



**UNIVERSIDAD AUTÓNOMA DEL ESTADO  
DE HIDALGO**

**INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA**

INTRODUCCIÓN A LAS REDES ETHERNET

MONOGRAFÍA:

PARA OBTENER EL TÍTULO DE INGENIERO EN  
ELECTRÓNICA Y TELECOMUNICACIONES

PRESENTA:

P.I.E.T. VIANEY ORTEGA HERNÁNDEZ

ASESOR:

LIC. ÁNGEL MARTÍNEZ RODRÍGUEZ

PACHUCA DE SOTO HIDALGO., MAYO DEL 2006.

## **AGRADECIMIENTOS**

Es muy satisfactorio para mí expresar un agradecimiento público a las personas que de alguna manera, con su apoyo, consejos y colaboración hicieron posible esta monografía.

En estas líneas lo dejo palpable a quienes con sus conocimientos y dedicación me ayudaron a escalar este nuevo peldaño en la realización de la meta que me he fijado, en primer término al Lic. Ángel Martínez Rodríguez por su colaboración y asesoría, mis más sinceras gracias profesor, por su tiempo, paciencia y dedicación en la realización de esta monografía.

A mis padres, hermanos y amigos porque en ellos me he inspirado para salir adelante con todos mis proyectos y sueños en los cuales incluyo esta monografía, Gracias por su confianza y amor.

# ÍNDICE

<b>OBJETIVO GENERAL, OBJETIVO ESPECÍFICO</b>	<b>I</b>
<b>JUSTIFICACIÓN</b>	<b>II</b>
<b>INTRODUCCIÓN</b>	<b>III</b>
<b>ÍNDICE DE FIGURAS</b>	<b>VI</b>
<b>ÍNDICE DE TABLAS</b>	<b>VII</b>

## **CAPÍTULO 1. INTRODUCCIÓN A NETWORKING**

### **1.1 Conexión a la Internet**

1. 1. 1 Requisitos para la conexión a Internet	<b>1</b>
1. 1. 2 Tarjeta de interfaz de red como base para la comunicación de redes.	<b>2</b>
1. 1. 3 Instalación de NIC y módem	<b>3</b>
1. 1. 4 Descripción y configuración TCP/IP	<b>3</b>
1. 1. 5 Probar la conectividad con ping	<b>4</b>

### **1.2 Dispositivos de networking**

1.2.1 Topología de red	<b>5</b>
1.2.2 Protocolos de red	<b>7</b>
1.2.3 Redes de área local (LAN)	<b>7</b>
1.2.4 Redes de área amplia (WAN)	<b>8</b>
1.2. 5 Redes de área metropolitana (MAN)	<b>8</b>
1.2. 6 Redes de área de almacenamiento (SAN)	<b>9</b>
1.2 .7 Red privada virtual (VPN)	<b>9</b>
1.2.8 Ventajas de las VPN	<b>10</b>
1.2.9 Redes internas y externas	<b>11</b>
1.2.10 Importancia del ancho de banda	<b>11</b>
1.2.11 Limitaciones	<b>12</b>

## **CAPÍTULO 2. MEDIOS DE NETWORKING**

### **2.1 Cableado LAN**

2. 1. 1 Capa física de la LAN	<b>13</b>
2. 1. 2 Conceptos de ethernet	<b>14</b>

2. 1. 3 Medios de ethernet y requisitos de conectores	15
2. 1. 4 Medios de conexión	15
2. 1. 5 Implementación del UTP	16
2. 1. 6 Repetidores	17
2. 1. 7 Concentradores	18
2. 1. 8 Redes inalámbricas	19
2. 1. 9 Puentes	20
2. 1. 10 Conmutadores	21
2. 1. 11 Conectividad del host	22
2. 1. 12 Comunicación de par a par	22
2. 1. 13 Cliente/servidor	23
<b>2.2 Cableado WAN</b>	
2. 2. 1 Capa física de las WAN	23
2. 2. 2 Conexiones seriales de WAN	24
2. 2. 3 Conexiones seriales y ruteadores	25
2. 2. 4 Conexiones BRI RDSI y ruteadores	25
2. 2. 5 Conexiones DSL y ruteadores	26
2. 2. 6 Conexiones de cable-modem y ruteadores	26
2. 2. 7 Configuración de las conexiones de la consola	27

