

**UNIVERSIDAD LASALLISTA BENAVENTE  
ESCUELA DE INGENIERIA EN COMPUTACION**



Con Estudios Incorporados a la  
**Universidad Nacional Autónoma de México**  
CLAVE: 8793-16

**SURGIMIENTO, EVOLUCIÓN Y  
FUTURO DE LA TECNOLOGÍA  
ETHERNET**

**TESIS**

QUE PARA OBTENER EL TÍTULO DE

**INGENIERO EN COMPUTACIÓN**

PRESENTA:

**ALEJANDRO FRANCO GASCA**

**ASESOR: ING. CARLOS HERNANDEZ VILLANUEVA**

CELAYA, GUANAJUATO

OCTUBRE DE 2007



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

**SURGIMIENTO,  
EVOLUCIÓN Y  
FUTURO  
DE LA TECNOLOGÍA  
ETHERNET**

# AGRADECIMIENTOS

Este documento está dedicado a mi *familia, profesores y amigos* que durante y después de mis años de estudio han colaborado en mi crecimiento profesional y personal hasta este momento, sin su apoyo no habría sido posible llegar hasta aquí.

# INDICE

## INTRODUCCION

### CAPITULO 1 FUNDAMENTOS DE REDES

1.1	COMPONENTES	
1.1.1	Introducción	2
1.1.2	Componentes electrónicos	2
1.1.3	Subsistemas de la PC	3
1.1.4	Componentes del Backplane	5
1.1.5	La NIC	6
1.1.6	Módem, DSL	8
1.1.7	Conexiones de red	9

### CAPITULO 2 REDES

2.1	Tipos de redes	
2.1.1	LAN	11
2.1.2	WAN	12
2.1.3	MAN	13
2.1.4	SAN	13
2.1.5	VPN	14
2.2	Medios de cobre	
2.2.1	Coaxial	15
2.2.2	STP	17
2.2.3	UTP	19
2.3	Medios ópticos	
2.3.1	Fibra óptica multimodo	22
2.3.2	Fibra óptica monomodo	26
2.4	Transceivers	27
2.5	Medios inalámbricos	28
2.6	Topologías	
2.6.1	Topología física	32
2.6.2	Topología lógica	34

### CAPITULO 3 ETHERNET

3.1	Historia	36
3.2	Denominaciones	38
3.3	Modelo OSI	40
3.4	Ethernet y OSI	42

3.5	Direcciones MAC	43
3.6	Trama	45
3.7	Protocolos MAC	48
3.8	Método de acceso CSMA/CD	49
3.9	Temporización	50
3.10	Espacio y postergación	52
3.11	Errores	53
3.12	Negociaciones	57
3.13	Tecnologías	
3.13.1	Ethernet 10Mbps	60
3.13.2	Ethernet 100Mbps	61
3.13.3	Ethernet 1000Mbps (1Gbps)	63
3.13.4	Ethernet 10Gbps	64
CAPITULO 4	CONFIGURACIONES ETHERNET	
4.1	Direccionamiento de Ethernet	
4.1.1	Manejo de direcciones MAC con puentes y switches	68
4.1.2	Tiempos de Latencia y conmutación	70
4.2	Métodos de transmisión y modos de conmutación	
4.2.1	Método de corte y método de almacenamiento y envío	71
4.2.2	Método Libre de Fragmentos	72
4.2.3	Protocolo Spanning Tree o Árbol de extensión	72
4.2.4	Dominios de Colisión y dominios de Broadcast	74
4.3	Señales y transmisión	
4.3.1	Segmentación	77
4.3.2	La señal Broadcast	78
4.3.3	Dominio de Broadcast	80
4.3.4	Transmisión de datos	81
CAPITULO 5	TECNOLOGÍAS WAN	
5.1	Introducción	84
5.2	Conexión analógica	87
5.3	ISDN	88
5.4	Líneas arrendadas o alquiladas	90
5.5	X 25	91
5.6	Frame Relay	92
5.7	ATM	93
5.8	DSL	94
5.9	Cable Módem	97

CONCLUSIONES

GLOSARIO

BIBLIOGRAFIA

# INTRODUCCIÓN

La globalización y la necesidad de información cada día demanda más del conocimiento y manejo de redes informáticas de datos, llámese red local, intranet, red privada, Internet, o cualquier nombre que pudiéramos escuchar, al final, todas tienen el mismo propósito, compartir información y recursos, y mientras más rápido lo hagan es mejor para todos, por esta razón es necesario conocer cómo funcionan, qué capacidades tienen, qué tecnología usan, quiénes las usan, incluso dónde están; y como los cambios en las técnicas de manejo de información, los dispositivos de red y las tecnologías avanzan día a día, si no estamos al tanto de los cambios podemos desaprovechar las ventajas que nos ofrecen y quedarnos atrás en nuestras áreas de trabajo o desarrollo, este documento presenta una recopilación de información basada en los cursos de capacitación del programa CCNA de Cisco Systems del programa Cisco Networking Academy, del cual he formado parte desde hace ya casi 5 años, que nos permitirá adentrarnos un poco más a la forma de trabajar de las redes, y al mismo tiempo prevenir que nuestra información se vea afectada por el mal uso de la infraestructura o incluso de nosotros mismos.

Este documento está enfocado a una de las tecnologías más comúnmente utilizadas a nivel mundial, la tecnología Ethernet, existen tecnologías que antiguamente eran muy superiores a esta, como Token Ring o FDDI, pero como veremos en la recopilación, actualmente Ethernet ofrece una excelente opción para trabajo de redes. Aunque Token Ring y FDDI son más rápidas que Ethernet, también son más costosas, y Ethernet que es más fácil de implementar y menos costosa, está avanzando a pasos agigantados y cada vez se vuelve más rápida y confiable, y expande sus límites geográficos, por esta razón sólo se incluye información referente a Ethernet.

La parte final de este documento incluye un vistazo a las tecnologías WAN, que aunque normalmente tenemos poco contacto con ellas, son de suma importancia para el manejo de datos a distancias grandes, y qué mejor, que conocer sus características para el día en que nos encontremos frente a frente con ellas, y aún cuando ese día no llegara pronto, lo más importante es estar preparado.

# CAPITULO I

---

## *FUNDAMENTOS DE REDES*



## **1 Componentes**

### **1.1 Introducción**

En este primer capítulo, veremos los componentes de una computadora y el papel que tienen las computadoras en un sistema de red, empezando por el componente más básico de una red, la computadora, cuanto más aprendamos acerca de las computadoras, más fácil será comprender el funcionamiento de las redes así como también su diseño y construcción.

Para comprender la función de las computadoras en un sistema de red, pensemos en Internet, se puede considerar a Internet como un árbol y a las computadoras como las hojas del árbol, las computadoras son las fuentes y las receptoras de información, en ambos casos, dando y recibiendo información de Internet, veamos que las computadoras pueden funcionar sin Internet, pero Internet no puede existir sin las computadoras. Las computadoras, además de ser parte integral de una red, también desempeñan un papel importante en el mundo laboral, las empresas utilizan sus computadoras para una gran variedad de propósitos, pero también las usan para tareas administrativas comunes. Utilizan los servidores para almacenar datos importantes y administrar las cuentas de los empleados, utilizan software de hojas de cálculo para organizar la información financiera, software procesador de texto para llevar registros y correspondencia y navegadores para acceder a los sitios Web de las distintas empresas. Después de todo esto, empecemos a analizar los componentes internos de una computadora.

## 1.2 Componentes electrónicos

- **Transistor:** Dispositivo que amplifica una señal o abre y cierra un circuito
- **Circuito integrado:** Dispositivo fabricado con material semiconductor que contiene varios transistores y realiza una tarea específica
- **Resistencia:** Un componente eléctrico que limita o regula el flujo de corriente eléctrica en un circuito electrónico.
- **Condensador:** Componente electrónico que almacena energía bajo la forma de un campo electrostático; se compone de dos placas de metal conductor separadas por material aislante.
- **Conector:** Parte de un cable que se conecta a un puerto o interfaz
- **Diodo electro luminiscente (LED):** Dispositivo semiconductor que emite luz cuando la corriente lo atraviesa

## 1.3 Subsistemas de la PC

- **Placa de circuito impreso (PCB, Printed Circuit Board):** Una placa que tiene pistas conductoras superpuestas o impresas, en una o ambas caras. También puede contener capas internas de señal y planos de alimentación eléctrica y tierra. Microprocesadores, chips, circuitos integrados y otros componentes electrónicos se montan en las PCB.
- **Unidad de DVD/CD-ROM/RAM:** Unidad de disco compacto con memoria de sólo lectura, que puede leer información de un DVD/CD-ROM/RAM
- **Unidad de procesamiento central (CPU):** La parte de una computadora que controla la operación de todas las otras partes, obtiene instrucciones de la memoria y las decodifica, realiza operaciones matemáticas y lógicas y traduce y ejecuta instrucciones.

- **Unidad de disquete:** Una unidad de disco que lee y escribe información a una pieza circular con un disco plástico cubierto de metal de 3.5 pulgadas. Un disquete estándar puede almacenar aproximadamente 1.44 MB de información.
- **Unidad de disco duro:** Un dispositivo de almacenamiento computacional que usa un conjunto de discos rotatorios con cubierta magnética para almacenar datos o programas. Los discos duros se pueden encontrar en distintas capacidades de almacenamiento.
- **Microprocesador:** Un microprocesador es un procesador que consiste en un chip de silicio diseñado con un propósito especial y físicamente muy pequeño, el microprocesador utiliza tecnología de circuitos de muy alta integración (VLSI, Very Large-Scale Integration) para integrar memoria, lógica y señales de control en un solo chip. Un microprocesador contiene una CPU.
- **Placa madre:** La placa de circuito impreso más importante de una computadora. La placa madre contiene el bus, el microprocesador y los circuitos integrados usados para controlar cualquier dispositivo tal como teclado, pantallas de texto y gráficos, puertos seriales y paralelos, joystick e interfaces para el mouse.
- **Bus:** Un conjunto de pistas eléctricas en la placa madre a través del cual se transmiten señales de datos y temporización de una parte de la computadora a otra.
- **Memoria de acceso aleatorio (RAM):** También conocida como memoria de lectura/escritura; en ella se pueden escribir nuevos datos y se pueden leer los datos almacenados. La RAM requiere energía eléctrica para mantener el almacenamiento de datos. Si la computadora se apaga o se le corta el suministro de energía, todos los datos almacenados en la RAM se pierden.

- **Memoria de sólo lectura (ROM):** Memoria de la computadora en la cual hay datos que han sido pregrabados. Una vez que se han escrito datos en un chip ROM, estos no se pueden eliminar y sólo se pueden leer.
- **Unidad del sistema:** La parte principal de la PC, que incluye el chasis, el microprocesador, la memoria principal, bus y puertos. La unidad del sistema no incluye el teclado, monitor, ni ningún otro dispositivo externo conectado a la computadora.
- **Ranura de expansión:** Un receptáculo en la placa madre donde se puede insertar una placa de circuito impreso para agregar capacidades a la computadora, como las ranuras de expansión PCI (Peripheral Component Interconnect/Interconexión de componentes periféricos) y AGP (Accelerated Graphics Port/Puerto de gráficos acelerado). PCI es una conexión de alta velocidad para placas tales como NIC, módems internos y tarjetas de video. El puerto AGP provee una conexión de alta velocidad entre dispositivos gráficos y la memoria del sistema. La ranura AGP provee una conexión de alta velocidad para gráficos 3-D en sistemas computacionales.
- **Fuente de alimentación:** Componente que suministra energía a un computador

#### 1.4 Componentes del backplane

- **Backplane:** Un backplane es una placa de circuito electrónico que contiene circuitos y zócalos en los cuales se pueden insertar dispositivos electrónicos adicionales en otras placas de circuitos en una computadora, generalmente sinónimo de o parte de la tarjeta madre.
- **Tarjeta de interfaz de red (NIC):** Placa de expansión insertada en la computadora para que se pueda conectar a la red.

- **Tarjeta de video:** Placa que se introduce en una computadora para darle capacidades de visualización
- **Tarjeta de sonido:** Placa de expansión que permite que la computadora manipule y reproduzca sonidos de alta fidelidad
- **Puerto paralelo:** Interfaz que puede transferir más de un bit simultáneamente y que se utiliza para conectar dispositivos externos tales como impresoras
- **Puerto serial:** Interfaz que se puede utilizar para la comunicación serial, en la cual sólo se puede transmitir un bit a la vez.
- **Puerto de ratón:** Puerto diseñado para conectar un ratón a la PC
- **Cable de alimentación:** Cable utilizado para conectar un dispositivo eléctrico a un tomacorrientes a fin de suministrar energía eléctrica al dispositivo.
- **Puerto USB:** Un conector de Bus Serial Universal (Universal Serial Bus). Un puerto USB conecta rápida y fácilmente dispositivos tales como un mouse o una impresora, incluso dispositivos portátiles como teléfonos celulares y memorias FLASH.
- **Firewire:** Una norma de interfaz de bus serial que ofrece comunicaciones de alta velocidad y servicios de datos isócronos de tiempo real.

Pensemos en los componentes internos de una PC como una red de dispositivos, los cuales se conectan al bus del sistema, en cierto sentido, una PC es una pequeña red informática.

## 1.5 La NIC

Una tarjeta de interfaz de red (NIC), o adaptador LAN, provee capacidades de comunicación en red desde y hacia una PC, es una tarjeta de circuito impreso que reside en una ranura en la tarjeta madre y provee una interfaz de conexión a los medios de red, en equipos portátiles, está comúnmente integrado en los

sistemas o está disponible como una pequeña tarjeta PCMCIA, del tamaño de una tarjeta de crédito, PCMCIA es el acrónimo para Personal Computer Memory Card International Association (Asociación Internacional de Tarjetas de Memoria de Computadores Personales). La NIC se comunica con la red a través de una conexión serial y con el computador a través de una conexión paralela, utiliza una Petición de interrupción (IRQ), una dirección de E/S y espacio de memoria superior para funcionar con el sistema operativo. Un valor IRQ (petición de interrupción) es un número asignado por medio del cual la computadora puede esperar que un dispositivo específico la interrumpa cuando dicho dispositivo envía señales acerca de su operación. Por ejemplo, cuando una impresora ha terminado de imprimir, envía una señal de interrupción a la computadora, la señal interrumpe momentáneamente a la computadora de manera que esta pueda decidir que procesamiento realizar a continuación. Debido a que hay múltiples señales a la computadora en la misma línea de interrupción pueden no ser entendidas por la computadora, se debe especificar un valor único para cada dispositivo y su camino a la computadora. Antes de la existencia de los dispositivos Plug-and-Play (PnP), los usuarios a menudo tenían que configurar manualmente los valores de la IRQ, o estar al tanto de ellas, cuando se añadía un nuevo dispositivo a la computadora.

Al seleccionar una NIC, hay que tener en cuenta los siguientes factores:

- **Protocolos:** Ethernet, Token Ring o FDDI
- **Tipos de medios:** Cable de par trenzado, cable coaxial, inalámbrico o fibra óptica
- **Tipo de bus de sistema:** PCI o ISA

Para poder realizar la instalación, debe contar con los siguientes recursos:

- conocimiento acerca de la configuración de la tarjeta de red, incluyendo los jumpers, el software "plug-and-play" y la *EPROM* (*memoria programable borrable de solo lectura*, un tipo de memoria que conserva su contenido hasta que se expone a la luz ultravioleta)
- uso de los diagnósticos de tarjetas de red, incluyendo los diagnósticos proporcionados por los distribuidores y pruebas de loopback (consultar la documentación de la tarjeta)
- la capacidad para resolver conflictos de recursos de hardware, incluyendo IRQ, dirección de base de E/S y *DMA* (*dirección de memoria directa*, que se utiliza para transferir datos desde la RAM a un dispositivo sin tener que atravesar la CPU)

## **1.6 MODEM, DSL**

A principios de la década de 1960, se introdujeron los módems para proporcionar conectividad desde las terminales no inteligentes a una computadora central, la velocidad de conexión era muy lenta, 300 bits por segundo (bps), lo que significaba aproximadamente 30 caracteres por segundo. En la década de 1990, los módems funcionaban a 9600bps y alcanzaron el estándar actual de 56kbps (56.000bps) para 1998. Para el año 2000 la necesidad de servicios de alta velocidad era muy demandada y surgen entonces los servicios de alta velocidad utilizados en el entorno empresarial, tales como la Línea de suscriptor digital (DSL) y el acceso de módem por cable, estos servicios ya no exigen el uso de un equipo caro o de una segunda línea telefónica, son servicios de conexión permanente que ofrecen acceso inmediato y no requieren que se establezca una conexión para cada sesión. Esto brinda mayor confiabilidad y flexibilidad y ha permitido que pequeñas oficinas y redes domesticas puedan conectarse a Internet.

## 1.7 Conexiones de red

La Internet es la red de datos más importante del mundo se compone de una gran cantidad de redes grandes y pequeñas interconectadas; las computadoras individuales son las fuentes y los destinos de la información a través de la Internet. La conexión a Internet o a cualquier red de datos se puede dividir en conexión física, conexión lógica y aplicaciones. Se realiza una conexión física conectando una tarjeta adaptadora, tal como un módem o una NIC, desde una PC a una red. La conexión física se utiliza para transferir las señales entre las distintas PC's dentro de la red de área local (LAN) y hacia los dispositivos remotos que se encuentran en Internet. La conexión lógica aplica estándares denominados protocolos. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen la manera en que se comunican los dispositivos de una red; las conexiones a Internet pueden utilizar varios protocolos. El Protocolo de control de transporte/protocolo Internet (TCP/IP) es el principal conjunto de protocolos que se utiliza en Internet. Los protocolos del conjunto TCP/IP trabajan juntos para transmitir o recibir datos e información. La aplicación que interpreta los datos y muestra la información en un formato comprensible es la última parte de la conexión. Las aplicaciones trabajan junto con los protocolos para enviar y recibir datos a través de Internet. Un navegador Web muestra el código HTML como una página Web. Ejemplos de navegadores Web incluyen Internet Explorer, Mozilla Firefox y Netscape entre los más populares. El Protocolo de transferencia de archivos (FTP) se utiliza para descargar archivos y programas de Internet. Los navegadores Web también utilizan aplicaciones plug-in propietarias para mostrar tipos de datos especiales como, por ejemplo, películas o animaciones flash.



