el término técnico que describe la manera en que se configura la red. La topología está determinada en parte, por la manera en que las PC's administran el acceso a la red (quien habla primero) y por las limitaciones del sistema de señales (la manera en que se envían señales de una PC a otra)

TCP: Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP: Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años ’70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

U

UDP: Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

X

X.25 Interfaz para la transmisión de datos en redes de conmutación de paquetes *(PSDN, Packed Switched Data Network).* Está definido por las 3 primeras capas del modelo OSI. Permite circuitos virtuales así como recuperación de datos y recuperación de errores. Son recomendaciones de la *UIT-T* para intercomunicaciones de paquetes.

Bibliografía

[1] http://fmc.axarnet.es/redes/tema_01.htm

[2]http://www.monografias.com/trabajos18/redescomputadoras/redescomputadoras.shtml

[3] http://www.cisco.com/global/LA/LATAM/sne/cmc/porque.shtml

[4] http://www.monografias.com/trabajos18/redes-computadoras/redes-computadoras2.shtml

[5] Moreno Luciano, “Topología de Redes” http://www.htmlweb.net/redes/topologia/topologia_5.html

[6] PTAFFENBERGER, Bryan. “Diccionario para usuarios de computadoras e Internet”. 6ta edicion

[7] http://www.monografias.com/trabajos3/redycomun/redycomun.shtm

[8]http://publicaciones.ua.es/?ExternalURL=http://publicaciones.ua.es/Deprox/4-7908-664-5.asp

[9] http://www.itlp.edu.mx/publica/tutoriales/redes/tema24.htm

[10] http://fmc.axarnet.es/redes/tema_09.htm

[11] “Sistema Operativo” Biblioteca de Consulta Microsoft ® Encarta ® 2005. © 1993-2004 Microsoft Corporation. Reservados todos los derechos

[12] http://fmc.axarnet.es/redes/tema_04.htm

[13] ST-PIERRE, ARMAND Y STÉPHANOS, William. “Redes Locales e Internet”. Editorial: Trillas,1997.

[14] http://davidelbuenas.tripod.com/

[15] http://www.itlp.edu.mx/publica/tutoriales/telepro/t4_4.htm

[16] http://www.arqhys.com/arquitectura/cableado-transmision.html

[17] http://trevinca.ei-uvigo.es/~mdiaz/rdo01_02/tema2.pdf

[18] http://html.rincondelvago.com/medios-de-transmision_1.html

[19] Gallardo, Roger “Trabajo sobre Modelo OSI” http://www.monografias.com/trabajos3/redycomun/redycomun.shtml

[20] http://www.inf.utfsm.cl/~liuba/iing/alumnos/redes/protocolos.html

[21] Aprendiendo TCP/IP en 14 dias, editorial Hispanoamérica,1995

[22] Garcia, Jesús y Raya, Rodrigo, Alta Velocidad y Calidad en Servicio en Redes IP, Editoral Alfaomega, 2002

[23] http://tau.uab.es/~gaby/IPV6/Memoria%20del%20proyecto%20IPv6.pdf

[24] http://www.reuna.cl/central_apunte/apuntes/listas.html

[25] http://www.ictnet.es+jtrujillo/framerelay.html

[26] http://redestel.tripod.com/atm.htm

[27] http://pracgsi.ulpgc.es/~a1467/cursos/tcp-ip/cap02s13.html

[28] http://www.consulintel.es/Html/Tutoriales/Articulos/fddi.html

[29] http://www.cicese.mx/~ aarmenta/frames/redes/fddi/spanish.html

[30] http://www.ldc.usb.ve/~redes/Temas/Tema07/comparac.htm

[31] www.map.es/csi/silice/Redman13.html

[32] http://usuario.cicese.mx/~aarmenta/frames/redes/fddi/fddi-ii/intro1/da.html

[33] http://www.cybercursos.net/cursos-online/fast-ethernet/fastethernet.htm

[34] http://www.ldc.usb.ve/~redes/Temas/Tema.31/cdqdb.html

[35] http://www.angelfire.com/md2/dqdb/index.html

[36] http://www.consulintel.es/Html/Tutoriales/Articulos/tutoriales_fr.html

[37] http://agamenon.unidades.edu.co/~revista/articulos/altavelocidad/alta.html

[38] http://www.die.udec.cl/~redes/apuntes/myapuntes/node90.html

[39] www.lantronix.com/training/tutorials/fastetnt.html

[40] http://tecinfosystem.iespana.es/files/topicos/html/smds.html

[41] García, Jesús, Piattini, Mario y Ferrando, Santiago, “Redes de Alta Velocidad”, editorial Alfaomega, 1997.

[42] Cruz, Ivan “ATM”
http://www.monografias.com/trabajos/atm/atm.shtml

[43] http://www.reduaeh.mx/servicios/telecom/.html

[44] Curso de Cisco CCNA, Módulos 1, 2,3.

[45] Jardon, Hildelberto y Linares, Roberto, “Sistemas de Comunicaron por Fibra Óptica”, Alfaomega, 1995.

[46] http://platea.pntic.mec.es/~lmarti2/cableado.htm

[47] http://www.desarrolloweb.com/articulos/513.php?manual=15.html

[48] Manual de Accesorios Para Redes de PANDUIT.

[49]http://html.rincondelvago.com/compartir-recursos-a-traves-de-una-red-de ordenadores.html

[50]http://www.pcwla.com/pcwla2.nsf/0/d433047995e5b96d80256d4b00567dd6?OpenDocument&Click=