## **CAPÍTULO 3. PRINCIPIOS BÁSICOS DE ETHERNET**

### **3.1 Principios básicos de Ethernet**

3. 1. 1 Introducción a ethernet	28
3. 1. 2 Reglas del IEEE para la denominación de ethernet	29
3. 1. 3 Ethernet y el modelo OSI	30
3. 1. 4 Denominación	31
3. 1. 5 Entramado de la capa 2	32
3. 1. 6 Estructura de la trama de ethernet	34
3. 1. 7 Campos de la trama de ethernet	35

### **3.2 Operación de Ethernet**

3. 2. 1 Control de acceso al medio (MAC )	36
3. 2. 2 Reglas de MAC y detección de la colisión/postergación	

de la retransmisión	37
3. 2. 3 Temporización de ethernet	38
3. 2. 4 Espacio entre las tramas y postergación	39
3. 2. 5 Manejo de los errores	40
3. 2. 6 Tipos de colisiones	41
3. 2. 7 Errores de ethernet	42
3. 2. 8 FCS y más allá	43
3. 2. 9 Auto-negociación de ethernet	44

## **CAPÍTULO 4 INTRODUCCIÓN A ETHERNET**

### **4. 1 Ethernet de 10-Mbps y 100-Mbps**

4.1.1 Ethernet de 10-Mbps	45
4.1.2 10BASE5	45
4.1.3 10BASE2	46
4.1.4 10BASE-T	46
4.1.5 Cableado y arquitectura de 10BASE-T	47
4.1.6 Ethernet de 100-Mbps	48
4.1.7 100BASE-TX	48
4.1.8 100BASE-FX	48
4.1.9 Arquitectura de la fast ethernet	49

### **4. 2 Ethernet Gigabit y 10-Gigabit**

4.2.1 Ethernet de 1000-Mbps	50
4.2.2 1000BASE-T	51
4.2.3 Arquitectura de gigabit ethernet	52
4.2.4 10-Gigabit ethernet	52
4.2.5 Arquitecturas de 10-gigabit ethernet	54

## **CAPÍTULO 5. CONMUTACIÓN DE ETHERNET**

### **5. 1 Conmutación de ethernet**

5.1.1 Punteo de capa 2	55
5.1.2 Conmutación a nivel de capa 2	57

5.1.3 Operación de conmutadores	57
5.1.4 Latencia	58
5.1.5 Modos de conmutación	59
<b>5.2 Dominios de colisión y de broadcast</b>	
5.2.1 Entorno de medios compartidos	59
5.2.2 Dominios de colisión	60
5.2.3 Segmentación	62
5.2.4 Broadcasts de capa 2	63
5.2.5 Dominios de broadcast	64

## **CAPÍTULO 6. ETHERNET DE 100Mbps, TECNOLOGÍAS COMPETITIVAS Y REDES INALÁMBRICAS 802.11**

<b>6.1 Evolución de ethernet</b>	66
6.1.2 Tecnología	66
6.1.3 Aplicaciones y productos	69
6.1.4 Tecnologías competitivas	70
6.1.5 Ethernet en el futuro	70
6.1.6 Packet bursting	71
<b>6.2 REDES INALÁMBRICAS 802.11</b>	
6.2.1 Wi-Fi	73
6.2.2 Funcionamiento de Internet Turbo Wi-Fi	74
6.2.3 Las redes inalámbricas o WN	74
6.2.4 Redes inalámbricas de consumo	75
6.2.5 Clasificación de las redes inalámbricas - Redes inalámbricas personales	76
6.2.6 Velocidad vs Modulación	77
6.2.7 Topología y Modos de funcionamiento de los dispositivos	78
<b>CONCLUSIONES</b>	79
<b>GLOSARIO</b>	80
<b>SIGLARIO</b>	87
<b>REFERENCIAS BIBLIOGRÁFICAS</b>	89

## **OBJETIVO GENERAL**

El principal objetivo de esta monografía es realizar el estudio de ethernet, con el propósito de encontrar mejores soluciones a las diferentes necesidades de comunicación e intercambio de información a través de redes ethernet que los países requieren para promover su desarrollo integral y poder anexarse aun mundo cada vez mas interrelacionado por las redes modernas.

## **OBJETIVO ESPECIFICO**

- Tener los conocimientos necesarios sobres los tipos de redes ethernet.
- Conocer la importancia de ethernet.
- Conocer diferentes tipos de ethernet.
- Diferenciar cada tipo de red ethernet.
- Aplicar y conocer los medios y dispositivos necesarios de ethernet para su conexión.