## CAPITULO II

---

### *REDES*

## **2 REDES**

### **2.1 Tipos de redes**

#### **2.1.1 LAN**

Las redes LAN o redes de área local, constan de los siguientes componentes:

- Computadoras
- Tarjetas de interfaz de red (NIC)
- Dispositivos periféricos
- Medios de comunicación (Coaxial, UPT, STP, Fibra óptica, Inalámbrico)
- Dispositivos de red (Hubs, Bridges, Switches, Routers)

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI

Las redes LAN se encuentran diseñadas para operar en un área geográficamente limitada, proporcionar acceso múltiple a medios de ancho de banda alto, proporcionar conectividad continua a los servicios locales y conectar dispositivos físicamente adyacentes.

### 2.1.2 WAN

Las redes WAN o redes de área extensa, interconectan a las redes LAN, que a su vez proporcionan acceso a las PC's o a los servidores de archivos ubicados en otros lugares, como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias también permiten que las computadoras, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona.

Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes
- Posibilitar capacidades de comunicación en tiempo real entre usuarios
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico

Algunas de las tecnologías comunes de WAN son:

- Módems
- Red digital de servicios integrados (RDSI)
- Línea de suscripción digital (DSL - Digital Subscriber Line)
- Frame Relay
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3
- Red óptica síncrona (SONET )

### 2.1.3 MAN

La MAN es una red de área metropolitana, por ejemplo, una ciudad o una zona suburbana incluso campus universitarios extensos. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN, normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

### 2.1.4 SAN

Una SAN o red de área de almacenamiento es una red dedicada, de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

Las SAN poseen las siguientes características:

- **Rendimiento:** Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.
- **Disponibilidad:** Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de 10 kilómetros (Km.) o 6,2 millas.

- **Escalabilidad:** Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

### 2.1.5 VPN

Una VPN es una red privada virtual que se construye dentro de una infraestructura de red pública, como la Internet. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre la PC del empleado y un router VPN en la sede.

Esto es cada día mas común, por ello las VPN son más demandas día con día.

Las VPN conservan las mismas políticas de seguridad y administración que una red privada, son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

Los principales tipos de VPN:

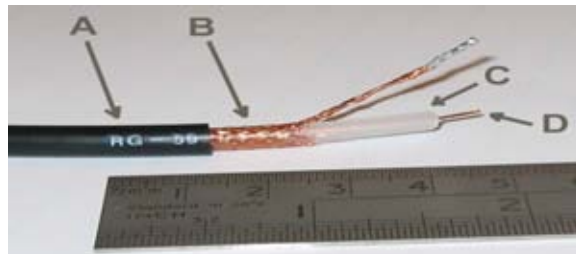
- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.
- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.

- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

## 2.2 Medios de cobre

### 2.2.1 Coaxial

El cable coaxial consiste de un conductor de cobre rodeado de una capa de aislante flexible el conductor central también puede ser hecho de un cable de aluminio cubierto de estaño que permite que el cable sea fabricado de forma económica sobre este material aislante existe una malla de cobre tejida u hoja metálica que actúa como el segundo hilo del circuito y como un blindaje para el conductor interno, esta segunda capa, o blindaje, también reduce la cantidad de interferencia electromagnética externa y cubriendo el blindaje está la cubierta de plástico del cable.



<sup>1</sup>Fig. 2.1 Cable coaxial (A. Cubierta B. Malla C. Aislante D. Núcleo de cobre)

Para las LAN, el cable coaxial ofrece varias ventajas, puede tenderse a mayores distancias que el cable de par trenzado blindado STP, y que el cable de par trenzado no blindado UTP, sin necesidad de repetidores. Los repetidores regeneran las señales de la red de modo que puedan abarcar mayores distancias. El cable coaxial es más económico que el cable de fibra óptica y la tecnología

<sup>1</sup> Imagen de cable coaxial tomada desde [www.wikipedia.com](http://www.wikipedia.com) en español

es sumamente conocida se ha usado durante muchos años para todo tipo de comunicaciones de datos, incluida la televisión por cable.

Al trabajar con cables, es importante tener en cuenta su tamaño a medida que aumenta el grosor, o diámetro del cable, resulta más difícil trabajar con él. El cable de mayor diámetro es de uso específico como cable de backbone de Ethernet porque tiene mejores características de longitud de transmisión y de limitación del ruido, este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa, como su nombre lo indica, este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. Generalmente, cuanto más difícil es instalar los medios de red, más costosa resulta la instalación, el cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet casi nunca se usa, salvo en instalaciones especiales.

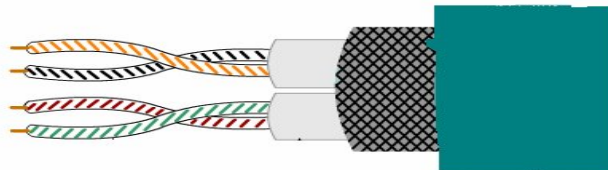
En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm. (a veces denominado thinnet o red fina) se usaba para las redes Ethernet, era particularmente útil para las instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas como la instalación de thinnet era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet (red barata).

El trenzado externo metálico o de cobre del cable coaxial abarca la mitad del circuito eléctrico se debe tener cuidado con la conexión eléctrica en ambos extremos, brindando así una correcta conexión a tierra, la incorrecta conexión del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial, por esta razón, thinnet ya no se usa con frecuencia ni está respaldado por los estándares más recientes (100 Mbps y superiores) para redes Ethernet.

El cable coaxial soporta velocidades de transmisión sólo de 10 a 100Mbps, más comúnmente de 10, una longitud máxima de 500mts y utiliza un conector tipo BNC.

### 2.2.2 STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables, cada par de hilos está envuelto en un papel metálico, los dos pares de hilos están envueltos juntos en una trenza o papel metálico generalmente es un cable de 150 ohmios, según se especifica para el uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como por ejemplo, el acoplamiento de par a par y la diafonía. El STP también reduce el ruido electrónico desde el exterior del cable como la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.



<sup>2</sup>Fig. 2.2. Cable STP

Un nuevo híbrido de UTP con STP tradicional se denomina UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El ScTP consiste básicamente en cable UTP envuelto en un blindaje de papel metálico. ScTP como UTP es también un cable de 100 Ohms. Muchos fabricantes e instaladores de cables pueden usar el término STP para describir el

<sup>2</sup> Dibujo ilustrativo de cable STP tomado desde [www.wikipedia.com](http://www.wikipedia.com) en español



cable ScTP. Es importante entender que la mayoría de las referencias hechas a STP hoy en día se refieren en realidad a un cable de cuatro pares apantallado. Es muy improbable que un verdadero cable STP sea usado durante un trabajo de instalación de cable.

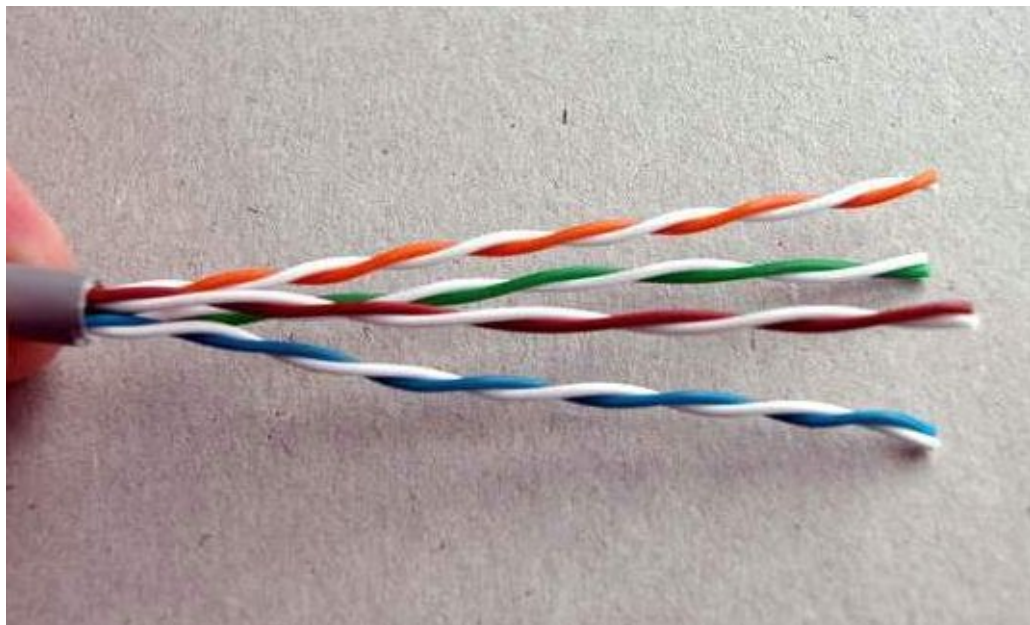
Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos si no están adecuadamente conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP y el ScTP se pueden volver susceptibles a graves problemas de ruido, son susceptibles porque permiten que el blindaje actúe como una antena que recoge las señales no deseadas sin embargo, este efecto funciona en ambos sentidos. El blindaje no sólo evita que ondas electromagnéticas externas produzcan ruido en los cables de datos sino que también minimiza la irradiación de las ondas electromagnéticas internas. Estas ondas podrían producir ruido en otros dispositivos.

Los cables STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios (cable coaxial y la fibra óptica) sin que se repita la señal, el uso del aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra sin embargo, el STP y el ScTP todavía desempeñan un papel importante, especialmente en Europa o en instalaciones donde exista mucha EMI y RFI cerca de los cables.

EL cable STP tiene una tasa de transferencia hasta 100Mbps, y una distancia de 100mts.

### 2.2.3 UTP

El cable de par trenzado no blindado (UTP) es un medio de cuatro pares de hilos que se utiliza en varios tipos de redes, cada uno de los 8 hilos de cobre del cable UTP está revestido de un material aislante, además, cada par de hilos está trenzado, este tipo de cable cuenta sólo con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan las EMI y las RFI, para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.



<sup>3</sup>Fig. 2.3 Cable UTP

El estándar TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas, y los procedimientos de medición necesarios para verificar los cables de par trenzado balanceado, exige el tendido de dos

---

<sup>3</sup> Fotografía de cable UTP categoría 5 tomada desde [www.wikipedia.com](http://www.wikipedia.com) en español

cables, uno para voz y otro para datos en cada toma, de los dos cables, el cable de voz debe ser UTP de cuatro pares.

El cable Categoría 5e es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5e en instalaciones de red. El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la Categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

El cable de par trenzado no blindado presenta muchas ventajas, es de fácil instalación y es más económico que los demás tipos de medios para redes, de hecho, el UTP cuesta menos por metro que cualquier otro tipo de cableado para LAN, la ventaja real es su tamaño, debido a que su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Esto puede ser un factor sumamente importante a tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ-45, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad. El cableado de par trenzado presenta ciertas desventajas, el cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios y la distancia que puede abarcar la señal sin el uso de repetidores es menor para UTP que para los cables coaxiales y de fibra óptica, tan sólo soportan 100mts.

Antes el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables sin embargo, hoy en día ya no es así, en la actualidad se considera que el cable de par trenzado es el más rápido entre los

medios basados en cobre, ya que puede alcanzar velocidades de transmisión en el grado de los Gbps (10,100, 1000Mbps según la categoría del cable).

Existen 3 tipos básicos de cables UTP

- El cable que se conecta desde un puerto de un hub o un switch al puerto de la NIC y recibe el nombre de cable directo o straight through.
- El cable que conecta 2 dispositivos, como hubs, switches o 2 PC's, recibe el nombre de cable de conexión cruzada o crossover
- El cable que conecta el adaptador de RJ-45 del puerto COM de la computadora al puerto de la consola de un router o switch recibe el nombre de cable transpuesto, de consola o rollover.

Para dejar un poco más claro esto, tengamos en cuenta lo siguiente, existen 2 normas o estándares para la elaboración de cables UTP, TIA/EIA-568-B y TIA/EIA-568-A y la diferencia entre estos dos estándares es la disposición de los pares en el conector RJ-45.

Cuando hablamos de un cable directo, significa que los dos extremos del cable están fabricados en base al mismo estándar, 568-A o 568-B, para que sea un cable directo deben estar ambos extremos en un solo estándar.

Cuando hablamos de un cable cruzado significa que un extremo del cable es construido con la norma 568-A y el otro con la norma 568-B.

Por último, el cable de consola es un extremo 568-A o 568-B y el otro extremo es el orden inverso del estándar utilizado.

Entonces si el cable UTP consta de 8 hilos (4 pares), cada uno de un color distinto, la disposición de los cables sería la siguiente:

- Par 1            verde (V)    /        verde-blanco (VB)
- Par 2            naranja(N)   /        naranja-blanco (NB)
- Par 3            azul (A)       /        azul-blanco (AB)
- Par 4            café ( C)      /        café-blanco (CB)

	Extremo 1								Extremo 2							
PIN	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Directo A	VB	V	NB	A	AB	N	CB	C	VB	V	NB	A	AB	N	CB	C
Directo B	NB	N	VB	A	AB	V	CB	C	NB	N	VB	A	AB	V	CB	C
Cruzado	VB	V	NB	A	AB	N	CB	C	NB	N	VB	A	AB	V	CB	C
Consola	VB	V	NB	A	AB	N	CB	C	C	CB	N	AB	A	NB	V	VB
Consola	NB	N	VB	A	AB	V	CB	C	C	CB	V	AB	A	VB	N	NB

<sup>4</sup> Tabla 1.1 Configuración de cables para UTPs

## 2.3 MEDIOS ÓPTICOS

### 2.3.1 FIBRA ÓPTICA MULTIMODO

La parte de una fibra óptica por la que viajan los rayos de luz recibe el nombre de núcleo de la fibra, los rayos de luz sólo pueden ingresar al núcleo si el ángulo está comprendido en la apertura numérica de la fibra, así mismo, una vez que los rayos han ingresado al núcleo de la fibra, hay un número limitado de recorridos ópticos que puede seguir un rayo de luz a través de la fibra, estos recorridos ópticos reciben el nombre de modos. Si el diámetro del núcleo de la fibra es lo suficientemente grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, esta fibra recibe el nombre de fibra "multimodo". La fibra monomodo tiene un núcleo mucho más pequeño que permite que los rayos de luz viajen a través de la fibra por un solo modo.

<sup>4</sup> Tabla ilustrativa de orden de cables para construcción de UTP cat 5

Cada cable de fibra óptica que se usa en las redes de datos está compuesto de dos fibras de vidrio envueltas en revestimientos separados, una fibra transporta los datos transmitidos desde un dispositivo A a un dispositivo B, la otra transporta los datos desde el dispositivo B hacia el dispositivo A, las fibras son similares a dos calles de un solo sentido que corren en sentido opuesto, esto proporciona una comunicación full-duplex. El par trenzado de cobre utiliza un par de hilos para transmitir y un par de hilos para recibir. Los circuitos de fibra óptica usan una hebra de fibra para transmitir y una para recibir, en general, estos dos cables de fibra se encuentran en un solo revestimiento exterior hasta que llegan al punto en el que se colocan los conectores. Hasta que se colocan los conectores, no es necesario blindar ya que la luz no se escapa del interior de una fibra, esto significa que no hay problemas de diafonía con la fibra óptica, es común ver varios pares de fibras envueltas en un mismo cable, esto permite que un solo cable se extienda entre armarios de datos, pisos o edificios, un solo cable puede contener de 2 a 48 o más fibras separadas. En el caso del cobre, sería necesario tender un cable UTP para cada circuito. La fibra puede transportar muchos más bits por segundo y llevarlos a distancias mayores que el cobre.

En general, un cable de fibra óptica se compone de cinco partes: el núcleo, el revestimiento, un amortiguador, un material resistente y un revestimiento exterior.



<sup>5</sup>Fig 2.4 Fibra óptica

---

<sup>5</sup> Imagen de cable de fibra óptica multimodo tomada desde [www.wikipedia.com](http://www.wikipedia.com) en español

El núcleo es el elemento que transmite la luz y se encuentra en el centro de la fibra óptica, todas las señales luminosas viajan a través del núcleo, es en general, vidrio fabricado de una combinación de dióxido de silicio (sílice) y otros elementos. La fibra multimodo usa un tipo de vidrio denominado vidrio de índice graduado para su núcleo, este vidrio tiene un índice de refracción menor hacia el borde externo del núcleo, de esta manera el área externa del núcleo es ópticamente menos densa que el centro y la luz puede viajar más rápidamente en la parte externa del núcleo. Se utiliza este diseño porque un rayo de luz que sigue un modo que pasa directamente por el centro del núcleo no viaja tanto como un rayo que sigue un modo que rebota en la fibra, todos los rayos deberían llegar al extremo opuesto de la fibra al mismo tiempo, entonces, el receptor que se encuentra en el extremo de la fibra, recibe un fuerte flash de luz y no un pulso largo y débil.

Alrededor del núcleo se encuentra el revestimiento. El revestimiento también está fabricado con sílice pero con un índice de refracción menor que el del núcleo, los rayos de luz que se transportan a través del núcleo de la fibra se reflejan sobre el límite entre el núcleo y el revestimiento a medida que se mueven a través de la fibra por reflexión total interna. El cable de fibra óptica multimodo estándar es el tipo de cable de fibra óptica que más se utiliza en las LAN. Un cable de fibra óptica multimodo estándar utiliza una fibra óptica con núcleo de 62,5 ó 50 micrones y un revestimiento de 125 micrones de diámetro. A menudo, recibe el nombre de fibra óptica de 62,5/125 ó 50/125 micrones. Un micrón es la millonésima parte de un metro ( $1\mu$ ).

Alrededor del revestimiento se encuentra un material amortiguador que es generalmente de plástico que ayuda a proteger al núcleo y al revestimiento de cualquier daño. Existen dos diseños básicos para cable. Son los diseños de cable de amortiguación estrecha y de tubo libre, la mayoría de las fibras utilizadas en

la redes LAN son de cable multimodo con amortiguación estrecha, los cables con amortiguación estrecha tienen material amortiguador que rodea y está en contacto directo con el revestimiento, la diferencia más práctica entre los dos diseños está en su aplicación. El cable de tubo suelto se utiliza principalmente para instalaciones en el exterior de los edificios mientras que el cable de amortiguación estrecha se utiliza en el interior de los edificios. El material resistente rodea al amortiguador, evitando que el cable de fibra óptica se estire cuando se tira de él, el material utilizado generalmente es el Kevlar, el mismo material que se utiliza para fabricar los chalecos a prueba de balas.

El último elemento es el revestimiento exterior, rodea al cable para así proteger la fibra de abrasión, solventes y demás contaminantes, el color del revestimiento exterior de la fibra multimodo es en general anaranjado, pero puede encontrarse en otros colores también.

Los Diodos de Emisión de Luz Infrarroja (LED) o los Emisores de Láser de Superficie de Cavidad Vertical (VCSEL) son dos tipos de fuentes de luz utilizadas normalmente con fibra multimodo. Se puede utilizar cualquiera de los dos. Los LED son un poco más económicos de fabricar y no requieren tantas normas de seguridad como el láser, sin embargo los LED no pueden transmitir luz por un cable a tanta distancia como el láser, la fibra multimodo (62,5/125) puede transportar datos a distancias de hasta 2000 metros (6.560 pies).

### **2.3.2 Fibra Monomodo**

La fibra monomodo consta de las mismas partes que una multimodo, el revestimiento exterior de la fibra monomodo es generalmente, de color amarillo, la mayor diferencia entre la fibra monomodo y la multimodo es que la



monomodo permite que un solo modo de luz se propague a través del núcleo de menor diámetro de la fibra óptica el núcleo de una fibra monomodo tiene de ocho a diez micrones de diámetro, los más comunes son los núcleos de nueve micrones. La marca 9/125 que aparece en el revestimiento de la fibra monomodo indica que el núcleo de la fibra tiene un diámetro de 9 micrones y que el revestimiento que lo envuelve tiene 125 micrones de diámetro.

En una fibra monomodo se utiliza un láser infrarrojo como fuente de luz el rayo de luz que el láser genera, ingresa al núcleo en un ángulo de 90 grados, como consecuencia, los rayos de luz que transportan datos en una fibra monomodo son básicamente transmitidos en línea recta directamente por el centro del núcleo, esto aumenta en gran medida, tanto la velocidad como la distancia a la que se pueden transmitir los datos. Por su diseño, la fibra monomodo puede transmitir datos a mayores velocidades (ancho de banda) y recorrer mayores distancias de tendido de cable que la fibra multimodo, la fibra monomodo puede transportar datos de LAN a una distancia de hasta 3000 metros, aunque esta distancia se considera un estándar, existen nuevas tecnologías que han incrementado esta distancia. La fibra multimodo sólo puede transportar datos hasta una distancia de 2000 metros, las fibras monomodo y el láser son más costosos que los LED y la fibra multimodo, debido a estas características, la fibra monomodo es la que se usa con mayor frecuencia para la conectividad entre edificios o backbones de Internet.

## 2.4 Transceivers

La mayoría de los datos que se envían por una LAN se envían en forma de señales eléctricas, sin embargo, los enlaces de fibra óptica utilizan luz para enviar datos, hace falta algún elemento para convertir la electricidad en luz y, en el otro extremo de la fibra, para convertir la luz nuevamente en electricidad, esto significa que se requiere un transmisor y un receptor, el transmisor recibe los datos que se deben transmitir desde los switches y routers, estos datos tienen forma de señales eléctricas, el transmisor convierte las señales electrónicas en pulsos de luz equivalentes, existen dos tipos de fuentes de luz que se utilizan para codificar y transmitir los datos a través del cable:

- Un diodo emisor de luz (LED) que produce luz infrarroja con longitudes de onda de 850 nm o 1310 nm. Se utilizan con fibra multimodo en las LAN. Para enfocar la luz infrarroja en el extremo de la fibra, se utilizan lentes.
- Amplificación de la luz por radiación por emisión estimulada (LASER) una fuente de luz que produce un fino haz de intensa luz infrarroja, generalmente, con longitudes de onda de 1310nm o 1550 nm. Los láseres se usan con fibra monomodo para las grandes distancias de los backbones; Se debe tener mucho cuidado para evitar daños a la vista.

En el otro extremo de la fibra óptica conectada al transmisor se encuentra el receptor, este funciona casi como una célula fotoeléctrica en una calculadora solar, cuando la luz llega al receptor se genera electricidad, la primera tarea del receptor es detectar el pulso de luz que llega desde la fibra, después el receptor convierte el pulso de luz nuevamente en la señal eléctrica original tal como ingresó al transmisor al otro extremo de la fibra, ahora la señal nuevamente adquiere la forma de cambios de voltaje, está lista para ser enviada por el cable de cobre al dispositivo electrónico receptor, como por ejemplo, una computadora, switch o router. Los dispositivos semiconductores que se utilizan

generalmente como receptores con enlaces de fibra óptica reciben el nombre de diodos p-intrínsecos-n (fotodiodos PIN).

Los fotodiodos PIN están fabricados para ser sensibles a 850, 1310 ó 1550 nm de luz que el transmisor genera al otro extremo de la fibra, cuando un pulso de luz de la longitud de onda adecuada da en el fotodiodo PIN, éste rápidamente genera una corriente eléctrica de voltaje apropiado para la red, cuando la luz deja de iluminar el fotodiodo PIN, éste deja de generar voltaje al instante, esto genera cambios de voltaje que representan los unos y ceros de los datos en el cable de cobre.

Hay conectores unidos a los extremos de las fibras de modo que éstas puedan estar conectadas a los puertos del transmisor y del receptor, el tipo de conector que se usa con mayor frecuencia con la fibra multimodo es el Conector Suscriptor (conector SC), en una fibra monomodo, el conector de Punta Recta (ST) es el más frecuentemente utilizado

## **2.5 Medios inalámbricos**

Hoy en día no existe una interoperabilidad entre todas las tecnologías y estándares para redes inalámbricas como existe en las redes cableadas, sin embargo la IEEE es la principal generadora de estándares para las redes inalámbricas, los estándares han sido creados en el marco de las reglamentaciones creadas por el Comité Federal de Comunicaciones (Federal Communications Commission - FCC).

La tecnología clave que contiene el estándar 802.11 es el Espectro de Dispersión de Secuencia Directa (DSSS). El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma. El siguiente estándar aprobado fue el

802.11b, que aumentó las capacidades de transmisión a 11 Mbps. Aunque las WLAN de DSSS podían interoperar con las WLAN de Espectro de Dispersión por Salto de Frecuencia (FHSS), se presentaron problemas que motivaron a los fabricantes a realizar cambios en el diseño, en este caso, la tarea de la IEEE fue simplemente crear un estándar que coincidiera con la solución del fabricante, 802.11b también recibe el nombre de Wi-Fi™ o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS, esta compatibilidad es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso.

Los dispositivos de 802.11b logran un mayor índice de tasa de transferencia de datos ya que utilizan una técnica de codificación diferente a la del 802.11, permitiendo la transferencia de una mayor cantidad de datos en la misma cantidad de tiempo, la mayoría de los dispositivos 802.11b todavía no alcanzan tasa de transferencia de 11 Mbps y, por lo general, trabajan en un intervalo de 2 a 4 Mbps.

802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHZ, el uso del rango de 5 GHZ no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHZ. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como "duplicación de la velocidad" ha alcanzado los 108 Mbps. En las redes de producción, la velocidad estándar es de 20-26 Mbps.

802.11g proporciona el mismo ancho de banda que el 802.11a pero además es compatible con 802.11b mediante la modulación de multiplexión por

división de frecuencia ortogonal (Orthogonal Frequency Division Multiplexing; OFDM) operando a una frecuencia de 2.4 GHZ en la banda de transmisión.

Una red inalámbrica puede constar de tan sólo dos dispositivos: los nodos pueden ser simples estaciones de trabajo de escritorio o computadoras de mano, equipada con NIC inalámbricas, se puede establecer una red 'ad hoc' comparable a una red cableada de par a par, ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia, otro problema de este tipo de red es la compatibilidad, muchas veces las NIC de diferentes fabricantes no son compatibles. Para resolver el problema de la compatibilidad, se suele instalar un punto de acceso (AP) para que actúe como hub central para el modo de infraestructura de la WLAN, el AP se conecta mediante cableado a la LAN cableada a fin de proporcionar acceso a Internet y conectividad a la red cableada, los AP están equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda, según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente, por lo general, el alcance es de 91.44 a 152.4 metros (300 a 500pies). Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición, esta superposición permite pasar de una celda a otra (roaming), esto es muy parecido a los servicios que brindan las empresas de teléfonos celulares. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN, aunque los estándares del IEEE no determinan nada al respecto, es aconsejable una superposición de un 20 o 30%, este índice de superposición permitirá el roaming entre las celdas y así la actividad de desconexión y reconexión no tendrá interrupciones.

Cuando se activa un cliente dentro de la WLAN, la red comenzará a "escuchar" para ver si hay un dispositivo compatible con el cual "asociarse". Esto se conoce como "escaneo" y puede ser activo o pasivo. El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red, este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo, se completan los pasos de autenticación y asociación.

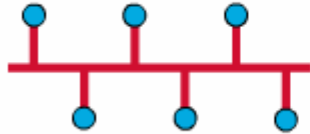
Los nodos de escaneo pasivo esperan las tramas de administración de beacons (beacons) que son transmitidas por el AP (modo de infraestructura) o nodos pares (ad hoc). Cuando un nodo recibe un beacon que contiene el SSID de la red a la que se está tratando de conectar, se realiza un intento de conexión a la red, el escaneo pasivo es un proceso continuo y los nodos pueden asociarse o desasociarse de los AP con los cambios en la potencia de la señal.

## 2.6 TOPOLOGÍAS

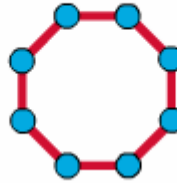
### 2.6.1 TOPOLOGÍA FÍSICA

La topología de red define la estructura de una red, una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios, la otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Las topologías físicas más usadas son las siguientes:



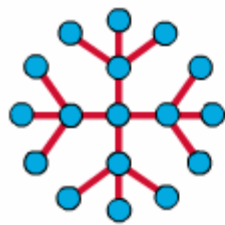
BUS



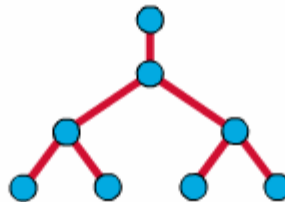
ANILLO



ESTRELLA



ESTRELLA EXTENDIDA



JERÁRQUICA



MALLA

<sup>6</sup>Fig. 2.4 Topologías físicas de red

<sup>6</sup> Dibujos ilustrativos de las formas físicas más comunes de topologías de redes tomados desde [www.monografias.com](http://www.monografias.com)

- Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La topología en estrella conecta todos los cables con un punto central de concentración, regularmente una MAU.
- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con una computadora que controla el tráfico de la topología.
- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.



## 2.6.2 TOPOLOGÍA LÓGICA

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red, no existe una orden que las estaciones deban seguir para utilizar la red, es por orden de llegada. Ethernet funciona así.

La segunda topología lógica es la transmisión de tokens, controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial, Cuando un host recibe el token, ese host puede enviar datos a través de la red, si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

## **CAPITULO III**

---

# ***ETHERNET***

### **3 ETHERNET**

#### **3.1 HISTORIA**

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet, desde su comienzo en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad, desde el momento en que aparece un nuevo medio, como la fibra óptica, Ethernet se adapta para sacar ventaja de un ancho de banda superior y de un menor índice de errores que la fibra ofrece, ahora el mismo protocolo que transportaba datos a 3 Mbps en 1973 transporta datos a 10 Gbps.

El éxito de Ethernet se debe a los siguientes factores:

- 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).

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales interfirieran entre sí, este problema de acceso por varios usuarios a un medio compartido se estudió a principios de los 70 en la Universidad de Hawai, se desarrolló un sistema llamado Alohanet para permitir que varias estaciones de las Islas de Hawai tuvieran acceso estructurado a la banda de radiofrecuencia compartida en la atmósfera, más tarde, este trabajo sentó las bases para el método de acceso a Ethernet conocido como CSMA/CD.

La primera LAN del mundo fue la versión original de Ethernet. Robert Metcalfe y sus compañeros de Xerox la diseñaron hace más de treinta años, el primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Company, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto, los primeros productos que se desarrollaron utilizando el estándar de Ethernet se vendieron a principios de la década de 1980. Ethernet transmitía a una velocidad de hasta 10 Mbps en cable coaxial grueso a una distancia de hasta 2 kilómetros, en 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN, estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el modelo OSI de la Organización Internacional de Estándares (ISO), por eso, el estándar IEEE 802.3 debía cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI, como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Las diferencias entre los dos estándares fueron tan insignificantes que cualquier tarjeta de interfaz de la red de Ethernet (NIC) puede transmitir y recibir tanto tramas de Ethernet como de 802.3. Básicamente, Ethernet y IEEE 802.3 son un mismo estándar.

El ancho de banda de 10 Mbps de Ethernet era más que suficiente para las lentas PC's de los años 80, a principios de los 90, las PC's se volvieron mucho más rápidas, los tamaños de los archivos aumentaron y se producían cuellos de botella en el flujo de los datos, la mayoría a causa de una baja disponibilidad del ancho de banda, en 1995, el IEEE anunció un estándar para la Ethernet de 100 Mbps, más tarde siguieron los estándares para Ethernet de un gigabit por segundo (Gbps, mil millones de bits por segundo) en 1998 y 1999.

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, el ancho de banda de la red podría aumentarse muchas veces sin cambiar la tecnología base de Ethernet.

### **3.2 DENOMINACIONES**

Ethernet es un conjunto de tecnologías que incluye Legacy, Fast Ethernet y Gigabit Ethernet. Las velocidades de Ethernet pueden ser de 10, 100, 1000 ó 10000 Mbps. El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet.

Cuando es necesario expandir Ethernet para agregar un nuevo medio o capacidad, el IEEE publica un nuevo suplemento del estándar 802.3. Los nuevos suplementos reciben una designación de una o dos letras, como por ejemplo: 802.3u. También se asigna una descripción abreviada (identificador) al suplemento.

La descripción abreviada consta de:

- Un número que indica el número de Mbps que se transmiten.
- La palabra "base", que indica que se utiliza la señalización banda base.
- Una o más letras del alfabeto que indican el tipo de medio utilizado (F = cable de fibra óptica, T = par trenzado de cobre no blindado).

Velocidades	Métodos de señalización	Medios
10	Base	2
100	Broad	5
1000		T
1000		TX
		SX (FX onda short)
		LX ( FX onda long)

<sup>7</sup> Tabla 3.1 Comparación de tecnologías

Ethernet emplea señalización banda base, la cual utiliza todo el ancho de banda del medio de transmisión. La señal de datos se transmite directamente por el medio de transmisión. Ethernet utiliza la señalización banda base, la cual usa la totalidad del ancho de banda del medio de transmisión. La data se transmite directamente sobre el medio de transmisión.

En la señalización banda ancha, la señal de datos nunca se transmite directamente sobre el medio. Ethernet usaba señalización de banda ancha en el estándar 10BROAD36. 10BROAD36 es el estándar IEEE para una red Ethernet 802.3 que usa cable coaxial grueso a 10 Mbps como medio de transmisión de banda ancha. 10BROAD36 se considera ahora obsoleto. Una señal analógica, o señal portadora, es modulada por la data, y la señal portadora modulada es transmitida. En la radio difusión y en la TV por cable se usa la señalización de banda ancha. Una señal analógica (señal portadora) es modulada por la data y se transmite la señal portadora modulada. Las estaciones de radio y la TV por cable utilizan la señalización banda ancha. Algunos estándares Ethernet son:

---

<sup>7</sup> Tabla comparativa de velocidades de tecnologías Ethernet

<b>802.7</b>	Grupo de asesoramiento técnico de banda ancha (BBTAG)
<b>802.16</b>	Acceso inalámbrico de banda ancha (BBWA)
<b>802.14</b>	Red de comunicación de banda ancha basada en CATV
<b>802.3</b>	CSMA/CD
<b>802.12</b>	Prioridad de demanda
<b>802.8</b>	Grupo de asesoramiento técnico en fibra óptica (FOTAG)
<b>802.1</b>	Estándar de interfaz de alto nivel (HILI)
<b>802.9</b>	LAN de servicios integrados (ISLAN)
<b>802.2</b>	Control de enlace lógico (LLC)
<b>802.6</b>	Red de área metropolitana (MAN)
<b>802.17</b>	Grupo de anillo de paquete flexible (RPRSG)
<b>802.0</b>	Estándares para redes LAN y MAN SEC-IEEE
<b>802.10</b>	Estándar para seguridad de LAN inter operable (SILS)
<b>802.4</b>	Token Bus
<b>802.5</b>	Token Ring
<b>802.11</b>	LAN inalámbrica (WLAN)
<b>802.15</b>	Red de área personal inalámbrica (WPAN)

<sup>8</sup> Tabla 3.2 IEEE 802

### 3.3 MODELO OSI

En sus inicios, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de red, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red. Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión, de la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información, el mismo problema surgía con las empresas que desarrollaban tecnologías de red privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo

<sup>8</sup> Tabla de estándares 802 más comunes utilizados en Ethernet

de empresas controlan todo uso de la tecnología. Las tecnologías de red que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de red, como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes, en base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO, proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red, aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI, esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos, se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo OSI reduce complejidad, estandariza las interfaces, facilita el diseño modular, asegura la interoperabilidad de la tecnología, acelera la evolución y simplifica la enseñanza y el aprendizaje, todo esto gracias a que se divide en 7 capas, cada una con una función específica:



<b>CAPAS</b>	<b>FUNCIÓN</b>
7.APLICACIÓN	Procesos de red a aplicaciones, suministra servicios de red a los procesos de aplicaciones.
6.PRESENTACIÓN	Representación de datos, formateo de datos para asegurar que sean legibles, estructura de datos y sintaxis
5.SESIÓN	Comunicación entre hosts, establece, administra y termina sesiones entre aplicaciones.
4.TRANSPORTE	Conexión de extremo a extremo: establece, mantiene y termina circuitos virtuales, detección de fallas y control de flujo de información de recuperación.
3.RED	Dirección de red y determinación de mejor ruta. Provee transparencia confiable de datos a través de los medios, y conectividad y selección de ruta entre sistemas.
2.ENLACE DE DATOS	Control directo de enlaces, acceso a los medios. Control de Acceso a Medios y Enlace de control lógico
1.FÍSICA	Transmisión binaria. Cables, conectores, voltajes, velocidades de transmisión de datos

<sup>9</sup>Tabla 3.3 Capas del modelo OSI

### 3.4 ETHERNET Y 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.

Enlace de datos	LLC (control de enlace lógico)
	MAC (control de acceso al medio)
Física	

Ethernet en la capa 1 incluye las interfaces con los medios, señales, corrientes de bits que se transportan en los medios, componentes que transmiten la señal a los medios y las distintas topologías. La Capa 1 tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones. La Capa 2 se ocupa de estas limitaciones, las

<sup>9</sup> Tabla con número y definición de las capas del modelo OSI tomada desde [www.cisco.com](http://www.cisco.com)

subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y comunicación con la computadora, 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.