## JUSTIFICACIÓN

En esta época en que la computación resultan indispensables en casi todas las actividades que realiza el ser humano, se hace necesario que independientemente de su campo de trabajo o estudio toda persona conozca al menos los fundamentos de la computación, ya que esta, y en general la informática son hoy por hoy un requerimiento fundamental para lograr un mejor puesto de trabajo en oficinas, industrias, bancos, escuelas centros de investigación e incluso para realizar tareas en el mismo hogar.

Por lo tanto debido a que ethernet ha evolucionado desde las primeras tecnologías, a las tecnologías fast, a las de gigabit y a las de multigigabit, es que hemos decidido investigar sobre este tema.

Se puede observar que las tecnología de ethernet en el mundo de las redes de telecomunicaciones en la actualidad tienen una participación muy importante e inclusive se sigue desarrollando, por lo tanto sabiendo que se necesita conocer mas a fondo sobre ethernet es que decidimos desarrollar esta monografía, con la finalidad de dar a conocer los elementos necesarios tales como estándares, dispositivos de red, protocolos, medios, etc., para comprender las tecnologías de ethernet en las redes de telecomunicaciones. Lo que representa un tema importante para su investigación y tema tomando en cuenta para la realización de una monografía, ya que la información que podemos encontrar sobre esta tema resulta ser indispensable a quienes utilizan y desean conocer mas sobre redes de computadoras y ethernet.

## INTRODUCCIÓN

Desde 1970 la red ethernet es la tecnología más representativa de las redes de trabajo. Hay un estimado que en 1996 el 82% de todos los equipos de redes eran Ethernet. En 1995 el estándar fast ethernet fue aprobado por la IEEE. El fast ethernet provisto de un ancho de banda 10 veces mayor y nuevas características tales como transmisión full-duplex y auto negociación. Se estableció ethernet como una tecnología escalable. Ahora, el estándar gigabit ethernet es aceptado como una escala superior.

Fast ethernet fue publicada por una alianza de consorcios de industriales. En mayo de 1996 se formó la alianza gigabit ethernet conformada por 11 compañías, poco después la IEEE anuncia la formación del 802.3z, proyecto del estándar gigabit ethernet.

En el capítulo 1 tratamos las NIC, TCP/IP, la conectividad con los diferentes tipos de ping, así como de los switches y ruteadores así como de hosts, tokens, también mencionamos los componentes de las LAN, mencionamos para qué están diseñadas las WAN, las características de las SAN, y cómo se puede crear una MAN, de las VPN y sus ventajas, también de las redes externas e internas y también tratamos de los anchos de banda.

En el capítulo 2 nos dice que se utilizan varios símbolos para representar los distintos tipos de medios. Y deducimos que ethernet es la tecnología LAN de uso más frecuente, y los medios de ethernet y requisitos de conectores, además vemos que un repetidor recibe una señal, la regenera, y la transmite, explicándonos su proceso, al igual que el de los concentradores que en realidad son repetidores multipuerto. Y nos da una reseña de las redes inalámbricas donde vemos los puentes los switch, host, así como la comunicación par a par, cliente servidor y los cableados.

Capítulo 3 en este capítulo nos basamos principalmente en ethernet donde vemos las reglas del IEEE para la denominación de ethernet y cómo ethernet opera en dos áreas del modelo OSI, también observamos la función del entramado de la capa 2 y la estructura de la trama, MAC que se refiere a los protocolos que determinan cuál de los computadores de un entorno de medios compartidos, así como reglas de MAC y detección de la colisión/postergación de la retransmisión, también se verán los tipos de colisiones que por lo general, las colisiones se producen cuando dos o más estaciones de ethernet transmiten al mismo tiempo dentro de un dominio de colisión. Así como los errores de ethernet donde nos dice que el conocimiento de los errores típicos es invaluable para entender tanto la operación como la detección de fallas de las redes ethernet.