Veamos las tecnologías Ethernet más utilizadas y su interacción con la capa 2:

Subcapa de Control de Acceso Lógico	
Subcapa de Control de Acceso al Medio	
Subcapa de señalización física	Medio físico
10BASE5 (500m) 50ohm coax n-style	10BASE2(185m) 50ohm Coax BNC
10BASET(100m) 100ohm UTP RJ-45	100BASE-TX (100m) 100ohm UTP-RJ45
100BASE-CX (25m) 150ohm UTP RJ-45	100BASE-T (100m) 100ohm UTP-RJ45
100BASE-SX (220-550m) MM FiberSC	100BASE-LX (550-5000) MM o SM Fiber SC

<sup>10</sup> Tabla 3.4 Diseño de capa 2 del modelo OSI

### 3.5 DIRECCIONES MAC

Para permitir el envío local de las tramas en Ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar las computadoras y las interfaces de manera exclusiva, Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales, los primeros seis dígitos hexadecimales, que el IEEE administra, identifican al fabricante o al vendedor, esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI), los seis dígitos hexadecimales restantes representan el número de serie de la interfaz u otro valor administrado por el proveedor mismo del equipo, las direcciones MAC a veces se denominan

<sup>10</sup> Tabla ilustrativa de las subcapas de la capa 2 del modelo OSI tomada desde [www.cisco.com](http://www.cisco.com)

direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la NIC.

En la capa MAC de enlace de datos se agregan encabezados e información final a los datos de la capa superior. El encabezado y la información final contienen información de control destinada a la capa de enlace de datos en el sistema destino. Los datos de las entidades de las capas superiores se encapsulan dentro de la trama de la capa de enlace, entre el encabezado y el cierre, para luego ser enviada sobre la red.

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.

En una red Ethernet, 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.

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

### 3.6 TRAMA

Las corrientes de bits codificadas (datos) en medios físicos representan un logro tecnológico extraordinario, pero por sí solas no bastan para que las comunicaciones puedan llevarse a cabo. El entramado ayuda a obtener información esencial que, de otro modo, no se podría obtener solamente con las corrientes de bits codificadas: Entre los ejemplos de dicha información se incluye:

- Cuáles son los computadores que se comunican entre sí
- Cuándo comienza y cuándo termina la comunicación entre computadores individuales
- Proporciona un método para detectar los errores que se produjeron durante la comunicación.
- Quién tiene el turno para "hablar" en una "conversación" entre computadores

El entramado es el proceso de encapsulamiento de la Capa 2. Una trama es la unidad de datos del protocolo de la Capa 2.

Hay varios tipos de tramas que se describen en diversos estándares. Una trama genérica tiene secciones denominadas campos, y cada campo está formado por bytes. Los nombres de los campos son los siguientes:

- Campo de inicio de trama
- Campo de dirección
- Campos de longitud/tipo
- Campo de datos
- Campo de secuencia de verificación de trama (FCS)

La razón del envío de tramas es hacer que los datos de las capas superiores, especialmente los datos de aplicación del usuario, lleguen desde el origen hasta el destino, el paquete de datos incluye el mensaje a ser enviado, o los datos de aplicación del usuario, puede resultar necesario agregar bytes de relleno de modo que las tramas tengan una longitud mínima para los fines de temporización. Los bytes de control de enlace lógico (LLC) también se incluyen en el campo de datos de las tramas del estándar IEEE, la subcapa LLC toma los datos de protocolo de la red, un paquete IP, y agrega información de control para ayudar a entregar ese paquete IP al nodo de destino. La Capa 2 se comunica con las capas de nivel superior a través de LLC.

Todas las tramas y los bits, bytes y campos ubicados dentro de ellas, están susceptibles a errores de distintos orígenes, el campo de Secuencia de verificación de trama (FCS) contiene un número calculado por el nodo de origen en función de los datos de la trama, entonces, esta FCS se agrega al final de la trama que se envía, cuando la computadora destino recibe la trama, se vuelve a calcular el número FCS y se compara con el número FCS que se incluye en la trama, si los dos números son distintos, se da por sentado que se ha producido un error, se descarta la trama y se le puede pedir al origen que vuelva a realizar la transmisión. Debido a que la fuente no puede detectar que la trama ha sido descartada, se deben iniciar retransmisiones por un protocolo de capa superior orientado a conexión que provea control de flujo de datos. Usualmente se dan retransmisiones debido a que los protocolos, como TCP/IP, requieren que las estaciones envíen tramas de reconocimiento, ACK, dentro de un tiempo preestablecido.

Hay tres formas principales para calcular el número de Secuencia de verificación de trama:

- **Verificación por redundancia cíclica (CRC):** Realiza cálculos en los datos.
- **Paridad bidimensional:** Coloca a cada uno de los bytes en un arreglo bidimensional y realiza chequeos verticales y horizontales de redundancia sobre el mismo, creando así un byte extra, que resulta en un número par o impar de unos binarios.
- **Checksum (suma de verificación) de Internet:** Agrega los valores de todos los bits de datos para obtener una suma

La estructura de una trama Ethernet es la siguiente:

Trama Ethernet							
Preámbulo	SFD	Destino	Origen	Long/tipo	Datos	Relleno	FCS
7	1	6	6	2	46 a 1500		4

<sup>11</sup> Tabla 3.5 Trama Ethernet

El SFD es el delimitador de inicio de trama

En los campos destino y origen van las MAC de cada host

En longitud y campo, se indica longitud si el tamaño es menor a 0x600hex, si no se indica el tipo de protocolo que se envía

En el campo datos, si el tamaño es menor a 46 octetos, se debe agregar el relleno al final

Y el campo de FCS, utiliza suma de comprobación (CRC)

---

<sup>11</sup> Ilustración de la división de una trama Ethernet tomada desde [www.cisco.com](http://www.cisco.com)

### 3.7 PROTOCOLOS MAC

MAC se refiere a los protocolos que determinan cuál de las computadoras 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 y hay dos categorías amplias de Control de acceso al medio: determinística (por turnos) y la no determinística (el que primero llega, primero se sirve).

Ejemplos de protocolos determinísticos son: el Token Ring y el FDDI. En una red Token Ring, los host individuales se disponen en forma de anillo y un token de datos especial se transmite por el anillo a cada host en secuencia. Cuando un host desea transmitir, retiene el token, transmite los datos por un tiempo limitado y luego envía el token al siguiente host del anillo, el Token Ring es un entorno sin colisiones ya que sólo un host es capaz de transmitir a la vez.

Los protocolos MAC no determinísticos utilizan el enfoque de "el primero que llega, el primero que se sirve". El CSMA/CD (Carrier Sense Multiple Access with Collision Detection) es un sistema simple, 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 tres tecnologías comunes de Capa 2 son Token Ring, FDDI y Ethernet. Las tres especifican aspectos de la Capa 2, LLC, denominación, entramado y MAC, así como también los componentes de señalización y de medios de Capa 1.

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)
- **Token Ring:** topología lógica de anillo (en otras palabras, el flujo de información se controla en forma de anillo) y una topología física en estrella (en otras palabras, está cableada en forma de estrella)
- **FDDI:** topología lógica de anillo (el flujo de información se controla en un anillo) y topología física de anillo doble (cableada en forma de anillo doble)

### 3.8 MÉTODO DE ACCESO CSMA/CD

Ethernet es una tecnología de broadcast de medios compartidos y el método de acceso CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones) que se usa en Ethernet ejecuta tres funciones:

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

En el método de acceso CSMA/CD los dispositivos de red 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 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 no está ocupado, comenzará a transmitir y a escuchar, 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 red detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios.

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, cabe señalar que los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

### **3.9 TEMPORIZACIÓN**

Cualquier estación de una red Ethernet que desee transmitir un mensaje, primero "escucha" para asegurar que ninguna otra estación se encuentre transmitiendo, si el cable está en silencio, la estación comienza a transmitir de inmediato, la señal eléctrica tarda un tiempo en transportarse por el cable (retardo) y cada repetidor subsiguiente introduce una pequeña cantidad de latencia en el envío de la trama desde un puerto al siguiente, debido al retardo y a la latencia, es posible que más de una estación comience a transmitir a la vez o casi al mismo tiempo esto produce una colisión. Si la estación conectada opera en full duplex entonces la estación puede enviar y recibir de forma simultánea y no se deberían producir colisiones, las operaciones en full-duplex también cambian las consideraciones de temporización y eliminan el concepto de la ranura temporal. La operación en full-duplex permite diseños de arquitectura de redes más grandes ya que se elimina la restricción en la temporización para la detección de colisiones.

En el modo half duplex, si se asume que no se produce una colisión, la estación transmisora enviará 64 bits de información de sincronización de tiempos que se conoce como preámbulo, la estación transmisora entonces transmitirá la siguiente información:

- Información de las direcciones MAC destino y origen.
- Otra información relacionada con el encabezado.
- Los datos
- La checksum (FCS) utilizada para asegurar que no se haya dañado el mensaje durante la transmisión.

Las estaciones que reciben la trama recalculan la FCS para determinar si el mensaje entrante es válido y luego envían los mensajes válidos a la siguiente capa superior.

Los tiempos de temporización para tecnologías Ethernet son las siguientes

Velocidad de Ethernet	Periodo de bit
10 Mbps	100ns
100 Mbps	10ns
1000Mbps = 1 Gbps	1ns
10000Mbps = 10 Gbps	0.1ns

<sup>12</sup> Tabla 3.6 Temporización

Para que Ethernet CSMA/CD opere, la estación transmisora debe reconocer la colisión antes de completar la transmisión de una trama del tamaño mínimo. A 100 Mbps, la temporización del sistema apenas es capaz de funcionar con cables de 100 metros. A 1000 Mbps, ajustes especiales son necesarios ya que se suele transmitir una trama completa del tamaño mínimo antes de que el primer bit alcance el extremo de los primeros 100 metros de cable UTP. Por este motivo, no se permite half duplex en la Ethernet de 10 Gigabits.

---

<sup>12</sup> Tabla comparativa de velocidades en las distintas tecnologías Ethernet

### 3.10 ESPACIO Y POSTERGACIÓN

El espacio mínimo entre dos tramas que no han sufrido una colisión recibe el nombre de espacio entre tramas. Se mide desde el último bit del campo de la FCS de la primera trama hasta el primer bit del preámbulo de la segunda trama, una vez enviada la trama, todas las estaciones de Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir, de manera legal, la siguiente trama. En versiones de Ethernet más veloces, el espacio sigue siendo el mismo, 96 tiempos de bit, pero el tiempo que se requiere para dicho intervalo se vuelve proporcionalmente más corto, este intervalo se conoce como separación. El propósito del intervalo es permitir que las estaciones lentas tengan tiempo para procesar la trama anterior y prepararse para la siguiente trama.

El espacio entre tramas es el siguiente <sup>13</sup> Tabla 3.7 Espacios

Velocidad	Espacio entre tramas	Tiempo requerido
10 Mbps	96 tiempos de bit	9.6 $\mu$ s
100 Mbps	96 tiempos de bit	0.96 $\mu$ s
1000Mbps = 1 Gbps	96 tiempos de bit	0.096 $\mu$ s
10000Mbps = 10 Gbps	96 tiempos de bit	0.0096 $\mu$ s

El tiempo de ranura temporal es el siguiente <sup>14</sup> Tabla 3.8 Ranuras

Velocidad	Ranura temporal	Intervalo de tiempo
10 Mbps	512 tiempos de bit	51.2 $\mu$ s
100 Mbps	512 tiempos de bit	5.12 $\mu$ s
1000Mbps = 1 Gbps	4096 tiempos de bit	4.096 $\mu$ s
10000Mbps = 10 Gbps	No aplica	No aplica

Si la capa MAC no puede enviar la trama después de dieciséis intentos, abandona el intento y genera un error en la capa de red, este caso es verdaderamente raro y suele suceder sólo cuando se producen cargas en la red muy pesadas o cuando se produce un problema físico en la red

<sup>13</sup> Tabla comparativa de tramas en las tecnologías Ethernet más comunes

<sup>14</sup> Tabla comparativa de ranuras entre tramas de las tecnologías Ethernet más comunes

### 3.11 ERRORES

El estado de error más común en redes Ethernet son las colisiones, estas son el mecanismo para resolver la contención del acceso a la red, unas pocas colisiones proporcionan una forma simple y sin problemas, que usa pocos recursos, para que los nodos de la red manejen la contención para el recurso de red, cuando la contención de la red se vuelve demasiado grave, las colisiones se convierten en un impedimento significativo para la operación útil de la red.

Las colisiones producen una pérdida del ancho de banda de la red equivalente a la transmisión inicial y a la señal de congestión de la colisión. Esto es una demora en el consumo y afecta a todos los nodos de la red causando posiblemente una significativa reducción en su rendimiento.

La mayoría de las colisiones se producen cerca del comienzo de la trama, a menudo, antes de la SFD, las colisiones que se producen antes de la SFD generalmente no se informan a las capas superiores, como si no se produjeran, tan pronto como se detecta una colisión, las estaciones transmisoras envían una señal de congestión de 32 bits, esto se hace de manera que se corrompen por completo los datos transmitidos y todas las estaciones tienen la posibilidad de detectar la colisión.

Una señal de congestión puede estar compuesta por cualquier dato binario siempre que no forme una checksum apropiada para la porción de la trama ya transmitida, el patrón de datos que se observa con mayor frecuencia para una señal de congestión es simplemente un patrón de uno, cero, uno, cero que se repite, al igual que el Preámbulo, cuando se observa con un analizador de protocolos, este patrón aparece como una secuencia repetida de A ó 5 hexadecimales. Los mensajes corrompidos, transmitidos de forma parcial, generalmente se conocen como fragmentos de colisión o runts. Las colisiones

normales tienen menos de 64 octetos de largo y, por lo tanto, reprobaban tanto la prueba de longitud mínima como la prueba de la checksum de FCS.

Una colisión simple es una colisión que se detecta al tratar de transmitir una trama, pero en el siguiente intento es posible transmitir la trama con éxito, las colisiones múltiples indican que la misma trama colisionó una y otra vez antes de ser transmitida con éxito, los resultados de las colisiones, los fragmentos de colisión, son tramas parciales o corrompidas de menos de 64 octetos y que tienen una FCS inválida.

Los tres tipos de colisiones son

- Locales
- Remotas
- Tardías

Para crear una colisión local en un cable coaxial (10BASE2 y 10BASE5), la señal viaja por el cable hasta que encuentra una señal que proviene de la otra estación, entonces las formas de onda se superponen cancelando algunas partes de la señal y reforzando o duplicando otras la duplicación de la señal empuja el nivel de voltaje de la señal más allá del máximo permitido. Esta condición de exceso de voltaje es detectada por todas las estaciones en el segmento local del cable como una colisión.

En el cable UTP como 10BASE-T, 100BASE-TX y 1000BASE-T, la colisión se detecta en el segmento local sólo cuando una estación detecta una señal en el par de recepción (RX) al mismo tiempo que está enviando una señal en el par de transmisión (TX), como las dos señales se encuentran en pares diferentes, no se produce un cambio en la característica de la señal.

Las colisiones se reconocen en UTP sólo cuando la estación opera en half duplex, la única diferencia funcional entre la operación en half duplex y full duplex en este aspecto es si es posible o no que los pares de transmisión y de recepción se utilicen al mismo tiempo, si la estación no participa en la transmisión, no puede detectar una colisión local. Por otra parte, una falla en el cable, como por ejemplo una diafonía excesiva, puede hacer que una estación perciba su propia transmisión como si fuera una colisión local.

La característica de una colisión remota es que es una trama que mide menos que la longitud mínima, tiene una checksum de FCS inválida, pero no muestra el síntoma de colisión local del exceso de voltaje o actividad de transmisión/recepción simultánea, este tipo de colisión generalmente es el resultado de colisiones que se producen en el extremo lejano de una conexión con repetidores. El repetidor no envía un estado de exceso de voltaje y no puede hacer que una estación tenga ambos pares de transmisión y de recepción activos al mismo tiempo. La estación tendría que estar transmitiendo para que ambos pares estén activos y esto constituiría una colisión local. En las redes de UTP este es el tipo más común de colisión que se observa.

No hay posibilidad de que se produzca una colisión normal o legal después de que las estaciones transmitan los primeros 64 octetos de datos, las colisiones que se producen después de los primeros 64 octetos reciben el nombre de "colisiones tardías", la diferencia más importante entre las colisiones tardías y las colisiones que se producen antes de los primeros 64 octetos radica en que la NIC de Ethernet retransmitirá de forma automática una trama que ha sufrido una colisión normal, pero no retransmitirá automáticamente una trama que ha sufrido una colisión tardía. En lo que respecta a la NIC, todo salió bien y las capas superiores deben determinar si se perdió la trama, a diferencia de la retransmisión, una estación que detecta una colisión tardía la maneja de la misma forma que si fuera una colisión normal.

El conocimiento de los errores típicos es fundamental para entender tanto la operación como la detección de fallas de las redes Ethernet.

Las siguientes son las fuentes de error de Ethernet.

- **Colisión o runt:** Transmisión simultánea que se produce antes de haber transcurrido la ranura temporal.
- **Colisión tardía:** Transmisión simultánea que se produce después de haber transcurrido la ranura temporal.
- **Errores de intervalo, trama larga, jabber:** Transmisión excesiva o ilegalmente larga.
- **Trama corta, fragmento de colisión o runt:** Transmisión ilegalmente corta.
- **Error de FCS:** Transmisión dañada
- **Error de alineamiento:** Número insuficiente o excesivo de bits transmitidos.
- **Error de intervalo:** El número real y el informado de octetos en una trama no concuerda.
- **Fantasma o jabber:** Preámbulo inusualmente largo o evento de congestión.

Dentro de los errores más comunes de la FCS se encuentran los casos cuando una trama recibida que tiene una Secuencia de verificación de trama incorrecta, también conocido como error de CRC o de checksum y difiere de la transmisión original en al menos un bit, en una trama con error de FCS, es probable que la información del encabezado sea correcta, pero la checksum que calcula la estación receptora no concuerda con la checksum que adjunta la estación transmisora al extremo de la trama, por lo tanto, se descarta la trama.

Una gran cantidad de errores FCS provenientes de una sola estación indican, por lo general, una NIC defectuosa y/o falla o controladores dañados del software, o un cable defectuoso que conecta esa estación a la red, si los errores FCS están asociados con muchas estaciones, por lo general, pueden rastrearse a la presencia de un cableado defectuoso, una versión defectuosa del controlador de la NIC, un puerto de hub defectuoso o a ruido inducido en el sistema de cables.

### **3.12 NEGOCIACIONES**

Al crecer Ethernet de 10 a 100 y 1000 Mbps, fue necesario hacer que cada tecnología pudiera operar con las demás, al punto que las interfaces de 10, 100 y 1000 pudieran conectarse directamente, se desarrolló un proceso que recibe el nombre de “Auto-negociación” de las velocidades en half duplex o en full duplex, específicamente, en el momento en que se introdujo Fast Ethernet, el estándar incluía un método para configurar de forma automática una interfaz dada para que concordara con la velocidad y capacidades de la interfaz en el otro extremo del enlace este proceso define cómo las interfaces en los extremos del enlace pueden negociar de forma automática una configuración ofreciendo el mejor nivel de rendimiento común, presenta la ventaja adicional de involucrar sólo la parte inferior de la capa física.

La 10BASE-T requirió que cada estación transmitiera un pulso de enlace aproximadamente cada 16 milisegundos, siempre que la estación no estuviera transmitiendo un mensaje la Auto-Negociación adoptó esta señal y la denominó Pulso de enlace normal (NLP). Cuando se envía una serie de NLP en un grupo con el propósito de Auto-Negociación, el grupo recibe el nombre de ráfaga de Pulso de enlace rápido (FLP), cada ráfaga de FLP se envía a los mismos intervalos que un NLP y tiene como objetivo permitir que los antiguos dispositivos de 10BASE-T operen normalmente en caso de que reciban una ráfaga de FLP



La Auto-Negociación se logra al transmitir una ráfaga de Pulsos de Enlace de 10BASE-T desde cada uno de los dos extremos del enlace, la ráfaga comunica las capacidades de la estación transmisora al otro extremo del enlace, una vez que ambas estaciones han interpretado qué ofrece el otro extremo, ambas cambian a la configuración común de mayor rendimiento y establecen un enlace a dicha velocidad. Si algo interrumpe la comunicación y se pierde el enlace, los dos hosts intentan conectarse nuevamente a la velocidad de la última negociación. Si esto falla o si ha pasado demasiado tiempo desde que se perdió el enlace, el proceso de Auto-Negociación comienza de nuevo, es posible que se pierda el enlace debido a influencias externas tales como una falla en el cable o la emisión de una reconfiguración por uno de los hosts.

La Auto-Negociación es optativa para la mayoría de las implementaciones de Ethernet. Gigabit Ethernet requiere de su implementación aunque el usuario puede deshabilitarla, originalmente, la Auto-Negociación se definió para las implementaciones de UTP de Ethernet y se extendió para trabajar con otras implementaciones de fibra óptica.

Cuando una estación Auto-Negociadora realiza un primer intento de enlace, debe habilitarse a 100BASE-TX para que intente establecer un enlace de inmediato, si la señalización de la 100BASE-TX está presente y la estación admite 100BASE-TX, intentará establecer un enlace sin negociación. Si la señalización produce el enlace o se transmiten las ráfagas de FLP, la estación procederá con dicha tecnología, si el otro extremo del enlace no ofrece una ráfaga de FLP, pero a cambio, ofrece NLP, entonces el dispositivo supone automáticamente que es una estación 10BASE-T. Durante este intervalo inicial de prueba para otras tecnologías, la ruta de transmisión envía ráfagas de FLP. El estándar no permite la detección paralela de ninguna otra tecnología.

Si se establece un enlace a través de la detección paralela, se requiere una conexión en half duplex, son dos los métodos para lograr un enlace en full-duplex: Uno es a través de un ciclo de Auto-Negociación completo y el otro es forzar administrativamente a que ambos extremos del enlace realicen una conexión en full duplex.

Si se fuerza a un extremo del enlace a conectarse en full duplex, pero el otro extremo intenta Auto-Negociar, entonces seguramente se producirá una falta de concordancia en el duplex. Se producirán colisiones y errores en ese enlace, además, si se fuerza a un extremo a una conexión en full duplex, el otro también debe ser forzado. La excepción es Ethernet de 10 Gigabits que no admite la conexión en half duplex.

Las prioridades de transmisión en Ethernet son:

1000BASE-T en full duplex

1000BASE-T en half duplex

100BASE-TX full duplex

100BASE-TX half duplex

10BASE-T full duplex

10BASE-T half duplex

### **3.13 TECNOLOGÍAS**

#### **3.13.1 ETHERNET 10Mbps**

Las Ethernet de 10BASE5, 10BASE2 y 10BASE-T se consideran implementaciones antiguas de Ethernet, las características comunes de Ethernet antigua son los parámetros de temporización, el formato de trama, el proceso de transmisión y una regla básica de diseño.

Las Ethernet 10BASE5, 10BASE2 y 10BASE-T comparten los mismos parámetros de temporización. Por ejemplo, 1 tiempo de bit a 10 Mbps = 100 nanosegundos = 0,1 microsegundos = 1 diez millonésima parte de un segundo. Esto significa que en una red Ethernet de 10 Mbps, 1 bit en la subcapa MAC requiere de 100 nseg para ser transmitido.

Para todas las velocidades de transmisión Ethernet igual o por debajo de 1000 Mbps, la transmisión no debe ser menor al margen de tiempo “Slot time”. El margen de tiempo es apenas mayor al tiempo, que en teoría, le tomaría a una transmisión desde un extremo de la red llegar hasta el otro extremo ubicado a la máxima distancia legal posible de un dominio de colisión Ethernet, colisionar con otra transmisión en el último instante posible, y regresar al origen como fragmentos de la colisión para su detección.

Ethernet de 10Mbps tiene características de arquitectura comunes, en general las redes contienen varios tipos de medios, el estándar asegura que se mantenga la interoperabilidad, el diseño arquitectónico general es de suma importancia a la hora de implementar una red de medios mixtos. Resulta más fácil pasar los límites máximos de retardo a medida que la red crece, estos límites de temporización se basan en parámetros como:

- La longitud del cable y su retardo de propagación.
- El retardo de los repetidores.
- El retardo de los transceptores (transceivers)
- El acortamiento del intervalo entre las tramas.
- Los retardos dentro del host.

Ethernet de 10-Mbps opera dentro de los límites de temporización ofrecidos por una serie de no más de cinco segmentos, separados por no más de cuatro repetidores. Esto se conoce como la regla de 5-4-3. No se pueden conectar más de cuatro repetidores en serie entre dos estaciones lejanas. Además, no puede haber más de tres segmentos poblados entre dos estaciones lejanas.

Revisemos los parámetros de operación de las Ethernet 10Mbps

Parámetro	Valor
Periodo de bit	100ns
Ranura temporal	512tiempos de bit (64 octetos)
Espacio entre tramas	96 bits
Límite de intentos de colisión	16
Límite de postergación	10
Tamaño de congestión	32 bits
Tamaño de trama máximo	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Codificación	Manchester

<sup>15</sup> Tabla 3.9 Ethernet 10

### 3.13.2 ETHERNET 100Mbps

Ethernet de 100-Mbps también se conoce como Fast Ethernet (Ethernet Rápida), las dos tecnologías más importantes son 100BASE-TX, que es un medio UTP de cobre y 100BASE-FX, que es un medio multimodo de fibra óptica.

---

<sup>15</sup> Tabla de definición de parámetros de la tecnología Ethernet 10 Mbps

Las características comunes a 100BASE-TX y a 100BASE-FX son los parámetros de temporización, el formato de trama y algunas partes del proceso de transmisión, tanto 100BASE-TX como 100BASE-FX comparten los parámetros de temporización, un tiempo de bit a 100-Mbps = 10 nseg = 0,01 microsegundos = 1 100-millonésima parte de un segundo.

Fast Ethernet representa un aumento de 10 veces en la velocidad respecto de 10BASE-T, debido al aumento de velocidad, se debe tener mayor cuidado porque los bits enviados se acortan en duración y se producen con mayor frecuencia, estas señales de frecuencia más alta son más susceptibles al ruido, para tratar estos problemas, Ethernet de 100-Mbps utiliza dos pasos de codificación, la primera parte de la codificación utiliza una técnica denominada 4B/5B, la segunda parte es la codificación real de la línea específica para el cobre o la fibra.

Revisemos los parámetros de operación de las Ethernet 100Mbps

Parámetro	Valor
Periodo de bit	10ns
Ranura temporal	512tiempos de bit (64 octetos)
Espacio entre tramas	96 bits
Limite de intentos de colisión	16
Limite de postergación	10
Tamaño de congestión	32 bits
Tamaño de trama máximo	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Codificación	4B/5B y ML3 (TX) transmisión multinivel NRZI (FX) sin retorno a cero invertido

<sup>16</sup> Tabla 3.10 Ethernet 100

---

<sup>16</sup> Tabla de definición de los parámetros de la tecnología Ethernet 100Mbps

### 3.13.3 ETHERNET 1000Mbps (1Gbps)

Los estándares para Ethernet de 1000-Mbps o Gigabit Ethernet representan la transmisión a través de medios ópticos y de cobre, para 1000BASE-FX, IEEE 802.3z, especifica una conexión full duplex de 1 Gbps en fibra óptica, para 1000BASE-TX, IEEE 802.3ab, especifica el uso de cable de cobre balanceado de Categoría 5, 5e, 6, o mejor.

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización, un tiempo de bit de 1 nanosegundo (0,000000001 segundos) o 1 mil millonésima parte de un segundo, la trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Según su implementación, Gigabit Ethernet puede hacer uso de distintos procesos para convertir las tramas a bits en el cable. Las diferencias entre Ethernet estándar, Fast Ethernet y Gigabit Ethernet se encuentran en la capa física, como los bits ingresan al medio por menor tiempo y con mayor frecuencia, es fundamental la temporización, esta transmisión de alta velocidad requiere de frecuencias cercanas a las limitaciones de ancho de banda para los medios de cobre, esto hace que los bits sean más susceptibles al ruido en los medios de cobre, estos problemas requieren que Gigabit Ethernet utilice dos distintos pasos de codificación, la transmisión de datos se realiza de manera más eficiente utilizando códigos para representar el flujo de bits, los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores características de la Relación entre Señal y Ruido. En la capa física, los patrones de bits a partir de la capa MAC se convierten en símbolos, estos también pueden ser información de control tal como trama de inicio, trama de fin, condiciones de inactividad del medio, la trama se codifica en símbolos de control y símbolos de datos para aumentar la tasa de transferencia de la red.

Gigabit Ethernet (1000BASE-X) con base de fibra utiliza una codificación 8B/10B que es similar a la 4B/5B. Entonces le sigue la simple codificación de línea Sin Retorno a Cero (NRZ) de la luz en la fibra óptica. Este proceso de codificación más sencillo es posible debido a que el medio de la fibra puede transportar señales de mayor ancho de banda.

Revisemos los parámetros de operación de las Ethernet 1Gbps

Parámetro	Valor
Periodo de bit	1ns
Ranura temporal	4096tiempos de bit
Espacio entre tramas	96 bits
Límite de intentos de colisión	16
Límite de postergación	10
Tamaño de congestión	32 bits
Tamaño de trama máximo	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Límite de ráfaga	65536bits
Codificación	8B/10B y NRZ (FX) sin retorno a cero

<sup>17</sup> Tabla 3.11 Ethernet 1G

### 3.13.4 ETHERNET 10 Gbps

El IEEE 802.3ae se adaptó para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica, las características de 802.3ae y 802.3 son similares, pero Ethernet de 10-Gigabit (10GbE) evoluciona no sólo para las LAN sino también para las MAN y las WAN. Con un formato de trama y otras especificaciones de Capa 2 de Ethernet compatibles con estándares anteriores, 10GbE puede proporcionar mayores necesidades de ancho de banda que son interoperables con la infraestructura de redes ya existentes.

---

<sup>17</sup> Tabla de definición de parámetros de la tecnología Ethernet 1Gbps

Por tradición, se considera que Ethernet es una tecnología de LAN, pero los estándares de la capa física de 10GbE permiten tanto una extensión de las distancias de hasta 40 km a través de una fibra monomodo como una compatibilidad con la red óptica síncrona (SONET) y con redes síncronas de jerarquía digital (SDH), la operación a una distancia de 40 km hace de 10GbE una tecnología MAN viable y la compatibilidad con las redes SONET/SDH que operan a velocidades de hasta OC-192 (9.584640 Gbps) hace de 10GbE una tecnología WAN viable, incluso es posible que 10GbE compita con la ATM en ciertas aplicaciones.

10-Gbps Ethernet (IEEE 802.3ae) se estandarizó en junio de 2002, es un protocolo full-duplex que utiliza sólo fibra óptica como medio de transmisión. Las distancias máximas de transmisión dependen del tipo de fibra que se utiliza, cuando se utiliza fibra monomodo como medio de transmisión, la distancia máxima de transmisión es de 40 kilómetros (25 millas) y en el futuro se ve la posibilidad de estándares para una Ethernet de 40, 80 e inclusive 100 Gbps, y como es típico para las nuevas tecnologías, se están considerando varias implementaciones, que incluye:

- **10GBASE-SR:** Para cubrir distancias cortas en fibra multimodo ya instalada, admite un rango de 26 m a 82 m.
- **10GBASE-LX4:** Utiliza la multiplexión por división de longitud de onda (WDM), admite a un rango de 240 m a 300 m en fibra multimodo ya instalada y de 10 km en fibra monomodo.
- **10GBASE-LR y 10GBASE-ER:** Admite entre 10 km y 40 km en fibra monomodo.
- **10GBASE-SW, 10GBASE-LW y 10GBASE-EW:** Conocidas colectivamente como 10GBASE-W, su objetivo es trabajar con equipos WAN SONET/SDH para módulos de transporte síncrono (STM) OC-192.



Revisemos los parámetros de operación de las Ethernet 10Gbps

Parámetro	Valor
Periodo de bit	0.1ns
Ranura temporal	No permite
Espacio entre tramas	96 bits
Límite de intentos de colisión	No permite
Límite de postergación	No permite
Tamaño de congestión	No permite
Tamaño de trama máximo	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Límite de ráfaga	No aplica
Ampliación de espacio entre tramas	104 bits
Codificación	Amplia Multiplexión por División de Longitud de Onda (WDM)

<sup>18</sup> Tabla 3.12 Ethernet 10G

---

<sup>18</sup> Tabla de definición de los parámetros de la tecnología Ethernet 10Gbps

## CAPITULO IV

---

# *CONFIGURACIONES*

# *ETHERNET*

## **4.1 Direccionamiento de Ethernet**

### **4.1.1 Manejo de direcciones MAC con Puentes y Switches**

Todas las tecnologías Ethernet trabajan en un medio compartido, es decir, que sólo un nodo de la red puede transmitir datos a la vez, al agregar nodos, se aumenta la demanda de uso sobre el ancho de banda y se crea una carga adicional sobre los medios de transmisión, cuando se aumenta el número de nodos en un segmento, aumenta la probabilidad de que haya colisiones, y esto causa más retransmisiones, una solución al problema es dividir un segmento grande en partes más pequeñas y separarlo en dominios de colisión. Para lograr esto, un puente o Bridge guarda una tabla de direcciones MAC y sus puertos asociados, luego envía o elimina tramas basándose en las entradas de su tabla.

Con cada transmisión que se realiza y que llega a un Puente, la tabla de direcciones MAC se actualiza, para saber por cuál puerto transmitir la información que llegue, al proceso de entrada de información a un puerto x , y salida por un puerto y, se llama conmutación. Se utilizan direcciones MAC debido a que todo el proceso se realiza a nivel de capa 2 del modelo OSI.

Por lo general un puente sólo tiene dos puertos y divide un dominio de colisión en dos partes, todas las decisiones que hace el puente se basan en direcciones MAC o de Capa 2 y no afectan el direccionamiento lógico (direccionamiento IP) o de Capa 3, es decir un puente divide el dominio de colisión pero no afecta el dominio lógico o de Broadcast., no importa cuántos puentes haya en la red, a menos que haya un dispositivo de capa 3 como un router, toda la red compartirá el mismo espacio de dirección lógica de Broadcast, el Puente creará más dominios de colisión pero no creará dominios de Broadcast

Si en lugar de un puente normal se utiliza un Switch que es un puente multipuerto, que puede tener varios puertos, en lugar de crear dos dominios de colisión, cada puerto creará su propio dominio de colisión, en una red de veinte nodos, existen veinte dominios de colisión si cada uno está conectado a su propio puerto del Switch, si el Switch incluye un puerto Uplink, se crean veintiún dominios de colisión de un solo nodo. Un switch crea y mantiene de forma dinámica una tabla de memoria de contenido direccionable (Content Addressable Memory, CAM), que contiene toda la información MAC necesaria para cada puerto.

Cuando se conecta sólo un nodo a un puerto del Switch el dominio de colisión en el medio compartido contiene sólo dos nodos, el puerto del Switch y el host conectado, a estos segmentos físicos pequeños se les llama microsegmentos, y al proceso como tal que realiza el Switch se le llama por lo tanto Microsegmentación. Otra ventaja del Switch aparece cuando sólo dos nodos se conectan, si la red utiliza cableado de par trenzado, un par se usa para llevar la señal transmitida de un nodo al otro, el otro par se usa para la señal recibida y es posible que las señales pasen a través de ambos pares de forma simultánea, esta capacidad de comunicación en ambas direcciones al mismo tiempo se conoce como full duplex. La mayoría de los Switches son capaces de admitir full duplex, igual que las tarjetas de interfaz de red (Network Interface Card, NIC), en el modo full duplex, no existe restricción de acceso a los medios, así se elimina un dominio de colisión, en teoría el ancho de banda se duplica cuando se usa full duplex, y con el uso de la memoria CAM el Switch encuentra directamente el puerto que está asociado con la dirección MAC sin usar un algoritmo de búsqueda, con un circuito integrado de aplicación específica (Application Specific Integrated Circuit, ASIC) que es un dispositivo

formado de compuertas lógicas no dedicadas que pueden programarse para realizar funciones a velocidades lógicas, las operaciones que antes realizaba el software ahora pueden hacerse en hardware usando el ASIC, el uso de estas tecnologías reduce los retardos causados por el procesamiento del software y permite que un Switch pueda mantenerse al ritmo de la demanda de los datos de muchos microsegmentos y velocidades de bits altas.