Capítulo 4 en este veremos ethernet de 10-Mbps de los cuales definimos 10BASE5, 10BASE2, 10BASE-T, así el cableado y arquitectura. Ethernet de 100-Mbps donde vemos que las dos tecnologías que han adquirido relevancia son 100BASE-TX, que es un medio UTP de cobre y 100BASE-FX, que es un medio multimodo de fibra óptica. Así como la arquitectura de la fast ethernet, también incluimos ethernet gigabit y 10-gigabit, en ethernet de 1000-Mbps se explican los estándares para ethernet de 1000-Mbps o gigabit ethernet representan la transmisión a través de medios ópticos y de cobre, su arquitectura. Y en la de 10-gigabit ethernet donde se considera una variedad de implementaciones y arquitecturas.

En el capítulo 5 veremos puenteo de capa 2 donde vemos que un puente guarda una tabla de direcciones mac y sus puertos asociados. Así como la conmutación a nivel de capa 2, otros temas que incluimos es la operación de switches, la latencia que es el retardo que se produce 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. Y modos de conmutación como son

conmutación por el método de corte, conmutación síncrona, conmutación asimétrica. Otro de los temas es entorno de medios compartidos, Los dominios de colisión que son los segmentos de red física conectados, donde pueden ocurrir colisiones. Segmentación, broadcasts de capa 2, y dominios de broadcast que es un grupo de dominios de colisión conectados por dos dispositivos de capa 2.

En el capítulo 6 veremos el futuro de ethernet que nos dice como ha evolucionado desde las primeras tecnologías, a las tecnologías fast, a las de gigabit y a las de multigigabit. Ethernet a mayor velocidad o conmutadores. Veremos que es Wi-Fi, que es un conjunto de estándares para redes inalámbricas, cómo funciona internet turbo Wi-Fi, donde vemos que utiliza un modem inalámbrico que opera con una frecuencia pública (no licenciada) de 2.4 Ghz. bajo el estándar 802.11 g., Las redes inalámbricas o WN, redes inalámbricas de consumo. Clasificación de las redes inalámbricas - Redes inalámbricas personales. Velocidad vs modulación y modos de funcionamiento de los dispositivos donde nos explica que es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi.

## ÍNDICE DE TABLAS

<b>NUMERO</b>	<b>NOMBRE</b>	<b>NÚMERO DE PÁGINA</b>
Tabla 1	Unidades de ancho de banda	12
Tabla 2	La disposición de pins para un cable transpuesto	27

---

---

## ÍNDICE DE FIGURAS

Figura1	Recepción, transmisión y detección de colisiones	2
Figura 2	NIC interna, MODEM externo 56 Kb, MODEM PC CARD	3
Figura 3	Dispositivos de networking	5
Figura 4	Topologías de red	6
Figura 5	Conexión típica de una VPN de acceso	10
Figura 6	Medios físicos	13
Figura 7	Medios de conexión	15
Figura 8	Implementación UTP	17
Figura 9	Redes inalámbricas	20
Figura10	Medio par a par	23
Figura11	Ruteador de cisco 1603 y 3640	25
Figura12	El puerto BRI al dispositivo del proveedor del servicio	26
Figura13	UOI Y PROVEEDOR ASIGNADO (NICS, Interfaces)	31
Figura14	Formas para calcular el # de secuencia de verificación de trama	34
Figura15	Similitudes y diferencias entre las capas 1 y 2 del modelo OSI	37
Figura16	Prueba de longitud mín. como la prueba de la checksum de FCS	40
Figura17	Una trama con error de FCS	43
Figura18	La ráfaga de pulsos FLP está hecha de múltiples en NLP	44
Figura 19	Cableado y Arquitectura de 10BASE-T	47
Figura 20	Conector de par trenzado balanceado de 100 ohms.	48
Figura 21	Subcapa de control de enlace lógica	51
Figura 22	El puente controla el tráfico entre los dominios de colisión	56
Figura 23	Broadcast de dominio	57
Figura 24	Medio compartido, medio extendido, punto a punto	60
Figura 25	La regla 5-4-3-2-1	62
Figura 26	Formato de trama ethernet cuando el carrier extensión es usado	71
Figura 27	Como trabaja el packet burst.	72
Figura 28	Diferentes capas de la arquitectura del protocolo gigabit ethernet	72

## **1 INTRODUCCIÓN A NETWORKING**

### **1.1 Conexión a la Internet**

- 1. 1. 1 Requisitos para la conexión a Internet
- 1. 1. 2 Tarjeta de interfaz de red como base para la comunicación de redes
- 1. 1. 3 Instalación de NIC y módem
- 1. 1. 4 Descripción y configuración TCP/IP
- 1. 1. 5 Probar la conectividad con ping

### **1.2 Dispositivos de networking**

- 1.2.1 Topología de red
- 1.2.2 Protocolos de red
- 1.2.3 Redes de área local (LAN)
- 1.2.4 Redes de área amplia (WAN)
- 1.2.5 Redes de área metropolitana (MAN)
- 1.2. 6 Redes de área de almacenamiento (SAN)
- 1.2. 7 Red privada virtual (VPN)
- 1.2 .8 Ventajas de las VPN
- 1.2.9 Redes internas y externas
- 1.2.10 Importancia del ancho de banda
- 1.2 .11 Limitaciones

## **1.1 CONEXIÓN A INTERNET**

### **1.1.1 Requisitos para la conexión a Internet**

La Internet se podría definir como una red que engloba una serie de redes de computadores con la finalidad de permitir el libre intercambio de información entre sus usuarios. Basa su utilidad su utilidad especialmente en 4 servicios: correo electrónico, servicio de noticias, acceso remoto y transferencia de archivos. [1]

La Internet es la red de datos más importante del mundo. Se compone de una gran cantidad de redes grandes y pequeñas interconectadas. Computadores individuales son las fuentes y los destinos de la información a través de la Internet. Se realiza una conexión física conectando una tarjeta adaptadora, tal como un módem o una NIC, desde un PC a una red. La conexión física se utiliza para transferir las señales entre los distintos PC 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. 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 y netscape. El protocolo de transferencia de archivos (FTP) se utiliza para descargar archivos y programas de internet. Los navegadores de Web también utilizan aplicaciones plug-in propietarias para mostrar tipos de datos especiales como, por ejemplo, películas o animaciones flash. [3]

### 1.1.2 La tarjeta de interfaz de red como base para la comunicación de redes.

Una tarjeta de interfaz de red (NIC), o adaptador LAN, provee capacidades de comunicación en red desde y hacia un PC. En los sistemas computacionales de escritorio, 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 los sistemas computacionales portátiles, está comúnmente integrado en los sistemas o está disponible como una pequeña tarjeta PCMCIA, del tamaño de una tarjeta de crédito. La NIC se comunica con la red a través de una conexión serial y con el computador a través de una conexión paralela. Ver figura 1. La NIC 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 asignado por medio del cual donde el computador puede esperar que un dispositivo específico lo interrumpa cuando dicho dispositivo envía al computador señales acerca de su operación. 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 al computador. Al seleccionar una NIC, hay que tener en cuenta los siguientes factores:

- **Protocolos:** Ethernet, Token Ring y FDDI.
- **Tipos de medios:** Cable UTP, STP, FTP.
- **Tipo de bus de sistema:** PCI o ISA. . [4]

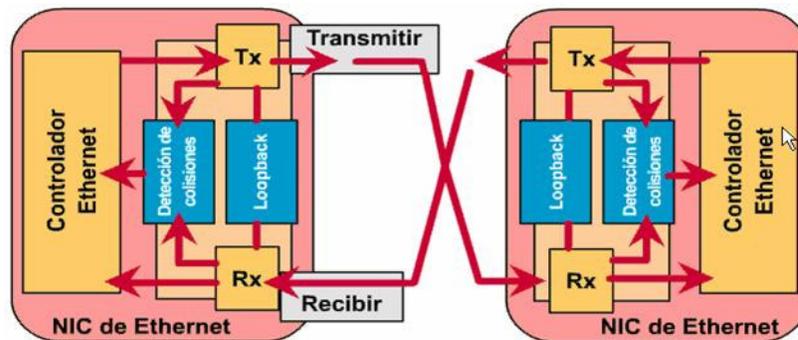


Figura 1. Recibir (Rx), transmitir (Tx) y detección de colisiones son muy importantes, el conector físico de Ethernet proporciona varios circuitos.