#### **4.1.2 Tiempos de Latencia y conmutación**

La latencia es el retardo que existe entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino, es decir desde que sale la trama por la NIC y accesa al medio hasta que llega al nodo destino, existen varias condiciones que pueden causar retardos mientras la trama viaja desde su origen a su destino:

- ✘ Retardos de los medios causados por la velocidad limitada a la que las señales pueden viajar por los medios físicos.
- ✘ Retardos de circuito causados por los sistemas electrónicos que procesan la señal a lo largo de la ruta.
- ✘ Retardos de software causados por las decisiones que el software debe tomar para implementar la conmutación y los protocolos.
- ✘ Retardos causados por el contenido de la trama y en qué parte de la trama se pueden tomar las decisiones de conmutación. Por ejemplo, un dispositivo no puede enrutar una trama a su destino hasta que la dirección MAC destino haya sido leída

## **4.2 Métodos de transmisión y modos de conmutación**

### **4.2.1 Método de Corte y Método de Almacenamiento y Envío**

Un Switch puede comenzar a enviar la trama tan pronto como recibe la dirección MAC destino, la conmutación en este punto se llama conmutación por el método de corte y da como resultado una latencia más baja en el Switch, sin embargo, no se puede verificar la existencia de errores, al usar conmutación por método de corte, tanto el puerto origen como el destino deben operar a la misma velocidad de bit para mantener intacta la trama, a esto se le denomina conmutación Síncrona.

Cuando el Switch puede recibir toda la trama antes de enviarla al puerto destino, esto le da al OS del switch la posibilidad de controlar la secuencia de verificación de trama (Frame Check Sequence, FCS) para asegurarse que la trama se haya recibido de modo correcto antes de enviarla al destino, si se descubre que la trama es inválida, se descarta en este Switch en lugar de hacerlo en el destino final, ya que toda la trama se almacena antes de ser enviada, y a este método se le llama de almacenamiento y envío. En el método de almacenamiento y envío se debe usar la conmutación asimétrica, esto es si las velocidades de bit no son iguales, la trama debe almacenarse a una velocidad de bit determinada antes de ser enviada a otra velocidad de bit. Esto se conoce como conmutación asíncrona. Una conmutación asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda, tal como una combinación de puertos de 1000 Mbps y de 100 Mbps. La conmutación asimétrica ha sido optimizada para el flujo de tráfico cliente/servidor en el que muchos clientes se comunican con el servidor de forma simultánea, lo cual requiere mayor ancho de banda dedicado al puerto del servidor para evitar un cuello de botella en ese puerto.

#### **4.2.2 Método Libre de Fragmentos**

Existe un punto medio entre los métodos de corte y de almacenamiento y envío, el Método Libre de Fragmentos, el método libre de fragmentos lee los primeros 64 bytes que incluye el encabezado de la trama, y la conmutación comienza antes de que se lea todo el campo de datos y la Checksum, este método verifica la confiabilidad de direccionamiento y la información del protocolo de control de enlace lógico (Logical Link Control, LLC) para asegurar que el destino y manejo de los datos sean correctos.

#### **4.2.3 El Protocolo Spanning Tree, o Protocolo de Árbol de Extensión**

Cuando varios Switches están ubicados en un árbol jerárquico sencillo, es poco probable que ocurran bucles de conmutación, sin embargo es común que las redes conmutadas se diseñen con rutas redundantes para ofrecer más confiabilidad y tolerancia a fallas, si es cierto que se recomienda el uso de rutas redundantes, estas pueden tener efectos colaterales no deseables, los bucles de conmutación son uno de estos efectos, pueden ocurrir ya sea por diseño o por accidente, y pueden llevar tormentas de Broadcast que rápidamente saturan la red, el STP es un protocolo basado en estándares que se usa para evitar bucles de Switchero o conmutación, cada Switch en una LAN que usa STP envía un mensaje especial llamado unidades de datos del protocolo puente (Bridge Protocol Data Unit, BPDU) desde todos sus puertos para que los otros Switches sepan de su existencia y elijan un puente raíz para la red, los Switches entonces usan un algoritmo Spanning-Tree (Spanning Tree Algorithm, STA) para resolver y desconectar las rutas redundantes.

Cada puerto del Switch que usa protocolo de spanning- tree se encuentra en uno de los cinco estados siguientes:

- ✘ Bloquear (Blocking)
- ✘ Escuchar (Listening)
- ✘ Aprender (Learning)
- ✘ Enviar (Forwarding)
- ✘ Desactivar (Disabled)

El puerto pasa por estos cinco estados de la forma siguiente:

- ✘ De la inicialización al bloqueo
- ✘ De bloqueo a escucha o desactivado
- ✘ De escucha a aprendizaje o desactivado
- ✘ De aprendizaje a envío o desactivado
- ✘ De envío a desactivado

El resultado de la resolución y eliminación de bucles usando STP es la creación de un árbol jerárquico lógico sin bucles, sin embargo, si se llegaran a necesitar las rutas alternativas estarían disponibles.



#### 4.2.4 Dominios de colisión y dominios de broadcast

Para comprender los dominios de colisión se necesita comprender lo que son las colisiones y cómo se originan.

La mayoría de las redes se conectan directamente y todos los Hosts comparten el medio o la Capa 1, por ejemplo, algunas formas en que están conectadas son:

- ⌘ **Entorno de medios compartidos:** Ocurre cuando varios Hosts tienen acceso al mismo medio, por ejemplo, si varios nodos se encuentran conectados al mismo cable físico, a la misma fibra óptica entonces se dice que comparten el mismo entorno de medios.
- ⌘ **Entorno extendido de medios compartidos:** Es un tipo especial de entorno de medios compartidos en el que los dispositivos de red pueden ampliar el entorno de modo que pueda incluir accesos múltiples o distancias mayores de cableado.
- ⌘ **Entorno de red punto a punto:** Se usa mucho en las conexiones de red de servicio de acceso telefónico y es la más común para el usuario de casa, se trata de un entorno de red compartido en el que un dispositivo se conecta a un dispositivo solamente, como por ejemplo una computadora al proveedor de servicios de Internet por cable módem y línea telefónica (DSL).

Es importante saber identificar un entorno de medios compartidos, debido a que las colisiones sólo ocurren en un entorno así. Un sistema de autopistas es un ejemplo de entorno compartido en el que las colisiones pueden ocurrir porque varios vehículos están utilizando las mismas rutas, a medida que más vehículos entran a las rutas, es probable que haya más colisiones. Una red de datos compartida se parece mucho a una autopista, existen reglas para determinar quién tiene acceso a los medios de red, pero a veces las reglas

simplemente no pueden manejar el volumen de tráfico, entonces se producen colisiones, esto frecuentemente ocurre por factores externos al diseño de las redes como la latencia y los retardos.

Entonces los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones, las colisiones causan que la red sea ineficiente, cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período de tiempo y la duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo en la red.

Los tipos de dispositivos que interconectan los segmentos de medios definen los dominios de colisión, estos dispositivos se clasifican en dispositivos OSI de Capa 1, 2 ó 3, los dispositivos de Capa 1 no dividen los dominios de colisión, los dispositivos de Capa 2 y 3 sí lo hacen, la división o aumento del número de dominios de colisión con los dispositivos de Capa 2 y 3 se conoce también como segmentación. Los dispositivos de Capa 1, como los repetidores y hubs, tienen la función principal de extender los segmentos de cable de Ethernet, al extender la red se pueden agregar más hosts o nodos, sin embargo, cada host que se agrega aumenta la cantidad de tráfico potencial en la red, como los dispositivos de Capa 1 transmiten todo lo que se envía en los medios, cuanto mayor sea el tráfico transmitido en un dominio de colisión, mayor serán las posibilidades de colisión, esto causa al final bajo rendimiento de la red, que será mayor si todas las computadoras en esa red exigen anchos de banda elevados. Entonces, al colocar dispositivos de Capa 1 se extienden los dominios de colisión, pero la longitud de una LAN puede verse sobrepasada y causar otros problemas de colisión. Con los dispositivos de capa2, ya se había señalado que dividen los dominios de colisión pero no los de Broadcast, y depende del uso de un puente o varios puentes, o en su lugar Switches, y los dispositivos de capa 3, dividen los dominios de Colisión y los de Broadcast.

Para evitar que los dominios de Colisión lleguen a ser un problema grave se utiliza la regla de los cuatro repetidores en Ethernet, ésta establece que no puede haber más de cuatro repetidores o hubs entre dos computadoras en la red, para asegurar que una red 10BASE-T con repetidores funcionará de forma adecuada, el cálculo del retardo del recorrido de ida y vuelta debe estar dentro de ciertos límites( retardo de repetidor + retardo de cable + retardo de la NIC, todo multiplicado por 2), de otro modo todas las estaciones de trabajo no podrán escuchar todas las colisiones en la red. La latencia del repetidor, el retardo de propagación y la latencia de la NIC contribuyen a la regla de 4 repetidores, si se excede la regla de los cuatro repetidores, esto puede llevar a la violación del límite de retardo máximo, cuando se supera este límite de retardo, la cantidad de colisiones tardías aumenta, una colisión tardía es una colisión que se produce después de la transmisión de los primeros 64 bytes de la trama, y cuando se produce una colisión tardía, no se requiere que los conjuntos de chips en las NIC retransmitan de forma automática, estas tramas de colisión tardía agregan un retardo denominado “retardo de consumo”, con el aumento del retardo de consumo y la latencia, se afecta más el rendimiento de la red.

La regla 5-4-3-2-1 requiere que se cumpla con las siguientes condiciones:

- ✘ Cinco segmentos de medios de red.
- ✘ Cuatro repetidores o hubs
- ✘ Tres segmentos de host de red
- ✘ Dos secciones de enlace (sin hosts)
- ✘ Un dominio de colisión grande

La regla 5-4-3-2-1 también explica cómo mantener el tiempo de retardo del recorrido de ida y vuelta en una red compartida dentro de los límites aceptables.

## **4.3 Señales y transmisión**

### **4.3.1 Segmentación**

La historia de cómo Ethernet maneja las colisiones y los dominios de colisión se remonta a la investigación realizada en la Universidad de Hawai en 1970 en su intento por desarrollar un sistema de comunicaciones inalámbrico entre las islas de Hawai, los investigadores de la Universidad desarrollaron un protocolo llamado Aloha, en realidad, el protocolo de Ethernet se basa en el protocolo Aloha.

Conectar varias computadoras a un solo medio de acceso compartido que no tiene ningún otro dispositivo de red conectado, crea un dominio de colisión, esta situación limita el número de Hosts que pueden utilizar el medio, también llamado “Segmento”, los dispositivos de Capa 1 amplían pero no controlan los dominios de colisión.

Como se mencionó anteriormente los dispositivos de Capa 2 dividen o segmentan los dominios de colisión, el control de propagación de trama con la dirección MAC asignada a todos los dispositivos de Ethernet ejecuta esta función, los dispositivos de Capa 2, los Puentes o Bridges y Switches, hacen un seguimiento de las direcciones MAC y el segmento en el que se encuentran, al hacer esto, estos dispositivos pueden controlar el flujo de tráfico en el nivel de Capa 2, esta función hace que las redes sean más eficientes, al permitir que los datos se transmitan por diferentes segmentos de la LAN al mismo tiempo sin que las tramas colisionen, al usar Puentes y Switches, el dominio de colisión se divide efectivamente en partes más pequeñas, que se transforman cada una a su vez en un dominio de colisión, estos dominios de colisión más pequeños tendrán menos hosts y menos tráfico que el dominio original, y en tanto menor sea la cantidad de hosts en un dominio de colisión, mayores son las probabilidades de que el medio se encuentre disponible, siempre y cuando el

tráfico entre los segmentos puenteados no sea demasiado pesado, una red puenteada funciona bien, de lo contrario, el dispositivo de Capa 2 puede retrasar las comunicaciones y convertirse en un cuello de botella en sí mismo.

Los dispositivos de Capa 3, al igual que los de Capa 2, no envían las colisiones, es por eso que usar dispositivos de Capa 3, como routers, en una red produce el efecto de dividir los dominios de colisión en dominios menores.

#### **4.3.2 La señal Broadcast**

Para comunicarse con todos los dominios de colisión, los protocolos utilizan tramas de broadcast y multicast a nivel de Capa 2 en el modelo OSI, cuando un nodo necesita comunicarse con todos los hosts de la red, envía una trama de broadcast con una dirección MAC destino 0xFFFFFFFFFFFF, esta es una dirección a la cual debe responder la tarjeta de interfaz de la red (Network Interface Card, NIC) de cada host, los dispositivos de Capa 2 deben inundar todo el tráfico de broadcast y multicast, esta acumulación de tráfico de broadcast y multicast de cada dispositivo de la red se denomina radiación de broadcast, en algunos casos, la circulación de radiación de broadcast puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones, en este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de broadcast, la probabilidad de las tormentas de broadcast aumenta a medida que crece la red conmutada.

Como la NIC tiene que interrumpir a la CPU para procesar cada grupo de broadcast o multicast al que pertenece, el efecto de radiación de broadcast afecta el rendimiento de los hosts de la red, incluso puede tener como consecuencia que los broadcasts que inundan la red efectivamente pueden desconectar una estación de trabajo IP.

La mayoría de las veces, el host no se beneficia al procesar la señal de broadcast, ya que no es el destino buscado, al host no le interesa el servicio que se publicita, o ya lo conoce, los niveles elevados de radiación de broadcast pueden disminuir el rendimiento del host de manera considerable. Las tres fuentes de broadcasts y multicasts en las redes IP son las estaciones de trabajo, los routers y las aplicaciones multicast.

Las estaciones de trabajo envían en broadcast una petición de protocolo de resolución de direcciones (Address Resolution Protocol, ARP) cada vez que necesitan ubicar una dirección MAC que no se encuentra en la tabla ARP. Cuando el tráfico de broadcast y multicast hace un pico debido a una tormenta, la pérdida pico de la CPU puede tener una magnitud mayor al promedio, las tormentas de broadcast pueden originarse en un dispositivo que requiere información de una red que ha crecido demasiado, la petición original recibe tantas respuestas que el dispositivo no las puede procesar, o la primera petición desencadena peticiones similares de otros dispositivos que efectivamente bloquean el flujo de tráfico en la red.

Como ejemplo, el comando **telnet yahoo.com** se traduce a una dirección IP a través de una búsqueda en el sistema de denominación de dominios (Domain Naming System, DNS), para ubicar la dirección MAC correspondiente, se envía una petición ARP, por lo general, las estaciones de trabajo IP guardan entre 10 y 100 direcciones en sus tablas ARP durante dos horas aproximadamente, la velocidad de un ARP en una estación de trabajo típica puede ser cercana a 50 direcciones cada dos horas o 0,007 ARP por segundo, esto significa que 2000 hosts IP producen casi de 14 ARP por segundo.

Los protocolos de enrutamiento que están configurados en la red pueden aumentar el tráfico de broadcast de modo significativo, algunos administradores configuran todas las estaciones de trabajo para que ejecuten el protocolo de información de enrutamiento (Routing Information Protocol, RIP) como una

política de redundancia y alcance, cada 30 segundos, el RIPv1 utiliza broadcasts para retransmitir toda la tabla de enrutamiento a otros routers RIP, si 2000 estaciones de trabajo se configuraran para ejecutar RIP y, en promedio, se requieren 50 paquetes para transmitir la tabla de enrutamiento, las estaciones de trabajo generarían 3333 broadcasts por segundo, la mayoría de los administradores de red sólo configuran un número pequeño de routers, por lo general de cinco a diez, para ejecutar un RIP, en el caso de una tabla de enrutamiento que tiene un tamaño de 50 paquetes, 10 routers RIP generarán cerca de 16 broadcasts por segundo.

Las aplicaciones multicast en IP pueden afectar negativamente el rendimiento de redes conmutadas de gran escala, aunque el multicast es una forma eficiente de enviar un flujo de datos de multimedia a muchos usuarios en un hub de medios compartidos, afecta a cada usuario de una red plana conmutada. Una aplicación de paquete de video determinada, puede generar un flujo de siete megabytes de datos multicast que en una red conmutada se enviarían a cada segmento causando una gran congestión.

#### **4.3.3 Dominio de Broadcast**

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2, dividir una LAN en varios dominios de colisión aumenta la probabilidad de que cada host de la red tenga acceso completo a los medios, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host, pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos pueden reducir la eficiencia de toda la LAN, los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo, el tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast, es decir, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3.

Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts, los routers en realidad, funcionan en las Capas 1, 2 y 3. y al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios, tienen un encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2, es la Capa 3 la que permite que el router segmente dominios de broadcast. Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe haberlo procesado y la información de la trama debe haber sido eliminada, el envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC, para que un paquete pueda enviarse, debe contener una dirección IP que esté por fuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

#### **4.3.4 Transmisión de datos**

La transmisión de datos en un contexto de dominios de colisión y de broadcast se centra en la forma en que las tramas se propagan a través de la red y se refiere al movimiento de datos a través de los dispositivos de capa 1, 2 y 3 y a la manera en que los datos deben encapsularse para poder realizar esa travesía en forma correcta, los datos se deben encapsular en la capa de la red con una dirección de origen y destino IP, y en la capa de enlace de datos con una dirección MAC origen y destino. Una buena regla a seguir es que un dispositivo de Capa 1 siempre envíe la trama, mientras que un dispositivo de Capa 2 desee enviar la trama, es decir, un dispositivo de Capa 2 siempre tratará de enviar la trama a menos que algo se lo impida y un dispositivo de Capa 3 no enviará la trama a menos que se vea obligado a hacerlo. Usar esta regla ayudará a identificar la forma en que los datos se transmiten en la red.