### 1.1.3 Instalación de NIC y módem

Para realizar la instalación de una NIC o un módem se requieren los siguientes recursos:

- Conocimiento acerca de cómo debe configurarse el adaptador, incluyendo los jumpers y el software plug-and-play
- Disponibilidad de herramientas de diagnóstico
- Capacidad para resolver conflictos de recursos de hardware. [5]



Figura 2 a) NIC interna. b) MODEM externo 56 Kb c) MODEM PC CARD

### 1.1.4 Descripción y configuración TCP/IP

Para habilitar TCP/IP en la estación de trabajo, ésta debe configurarse utilizando las herramientas del sistema operativo. Ya sea que se utilice un sistema operativo windows o mac, el proceso es muy similar. [6]

El protocolo TCP/IP transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de datos. IP, un protocolo del nivel de red de OSI, permite a las aplicaciones ejecutarse en forma transparente sobre las redes interconectadas. De esta forma las aplicaciones no necesitan conocer que hardware esta siendo utilizado en la red, por lo que la misma aplicación puede ejecutarse en una topología de X.25. TCP, un protocolo del nivel de transporte de ethernet, token-ring o OSI, asegura que los datos sean, entregados, que lo que recibe se corresponda con lo que se envió y que los paquetes sean reensamblados en el orden en que fueron enviados. [1]

### 1.1.5 Probar la conectividad con ping

El comando `ping` funciona enviando paquetes IP especiales, llamados datagramas de petición de eco ICMP a un destino específico. Cada paquete que se envía es una petición de respuesta. La pantalla de respuesta de un ping contiene la proporción de éxito y el tiempo de ida y vuelta del envío hacia llegar a su destino. A partir de esta información, es posible determinar si existe conectividad a un destino. El comando `ping` se utiliza para probar la función de transmisión/recepción de la NIC, la configuración TCP/IP y la conectividad de red.

**Ping 127.0.0.1:** Este es un tipo especial de ping que se conoce como prueba interna de loopback. Se usa para verificar la configuración de red TCP/IP.

**Ping dirección IP del computador host:** Un ping a un PC host verifica la configuración de la dirección TCP/IP para el host local y la conectividad al host.

**Ping dirección IP de gateway por defecto:** Un ping al gateway por defecto verifica si se puede alcanzar el ruteador que conecta la red local a las demás redes.

**Ping dirección IP de destino remoto:** Un ping a un destino remoto verifica la conectividad a un host remoto. [7]

## 1.2 DISPOSITIVOS DE NETWORKING

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos:

El primer grupo { esta compuesto por los dispositivos de usuario final { computadores, impresoras, escáneres, además dispositivos que brindan servicios directamente al usuario.

El segundo grupo { formado por los dispositivos de red { son todos aquellos que conectan entre si a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas. Los dispositivos host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos. [8]

Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, concentradores, puentes, conmutadores y ruteadores. (ver figura 3). [8]

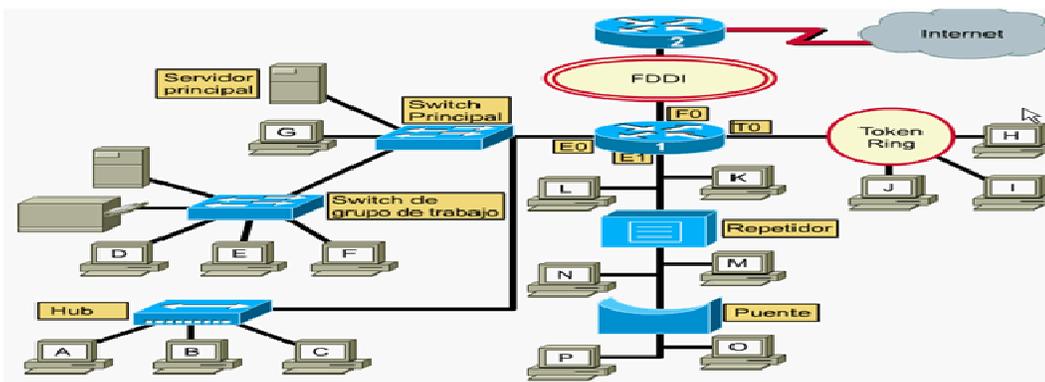


Figura 3 dispositivos de networking

### 1.2.1 Topología de red

Se denomina topología a la forma geométrica en que están distribuidos las estaciones de trabajo y los cables que las conectan. [1]

Una parte de la definición topológica es:

topología	}	es la disposición
física		real de los cables o medios
topología	}	define la forma en que los host acceden a los medios
lógica		para enviar datos.

Las topologías físicas más comúnmente usadas son las siguientes:

- Una topología de bus usa un solo cable que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este.
- 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.
- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de concentradores o conmutadores.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los concentradores o conmutadores entre sí, el sistema se conecta con un computador 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. (ver figura 4)

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. La segunda topología lógica es la transmisión de tokens. 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. [9]

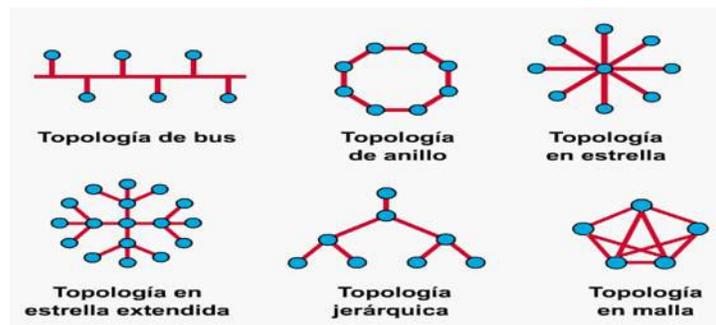


Figura 4. Topologías de red

### **1.2.2 Protocolos de red**

Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador. Controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo los computadores se conectan a la red
- Cómo se formatean los datos para su transmisión
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de diferentes institutos y asociaciones: IEEE, ANSI, TIA, la EIA y UIT. [10]

### **1.2.3 Redes de ares local (LAN)**

Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red
- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking

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. [9]

#### **1.2.4 Redes de área amplia (WAN)**

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores 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. Las WAN permiten que los computadores, 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. 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). [9]

#### **1.2.5 Redes de área metropolitana (MAN)**

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. 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. [11]

### 1.2.6 Redes de área de almacenamiento (SAN)

Una SAN 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. [12]

### 1.2.7 Red privada virtual (VPN)

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. 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 el PC del empleado y un ruteador VPN en la sede. [13]

### 1.2.8 Ventajas de las VPN

La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como internet. 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. A continuación se describen los tres 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, DSL, IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales (figura 5). [14]

**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. [14]

**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. [14]

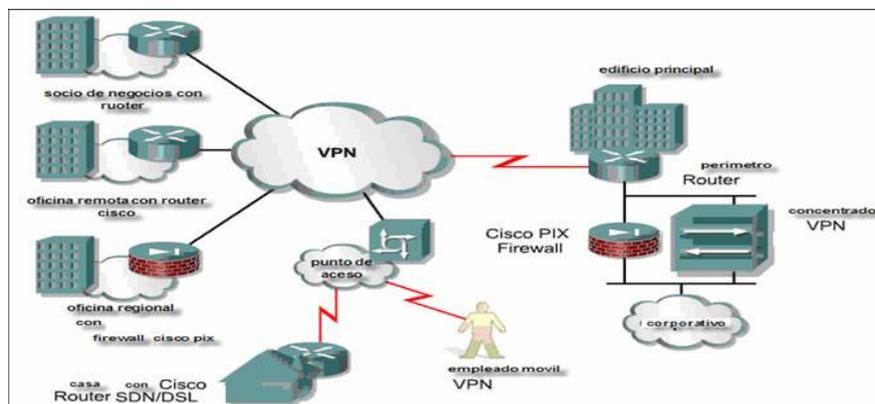


Figura 5 Conexión típica de una VPN de acceso.

### **1.2.9 Redes internas y externas**

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet. Dentro de una red interna, los servidores de web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores. Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas. [15]

### **1.2.10 Importancia del ancho de banda**

El ancho de banda se define como la cantidad de información que puede fluir a través de una conexión de red en un período dado es esencial comprender el concepto de ancho de banda al estudiar networking, por las siguientes cuatro razones:

**El ancho de banda es finito.** Existen límites para la capacidad de la red para transportar información. El ancho de banda está limitado por las leyes de la física y por las tecnologías empleadas para colocar la información en los medios. La fibra óptica posee el potencial físico para proporcionar un ancho de banda prácticamente ilimitado.

**El ancho de banda no es gratuito.** Es posible adquirir equipos para una red de área local (LAN) capaz de brindar un ancho de banda casi ilimitado durante un período extendido de tiempo. Para conexiones de red de área amplia (WAN), casi siempre hace falta comprar el ancho de banda de un proveedor de servicios.

**El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender internet.** La información fluye en una cadena de bits de un computador a otro en todo el mundo. Estos bits representan enormes cantidades de información que fluyen de ida y de vuelta a través del planeta en segundos, o menos.