Los dispositivos de Capa 1 no funcionan como filtros, entonces todo lo que reciben se transmite al segmento siguiente, la trama simplemente se regenera y retemporiza y así vuelve a su calidad de transmisión original, cualquier segmento conectado por dispositivos de Capa 1 forma parte del mismo dominio, tanto de colisión como de broadcast.

Los dispositivos de Capa 2 filtran tramas de datos basados en la dirección MAC destino, la trama se envía si se dirige a un destino desconocido fuera del dominio de colisión, la trama también será enviada si se trata de un broadcast, multicast o unicast que se dirige fuera del dominio local de colisión. La única vez en que la trama no se envía es cuando el dispositivo de Capa 2 encuentra que el host emisor y el receptor se encuentran en el mismo dominio de colisión.

Los dispositivos de Capa 3 filtran paquetes basados en la dirección IP destino la única forma en que un paquete se enviará es si su dirección IP destino se encuentra fuera del dominio broadcast y si el router tiene una ubicación identificada para enviar el paquete. Un dispositivo de Capa 3 crea varios dominios de colisión y broadcast.

Resumiendo, la transmisión de datos en una red enrutada basada en IP, requiere el paso de datos a través de dispositivos de administración de tráfico en las Capas 1, 2 y 3 del modelo OSI, la Capa 1 se utiliza en la transmisión por medios físicos, la Capa 2 para la administración de dominios de colisión, y la Capa 3 para la administración de dominios de broadcast.

## CAPITULO V

---

# *TECNOLOGÍAS WAN*

## **5 TECNOLOGÍAS WAN**

### **5.1 INTRODUCCIÓN**

Una WAN es una red de comunicación de datos que opera más allá del alcance geográfico de una LAN, una de las principales diferencias entre una WAN y una LAN es que una empresa u organización debe suscribirse a un proveedor de servicio WAN para utilizar los servicios de red y utiliza enlaces de datos suministrados por los servicios de una operadora para acceder a Internet y conectar los sitios de la organización entre sí, con sitios de otras organizaciones, con servicios externos y con usuarios remotos. Las WAN generalmente transportan varios tipos de tráfico, como voz, datos y vídeo, aunque los servicios telefónicos y de datos son los servicios WAN de uso más común.

Los dispositivos de las instalaciones del suscriptor se conocen como equipo terminal del abonado (CPE), el suscriptor es dueño de un CPE o alquila un CPE del proveedor de servicios, un cable de cobre o fibra conecta el CPE a la central telefónica del proveedor de servicio más cercano, este cableado se llama bucle local, o última milla, con una llamada se conecta de forma local a otros bucles locales o de forma no local a través de un enlace troncal a un centro primario, luego se dirige a un centro de sección y luego a un centro de operación internacional o regional a medida que la llamada viaja a su destino.

Para que el bucle local transporte datos, se necesita un dispositivo como un módem que prepare los datos para su transmisión, estos dispositivos que colocan los datos en el bucle local se llaman equipos de terminación de circuito de datos, o equipos de comunicación de datos (DCE), los dispositivos del cliente que transmiten datos al DCE se llaman equipo terminal de datos (DTE), el propósito principal del DCE es suministrar una interfaz para el DTE al enlace de comunicación en la nube WAN. La interfaz DTE/DCE utiliza

varios protocolos de capa física, tales como la Interfaz serial de alta velocidad (HSSI) y V.35, los enlaces WAN vienen en varias velocidades medidos en bits por segundo (bps), kilobits por segundo (kbps o 1000 bps), megabits por segundo (Mbps o 1000 kbps) o gigabits por segundo (Gbps o 1000 Mbps)

Como las redes WAN son grupos de redes LAN conectadas con enlaces de comunicaciones desde un proveedor de servicios, como los enlaces de comunicaciones no pueden conectarse directamente a la LAN es necesario identificar las distintas piezas del equipo que realiza la conexión, las computadoras basadas en redes LAN con datos a transmitir, envían datos a un “router” que contiene tanto interfaces LAN como WAN este utiliza información de dirección de Capa 3 del modelo OSI para enviar los datos en la interfaz WAN apropiada, los routers son dispositivos de red activos e inteligentes y por lo tanto pueden participar en la administración de una red como conectividad, desempeño confiable, control de administración y flexibilidad.

El enlace de comunicaciones necesita señales en un formato correcto, para las líneas digitales, se requiere una unidad de servicio de canal (CSU) y una unidad de servicio de datos (DSU), frecuentemente las dos se encuentran combinadas en una sola pieza llamada CSU/DSU.

Si el bucle local es analógico y no digital, requiere de un módem, estos transmiten datos a través de las líneas telefónicas de grado de voz, modulando y demodulando la señal, las señales digitales se superponen en la señal analógica de la voz que se modula para su transmisión.

Cuando se utiliza ISDN (RDSI) como el enlace de comunicaciones, todos los equipos conectados al bus ISDN tienen que ser compatibles con ISDN, la compatibilidad, en general, se integra a la interfaz de la computadora para conexiones de acceso telefónico directas o a la interfaz del router para conexiones LAN o WAN, los equipos más antiguos sin interfaz ISDN requieren

un adaptador de terminal ISDN (TA) para la compatibilidad con ISDN, los servidores de comunicaciones atienden la comunicación de usuarios de acceso telefónico entrante y de acceso remoto a una LAN y pueden tener una mezcla de interfaces analógicas y digitales (ISDN) y admitir a cientos de usuarios al mismo tiempo.

Algunos estándares utilizados en redes WAN para la capa 1 del modelo OSI son los siguientes mostrados en la tabla 5.1

ESTÁNDAR	DESCRIPCIÓN
EIA/TIA 232	Velocidad hasta 115200bps
EIA/TIA 449/530	Velocidad hasta 2Mbps
EIA/TIA 612/613	Interfaz serial de alta velocidad HSSI hasta 52 Mbps
V.35	Velocidades hasta 2,048Mbps
X.21	Para comunicaciones digitales síncronas

<sup>19</sup> Tabla 5.1 Estándares

Los protocolos de la capa 2 del modelo OSI definen cómo se encapsulan los datos para su transmisión, y los mecanismos de transferencia de las tramas, y se utilizan tecnologías como ISDN, Frame Relay o el Modo de Transferencia Asíncrona (ATM). Estos protocolos utilizan los mismos mecanismos de entramado, control de enlace de datos de alto nivel (HDLC), un estándar ISO o uno de sus subgrupos o variantes.

Los enlaces WAN se pueden clasificar en dos partes, los enlaces dedicados y los enlaces conmutados, los enlaces dedicados incluyen tecnologías de líneas arrendadas o alquiladas, como T1 y E1, T3/E3 o DLS; los enlaces conmutados también se dividen en 3 categorías, conmutados por circuitos, por paquetes y por celdas, dentro de la clasificación de conmutación por circuitos se encuentran los POTS o servicio telefónico analógico, como ISDN básico (BRI) y primario (PRI), conmutado de 56Kbps; dentro de los conmutados por

---

<sup>19</sup> Tabla de estándares WAN para transmisión de datos.

paquetes se encuentran las tecnologías X.25 y Frame Relay, y finalmente los conmutados por celdas, que incluyen ATM y SMDS.

## 5.2 CONEXIÓN ANALÓGICA

Cuando se necesitan transferencias de datos de bajo volumen y esporádicos, los módems y las líneas telefónicas analógicas ofrecen conexiones conmutadas dedicadas y de baja capacidad, la telefonía normal utiliza cables de cobre llamados bucle local, para conectar el equipo telefónico a las instalaciones del suscriptor a la red telefónica pública conmutada (PSTN), el bucle local no es adecuado para el transporte directo de datos, pero el módem puede enviar datos de computadora a través de la red telefónica de voz, el módem modula los datos binarios en una señal analógica en el origen y, en el destino, demodula la señal analógica a datos binarios, las características físicas del bucle local y su conexión a PSTN limitan la velocidad de la señal, el límite superior está cercano a 33kbps y es posible aumentar la velocidad a 56kbps si la señal viene directamente por una conexión digital.

Para las empresas pequeñas, esto puede resultar adecuado para el intercambio de cifras de ventas, precios, informes regulares y correo electrónico, al usar el sistema de conexión automático de noche o durante los fines de semana para realizar grandes transferencias de archivos y copias de respaldo de datos, la empresa puede aprovecharse de las tarifas más bajas de las horas no pico, las tarifas se calculan según la distancia entre los extremos, la hora del día y la duración de la llamada. Las ventajas del módem y las líneas analógicas son simplicidad, disponibilidad y bajo costo de implementación. Las desventajas son la baja velocidad en la transmisión de datos y el relativamente largo tiempo de conexión. Los circuitos dedicados que ofrece el sistema de conexión telefónica tendrán poco retardo y fluctuación de fase para el tráfico

punto a punto, pero el tráfico de voz o video no funcionará de forma adecuada a las velocidades de bits relativamente bajas.

### 5.3 ISDN

Las conexiones internas o troncales de PSTN evolucionaron y pasaron de llevar señales de multiplexión por división de frecuencia, a llevar señales digitales de multiplexión por división de tiempo (TDM) para permitir que el bucle local lleve las señales digitales que resultan en conexiones conmutadas de mayor capacidad. La red digital de servicios integrados (ISDN) convierte el bucle local en una conexión digital TDM, la conexión utiliza canales portadores de 64 kbps (B) para transportar voz y datos, y una señal, canal delta (D), para la configuración de llamadas y otros propósitos.

La interfaz de acceso básico (BRI) ISDN está destinada al uso doméstico y a las pequeñas empresas y provee dos canales B de 64 kbps y un canal D de 16 kbps, para las instalaciones más grandes, está disponible la interfaz de acceso principal (PRI) ISDN, en América del Norte, PRI ofrece veintitrés canales B de 64 kbps y un canal D de 64 kbps, para un total de velocidad de transmisión de hasta 1,544 Mbps, esto incluye algo de carga adicional para la sincronización, en Europa, Australia, y otras partes del mundo, PRI ISDN ofrece treinta canales B y un canal D para un total de velocidad de transmisión de hasta 2,048 Mbps, incluyendo la carga de sincronización, PRI corresponde a una conexión T1.

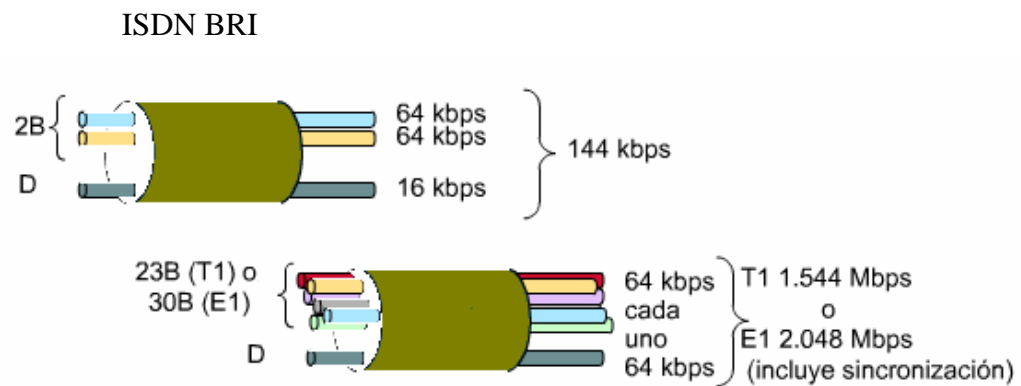
La velocidad de PRI internacional corresponde a una conexión E1. El canal D BRI no utiliza su potencial máximo, ya que tiene que controlar solamente dos canales B, algunos proveedores permiten que los canales D transmitan datos a una velocidad de transmisión baja como las conexiones X.25 a 9,6 kbps, para las WAN pequeñas, ISDN BRI puede ofrecer un mecanismo de conexión ideal. BRI posee un tiempo de establecimiento de llamada que es menor a un segundo y su canal B de 64 kbps ofrece mayor capacidad que un enlace de módem

analógico, si se requiere una mayor capacidad, se puede activar un segundo canal B para brindar un total de 128 kbps, aunque no es adecuado para el video, esto permitiría la transmisión de varias conversaciones de voz simultáneas además del tráfico de datos.

Otra aplicación común de ISDN es la de ofrecer capacidad adicional según la necesidad en una conexión de línea alquilada, la línea tiene el tamaño para transportar el tráfico usual mientras que ISDN se agrega durante los períodos de mayor demanda, ISDN también se utiliza como respaldo en caso de que falle la línea. Las tarifas de ISDN se calculan según cada canal B y son similares a las de las conexiones analógicas.

Con ISDN PRI, se pueden conectar varios canales B entre dos extremos, esto permite que se realicen conferencias de video y conexiones de datos de banda ancha sin latencia ni fluctuación de fase, aunque las conexiones múltiples pueden resultar muy caras para cubrir grandes distancias.

Visualmente podríamos identificar a ISDN de la siguiente manera:



<sup>20</sup>Fig. 5.1 Cables ISDN

<sup>20</sup> Dibujo de cables ISDN de interfaz BRI y PRI tomados desde [www.monografias.com](http://www.monografias.com)



## 5.4 LÍNEAS ARRENDADAS O ALQUILADAS

Cuando se requieren conexiones dedicadas permanentes se utilizan líneas arrendadas con capacidades de hasta 2.5 Gbps, Un enlace punto a punto ofrece rutas de comunicación WAN preestablecidas desde las instalaciones del cliente a través de la red hasta un destino remoto, las líneas punto a punto se alquilan por lo general a una operadora de servicios de telecomunicaciones y se denominan líneas arrendadas. Se pueden conseguir líneas arrendadas con distintas capacidades y se cotizan según el ancho de banda necesario y la distancia entre los dos puntos conectados. Los enlaces punto a punto por lo general son más caros que los servicios compartidos como Frame Relay, el costo de la línea dedicada puede elevarse cuando se utiliza para conectar varios sitios, sin embargo a veces los beneficios de una línea arrendada son mayores que los costos, la capacidad dedicada no presenta ni latencia ni fluctuaciones de fase entre extremos, y aspectos como la disponibilidad constante es esencial para algunas aplicaciones, como el comercio electrónico.

Cada conexión de línea arrendada requiere un puerto serial de router, también se necesita un CSU/DSU y el circuito físico del proveedor de servicios, las líneas arrendadas se utilizan con mucha frecuencia en la construcción de las WAN y ofrecen una capacidad dedicada permanente, ha sido la conexión tradicional de preferencia aunque presenta varias desventajas, el tráfico de WAN es a menudo variable y las líneas arrendadas tienen una capacidad fija, esto da por resultado que el ancho de banda de la línea rara vez sea el que se necesita, además cada punto necesitaría una interfaz en el router que aumentaría los costos de equipos.

Las líneas arrendadas ofrecen conexiones punto a punto entre las LAN y también se pueden multiplexar en las líneas arrendadas, dando por resultado enlaces más cortos y menos necesidad de interfaces.

Algunos tipos de líneas disponibles en el mercado son:

Tipo	Estándar	Velocidad
56	DS0	56Kbps
64	DS0	64Kbps
T1	DS1	1.544Mbps
E1	ZM	2.048Mbps
E3	M3	34.064Mbps
J1	Y1	2.048Mbps
T3	DS3	44.736Mbps
OC-1	SONET	51.84Mbps
OC-3	SONET	155.54Mbps
OC-9	SONET	466.56Mbps
OC-12	SONET	622.08Mbps
OC-18	SONET	933.12Mbps
OC-24	SONET	1244.16Mbps
OC-36	SONET	1866.24Mbps
OC-48	SONET	2488.32

<sup>21</sup>Tabla 5.1 Líneas arrendadas

## 5.5 X 25

Debido al costo de las líneas alquiladas los proveedores de telecomunicaciones introdujeron las redes conmutadas por paquetes utilizando líneas compartidas para reducir los costos, la primera de estas redes conmutadas por paquetes se estandarizó como el grupo de protocolos X.25, ofrece una capacidad variable y compartida de baja velocidad de transmisión que puede ser conmutada o permanente, es un protocolo de capa de red y los suscriptores disponen de una dirección en la red, los circuitos virtuales se establecen a través de la red con paquetes de petición de llamadas a la dirección destino, un número de canal identifica el SVC (circuito virtual conmutado) resultante, los

---

<sup>21</sup> Tabla de velocidades de transmisión de datos en líneas arrendadas tomada desde [www.cisco.com](http://www.cisco.com)

paquetes de datos rotulados con el número del canal se envían a la dirección correspondiente, varios canales pueden estar activos en una sola conexión.

Los suscriptores se conectan a la red X.25 con una línea alquilada o con una conexión de acceso telefónico. Además, las redes X.25 pueden tener canales preestablecidos entre los suscriptores que proveen un PVC (circuito virtual permanente).

X.25 puede resultar muy económica porque las tarifas se calculan con base en la cantidad de datos enviados y no el tiempo de conexión ni la distancia, los datos se pueden enviar a cualquier velocidad igual o menor a la capacidad de conexión, esto ofrece más flexibilidad, por lo general tienen poca capacidad con un máximo de 48 kbps, y los paquetes de datos están sujetos a los retrasos típicos de las redes compartidas.

Actualmente en los EEUU X.25 ya no está disponible como una tecnología WAN, Frame Relay la ha reemplazado, las aplicaciones típicas de X.25 son los lectores de tarjeta de punto de venta, estos lectores utilizan X.25 en el modo de conexión telefónica para validar las transacciones en una computadora central. Algunas empresas usan también las redes de valor agregado (VAN) basadas en X.25 para transmitir facturas, pólizas de embarque y otros documentos comerciales usando el Intercambio electrónico de datos (EDI) y para estas aplicaciones, el bajo ancho de banda y la alta latencia no constituyen un problema, porque el bajo costo de X.25 lo compensa.

## **5.6 FRAME RELAY**

Con la creciente demanda de mayor ancho de banda y menor latencia en la conmutación de paquetes, los proveedores de comunicaciones introdujeron el

Frame Relay, aunque la configuración de la red parece similar a la de X.25, la velocidad de transmisión de datos disponible es por lo general de hasta 4 Mbps y algunos proveedores ofrecen aún mayores velocidades, Frame Relay difiere de X.25 en muchos aspectos, el más importante es que es un protocolo mucho más sencillo que funciona a nivel de la capa de enlace de datos y no en la capa de red, además Frame Relay no realiza ningún control de errores o flujo, la simplificada administración de las tramas es una reducción en la latencia, y las medidas tomadas para evitar la acumulación de tramas en los switches intermedios ayudan a reducir las fluctuaciones de fase.

La mayoría de las conexiones de Frame Relay son PVC y no SVC, la conexión al extremo de la red con frecuencia es una línea alquilada, pero algunos proveedores ofrecen conexiones telefónicas utilizando líneas ISDN, el canal D ISDN se utiliza para configurar una SVC en uno o más canales B, las tarifas de Frame Relay se calculan con base en la capacidad del puerto de conexión al extremo de la red.

Frame Relay ofrece una conectividad permanente, compartida, de ancho de banda mediano, que envía tanto tráfico de voz como de datos, es ideal para conectar las LAN de una empresa, el router de la LAN necesita sólo una interfaz, aún cuando se estén usando varios VC, la línea alquilada corta que va al extremo de la red Frame Relay permite que las conexiones sean económicas entre LANs muy dispersas.

## **5.7 ATM**

Los proveedores de comunicaciones vieron la necesidad de una tecnología de red compartida permanente que ofreciera muy poca latencia y fluctuación a anchos de banda mucho más altos, su solución fue el Modo de Transferencia

Asíncrona (ATM) que tiene una velocidad de transmisión de datos superior a los 155 Mbps, es capaz de transferir voz, video y datos a través de redes privadas y públicas, tiene una arquitectura basada en celdas más que una basada en tramas, las celdas ATM tienen siempre una longitud fija de 53 bytes, contiene un encabezado ATM de 5 bytes seguido de 48 bytes de carga ATM. Las celdas pequeñas de longitud fija son adecuadas para la transmisión de tráfico de voz y video porque este tráfico no tolera demoras, el tráfico de video y voz no tiene que esperar que se transmita un paquete de datos más grande.

La celda ATM de 53 bytes es menos eficiente que las tramas y paquetes más grandes de Frame Relay y X.25, además, la celda ATM tiene un encabezado de por lo menos 5 bytes por cada 48-bytes de datos, cuando la celda está transportando paquetes de capa de red segmentados, la carga general será mayor porque el switch ATM tiene que poder reagrupar los paquetes en el destino. Una línea ATM típica necesita casi un 20% más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM ofrece tanto los PVC como los SVC, aunque los PVC son más comunes en las WAN y como las otras tecnologías compartidas, ATM permite varios circuitos virtuales en una sola conexión de línea alquilada al extremo de red.

## **5.8 DSL**

La tecnología de línea Digital del suscriptor (DSL) es una tecnología de banda ancha que utiliza líneas telefónicas de par trenzado para transportar datos de alto ancho de banda, se considera de banda ancha, en contraste con el servicio de banda base típico de las LAN, banda ancha se refiere a la técnica que utiliza varias frecuencias dentro del mismo medio físico para transmitir datos, el término xDSL se refiere a un número de formas similares, aunque en competencia, de tecnologías DSL:

- DSL Asimétrico (ADSL)
- DSL simétrico (SDSL)
- DSL de alta velocidad de bits (HDSL)
- ISDN (como) DSL (IDSL)
- DSL para consumidores (CDSL), también llamado DSL-lite o G.lite

La tecnología DSL permite que el proveedor de servicios ofrezca a los clientes servicios de red de alta velocidad, utilizando las líneas de cobre de bucle local instaladas, además permite que la línea de bucle local se utilice para realizar conexiones telefónicas de voz normales y conexiones permanentes para tener conectividad de red al instante. Las líneas del suscriptor DSL múltiples se pueden multiplexar a un enlace de alta capacidad al usar el Multiplexor de acceso DSL (DSLAM) en el sitio del proveedor, los DSLAM incorporan la tecnología TDM para juntar muchas líneas del suscriptor a un solo medio más pequeño, en general una conexión T3/DS3, las tecnologías DSL están utilizando técnicas de codificación y modulación complejas para lograr velocidades de transmisión de datos de hasta 8.192 Mbps.

El canal de voz de un teléfono estándar cubre un rango de frecuencia de 330 Hz a 3.3 KHz un rango de frecuencia de 4KHz se considera como requisito para cualquier transmisión de voz en un bucle local, las tecnologías DSL cargan (upstream: corriente arriba) y descargan (downstream: corriente abajo) datos a frecuencia superiores a este rango de 4KHz, esta técnica es lo que permite que la transmisión de voz y datos tenga lugar de modo simultáneo en un servicio DSL. Existen dos tipos básicos de tecnología DSL: la asimétrica (ADSL) y la simétrica (SDSL), todas las formas de servicio DSL se pueden clasificar como ADSL o SDSL y existen muchas variedades de cada tipo, el servicio asimétrico brinda mayor ancho de banda de descarga o downstream al usuario que el ancho de banda de carga.

El servicio simétrico brinda la misma capacidad en ambas direcciones. No todas las tecnologías DSL permiten el uso de un teléfono, por ejemplo SDSL se conoce como “cobre seco” porque no tiene un tono de llamada y no ofrece servicio telefónico en la misma línea, por eso se necesita una línea separada para el servicio SDSL.

Los distintos tipos de DSL brindan diferentes anchos de banda, con capacidades que exceden aquellas de línea alquilada T1 o E1, la velocidad de transferencia depende de la longitud real del bucle local y del tipo y condición de su cableado. Para obtener un servicio satisfactorio, el bucle debe ser menor a 5,5 kilómetros (3,5 millas). La disponibilidad de DSL está lejos de ser universal, y hay una gran variedad de tipos y normas emergentes. No es una opción popular de las empresas para apoyar a las personas que trabajan en sus hogares, por lo general, el suscriptor no puede optar por conectarse a la red de la empresa directamente, sino que primero tiene que conectarse a un proveedor de servicios de Internet (ISP), desde ahí se realiza una conexión IP a través de Internet hasta la empresa, así se corren riesgos de seguridad. Para tratar las cuestiones de seguridad, los servicios DSL ofrecen funciones para utilizar conexiones la Red privada virtual (VPN) a un servidor VPN, que por lo general se encuentra ubicado en la empresa.

Los servicios más populares de DSL son:

DSL	Descarga	Carga
ADSL	64kbps a 8.192Mbps	16kbps a 640kbps
SDSL	1.544Mbps a 2.048Mbps	1.544Mbps a 2.048Mbps
HDSL	1.544Mbps a 2.048Mbps	1.544Mbps a 2.048Mbps
IDSL	144Kbps	144kbps
CDSL	1Mbps	16 a 160kbps

<sup>22</sup> Tabla 5.2 DSL

<sup>22</sup> Tabla de descripción de velocidades de dispositivos DSL tomada desde [www.cisco.com](http://www.cisco.com)

## 5.9 CABLE MODEM

El cable coaxial es muy usado en áreas urbanas para distribuir las señales de televisión por cable (CATV), y en algunos casos el acceso a la red está disponible desde estas redes de televisión por cable, esto permite que haya un mayor ancho de banda que con el bucle local de teléfono, el cable módem mejorado permite transmisiones de datos de alta velocidad de dos vías, usando las mismas líneas coaxiales que transmiten la señal de CATV, algunos proveedores de servicio de cable prometen velocidades de transmisión de datos de hasta 6,5 veces más altas que las líneas alquiladas T1, esta velocidad hace que el cable sea un medio atractivo para transferir grandes cantidades de información digital de manera rápida, incluyendo video clips, archivos de audio y grandes cantidades de datos, la información que tardaría dos minutos en descargar usando un BRI ISDN puede descargarse en dos segundos a través de una conexión de cable módem.

Los cable módem ofrecen una conexión permanente y una instalación simple, una conexión de cable permanente significa que las computadoras conectadas pueden estar sujetas a una violación en la seguridad en cualquier momento y necesitan estar adecuadamente aseguradas con “firewalls” o “corta fuegos”, para tratar las cuestiones de seguridad, los servicios cable módem ofrecen funciones para utilizar conexiones de Red privada virtual (VPN) a un servidor VPN, que por lo general se encuentra ubicado en la empresa que ofrece el servicio de CATV.

Un cable módem puede ofrecer de 30 a 40Mbps de datos en un canal de cable de 6MHz, casi 500 veces más rápido que un módem de 56Kbps. Con un cable módem, el suscriptor puede continuar recibiendo servicio de televisión por cable mientras recibe datos en su computador personal de forma simultánea. Esto se logra con la ayuda de un divisor de señal uno a dos.



Los suscriptores de cable módem deben utilizar el ISP asociado con el proveedor de servicio, todos los suscriptores locales comparten el mismo ancho de banda del cable, a medida que más usuarios contratan el servicio el ancho de banda disponible puede caer por debajo de la velocidad esperada.

## CONCLUSIONES

Para concluir, se puede decir que al analizar las características de las distintas tecnologías de red existentes en el mercado, Ethernet tiene todavía un campo laboral por cubrir algo extenso, primero, si vemos a las tecnologías Token Ring y FDDI como las más cercanas a Ethernet, debido a su alcance (LAN's), Ethernet anteriormente era superada por estas 2 tecnologías en cuanto velocidad (16 y 100 Mbps respectivamente), pero viendo el futuro de Ethernet a velocidades de 1 y hasta 10 Gbps, se puede decir está a la par al momento de diseñar una red, sólo queda mencionar algunos aspectos, una desventaja que tiene Ethernet con respecto a Token Ring es que sigue siendo propensa a fallas de transmisión, y que entre más grande sean las redes la desventaja es mayor, todo esto debido a sus modos de transmisión, Ethernet con CSMA/CD y Token ring sus Tokens, en redes de gran extensión las redes Token Ring serán más confiables; otra desventaja que tiene Ethernet, es que cuando hablamos de tecnología de Tokens aplicada con fibra óptica (FDDI), es la vulnerabilidad que tiene respecto a las interferencias de radio frecuencia y electromagnéticas, ya que las redes FDDI son inmunes a este tipo de interferencia, y los medios comúnmente utilizados en redes con tecnología Ethernet (UTP Cat5, Cat5e y Cat6) no son tan efectivos para contrarrestar esas interferencias, aun cuando se aplican algunas técnicas de construcción de cables para contrarrestar efectos relacionados a las diafonías, cabe mencionar también que regularmente los medios de fibra óptica son utilizados con Ethernet sólo para aplicaciones de Backbone, esto es para distancias mayores a 100 metros para interconexión de LAN's, por la misma desventaja que se mencionó de las interferencias, pero

estas desventajas que aparentan ser grandes y difíciles de superar, se pueden minimizar si se toma en cuenta los costos que requieren el diseño y la instalación de las redes Token Ring, ya que estos son mucho más elevados que los que requieren el diseño y la instalación de las redes basadas en tecnologías Ethernet, y si a esto agregamos que actualmente las redes más comunes son las Ethernet debido a que a nivel local pueden existir redes de menos de 10 hosts, y pueden ser instaladas en espacios muy reducidos sin la necesidad de grandes y costosos equipos de interconexión de equipos como las MAU utilizadas en las redes de tecnología de Tokens, y que además no se requiere de un servidor principal para que puedan compartir recursos e información entre ellas, y que basta con tener un buen diseño de cableado estructurado para evitar las interferencias, entonces las redes informáticas basadas en tecnología Ethernet son la opción más viable actualmente con respecto a las redes de tecnología de Tokens, y estas están siendo dejadas de implementar o sustituidas por las redes de tecnología Ethernet.

Otro campo con el cual está compitiendo la tecnología Ethernet, es con ATM, que es una tecnología implementada desde hace mucho tiempo y cuando fue implementada ofrecía una velocidad de 155 Mbps, y desde entonces es utilizada para aplicaciones multimedios, y principalmente en conexiones de backbone, en tiempos anteriores tenía gran auge debido principalmente a que la tecnología Ethernet estaba restringida o limitada a las redes LAN, y aunque en la actualidad no tiene ya esta restricción, aun hay varios aspectos a tomar en cuenta para determinar quien es mejor, si ATM o Ethernet, primeramente, las ventajas que tiene ATM son, una que la toda infraestructura de comunicación esta implementada e instalada desde hace mucho tiempo en grandes terrenos de las redes informáticas, y si la tecnología Ethernet quiere ganar este terreno se necesita nueva infraestructura que sea capaz de soportar las velocidades que ofrece actualmente la tecnología Ethernet (1 y 10 Gbps).

Otra ventaja de ATM es que está más apta para aplicaciones de video, debido a que cuenta con servicios como QoS (Quality of service) y CBR (Constant bit rate) para una mejor transmisión de grandes cantidades de datos, aunque actualmente también el IETF (Internet Engineering Task Force, un conjunto de protocolos de Internet) esta trabajando con RSVP (Resource Reservation Protocol) para proveer de un QoS a la tecnología Ethernet, aunque esta un poco limitado debido a que es un protocolo considerado de “máximo esfuerzo”, aunque con todo esto parece una mejor opción ATM sobre Ethernet, no debemos perder de punto de vista, otra vez, los costos, es decir, la tecnología Ethernet a velocidades de Gbps, se pretende que sea siempre gratuita, y la ATM requiere de un costo o una renta por el uso de la banda ancha, y además todas las aplicaciones e infraestructura ya aplicadas sobre Ethernet podrán trabajar con las nuevas velocidades de las redes Fast Ethernet y Gigabit Ethernet (100 Mbps, 1 Gbps, 10 Gbps) sin necesidad se implementar nuevas infraestructuras, y aunque actualmente ATM tiene aplicaciones con capacidad de transmisión superiores a 9.6 Gbps mediante SONET, es menor de lo que un futuro muy próximo podrá ofrecer gratis Ethernet para conexiones de Backbone, y debido a que no esta claro el futuro de las dos tecnologías, la conclusión más probable es que en el futuro próximo en lugar de competir todas estas tecnologías por el mercado, la tendencia las lleva a una fusión para mejor interoperabilidad y beneficio para todos los usuario de redes informáticas.

Entonces al finalizar este documento se concluye que ha cumplido su objetivo satisfactoriamente, logra dar una introducción a la tecnología Ethernet y sus principales características y funciones, se reconocen las distintas tecnologías WAN existentes, y sobre todo, ayuda a decidir cuándo usar la tecnología más apropiada a nuestras necesidades; al mismo tiempo da los fundamentos o guías para seguir estudiando más sobre el tema, conociendo el principio básico, deja puertas abiertas a cualquiera que desee adentrarse más en

temas de redes y tecnologías, sin restringir, si la persona es del área de informática o no lo es, creo que es entendible y despierta el interés de quien lo consulte. También cabe mencionar que además de ser un documento introductorio a las nuevas tecnologías, resulta ser un documento de consulta para aquellos que se encuentren estudiando una carrera afín a la informática o la computación en general.

Sabemos que existen diversos temas sobre los cuáles las redes se vuelven más interesantes y complejas como VLANs, VPN, protocolos de enrutamiento, direccionamiento VLSM, Wireless, etc. Ojala que con este trabajo se inicie una investigación más a fondo por parte del lector a todos esos temas de redes y se generen más documentos de consulta y apoyo para todos aquellos que se inician en la materia.

## GLOSARIO

AGP	Accelerated Graphics Port
CPU	Unidad de Procesamiento Central
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DMA	Dirección de Memoria Directa
DSL	Línea de Suscriptor Digital
EMI	Interferencia Electro Magnética
EPROM	Memoria Programable Borrable de Solo Lectura
FDDI	Interfaz de Datos Distribuida por Fibra
FTP	Protocolo de Transferencia de archivos
HTML	Hyper Text Markup Language
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IRQ	Petición de interrupción
ISA	Arquitectura estándar de la industria
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LASER	Amplificación de Luz por Radiación por Emisión Estimulada
LED	Diodo electro luminiscente
LLC	Control de Enlace Lógico
MAC	Control de Acceso al Medio
MAN	Red de Área Metropolitana
MAU	Unidad de Acceso Múltiple
NIC	Network Interface Card
OSI	Open Systems Interconnection
OUI	Identificador Exclusivo Organizacional
PCB	Printed Circuit Board, placa de circuito impreso
PCI	Peripheral Component Interconnect, Interconexión de componentes periféricos
PCMCIA	Personal Computer Memory Card International Association
RDSI	Red Digital de Servicios Integrados
RFI	Interferencia de Radio Frecuencia
SAN	Red de Área de Almacenamiento
SONET	Red Óptica Síncrona
STP	Shielded Twisted Pair
TCP/IP	Protocolo de Control de Transporte/Protocolo de Internet
TIA/EIA	Asociación de la Industria de Telecomunicaciones/ Asociación de Industrias Electrónicas
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VLSI	Very Large-Scale Integration
VLSM	Máscara de Subred de Longitud Variable
VPN	Red Privada Virtual

## BIBLIOGRAFIA

### LIBROS:

BROWN TODD, MILLER CHRIS, *Microsoft Windows 2000 Server Al descubierto*, Editorial Prentice Hall de Pearson, España, 2000, p.p 793

CISCO PRESS, *Academia de Networking de Cisco Systems CCNA 3 y 4 Guía del segundo año 3ª Edición*, Editorial Pearson Educación, México, 2004, p.p. 800

DAVIES JOSEPH, LEE THOMAS, *Microsoft Windows Server 2003 Protocolos y servicios TCP/IP Referencia Técnica*, McGraw Hill, México, 2003. p.p 657

RAYA JOSE LUIS, RAYA ELENA, *Aprenda Windows 2000 Server*, Editorial Alfaomega RA-MA, México, p.p 729

RAYA JOSE LUIS, RAYA LAURA, *Como construir una INTRANET con Windows 2000 Server*, Editorial Alfaomega RA-MA, México, 2001. p.p. 908

RAYA JOSE LUIS, RAYA LAURA, *Intranets y TCP/IP con Microsoft Windows Server 2003*, Editorial Alfaomega RA-MA, México, 2005, p.p. 920

WILLIAMS ROBERT, WALLA MARK, *La Biblia de Windows Server 2003. Administración de sistemas*, Editorial Anaya Multimedia, España, 2004, p.p. 1024

.

## OTRAS FUENTES:

[www.monografias.com](http://www.monografias.com)

[www.wikipedia.com](http://www.wikipedia.com)

[www.cisco.com/web/learning/netacad/index.html](http://www.cisco.com/web/learning/netacad/index.html)

[www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw\\_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm)

[www.erg.abdn.ac.uk/users/gorry/course/lan-pages/csma-cd.html](http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/csma-cd.html)

[www.howstuffworks.com/lan-switch3.htm](http://www.howstuffworks.com/lan-switch3.htm)