**La demanda de ancho de banda no para decrecer** a entrega de contenidos de medios enriquecidos a través de la red, incluyendo video y audio fluido, requiere muchísima cantidad de ancho de banda. Hoy se instalan comúnmente sistemas telefónicos IP en lugar de los tradicionales sistemas de voz, lo que contribuye a una mayor necesidad de ancho de banda. [16]

unidades de ancho de banda	abreviacion	equivalencias
bits por segundo	bps	1 bps =unidad fundamental de ancho de banda
kilobits por segundo	kbps	1 kbps = 1,000 bps = $10^3$ bps
megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

Tabla 1 Unidades de ancho de banda

### 1.2.11 Limitaciones

Las señales se transmiten a través de cables de cobre de par trenzado, cables coaxiales, fibras ópticas, y por el aire. Las diferencias físicas en las formas en que se transmiten las señales son las que generan las limitaciones fundamentales en la capacidad que posee un medio dado para transportar información. No obstante, el verdadero ancho de banda de una red queda determinado por una combinación de los medios físicos y las tecnologías seleccionadas para señalizar y detectar señales de red. [17].

## CAPÍTULO 2

### 2 MEDIOS DE NETWORKING

#### 2.1 Cableado LAN

- 2. 1. 1 Capa física de la LAN
- 2. 1. 2 Concepto de ethernet
- 2. 1. 3 Medios de Ethernet y requisitos de conectores
- 2. 1. 4 Medios de conexión
- 2. 1. 5 Implementación del UTP
- 2. 1. 6 Repetidores
- 2. 1. 7 Concentradores
- 2. 1. 8 Redes inalámbricas
- 2. 1. 9 Puentes
- 2. 1. 10 Conmutadores
- 2. 1. 11 Conectividad del host
- 2. 1. 12 Comunicación de par a par
- 2. 1. 13 Cliente/servidor

#### 2.2 Cableado WAN

- 2. 2. 1 Capa física de las WAN
- 2. 2. 2 Conexiones seriales de WAN
- 2. 2. 3 Conexiones seriales y ruteadores
- 2. 2. 4 Conexiones BRI RDSI y routers
- 2. 2. 5 Conexiones DSL y routers
- 2. 2. 6 Conexiones de cable-modem y routers
- 2. 2. 7 Configuración de las conexiones de la consola.

## 2.1 CABLEADO LAN

### 2.1.1 Capa física de la LAN

Se utilizan varios símbolos para representar los distintos tipos de medios. token ring se representa con un círculo. La Interfaz de datos distribuida por fibra (FDDI) se representa con dos círculos concéntricos y el símbolo de ethernet es una línea recta. Las conexiones seriales se representan con un rayo. Cada red informática se puede desarrollar con varios tipos de medios distintos. La función de los medios consiste en transportar un flujo de información a través de la LAN. Las LAN inalámbricas usan la atmósfera, o el espacio como medio. Otros medios para networking limitan las señales de red a un cable o fibra. Los medios de networking se consideran componentes de la capa 1, o la capa física, de las LAN. Cada medio tiene sus ventajas y desventajas. Algunas de las ventajas y desventajas se relacionan con:

- La longitud del cable
- El costo
- La facilidad de instalación
- La susceptibilidad a interferencias

El cable coaxial, la fibra óptica, e incluso el espacio abierto pueden transportar señales de red. Sin embargo, el principal medio que se estudiará es el cable de par trenzado no blindado de categoría 5 (UTP CAT 5) que incluye la familia de cables categoría 5e. Muchas topologías son compatibles con las LAN así como muchos diferentes medios físicos. [18] (Figura 6)

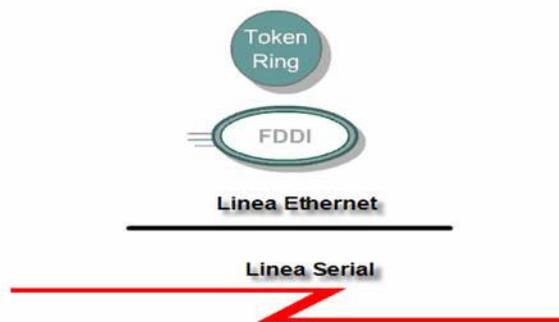


Figura 6 medios físicos

### 2.1.2 Conceptos de ethernet

Ethernet es la tecnología LAN de uso más frecuente. Un grupo formado por las empresas: digital equipment company, intel y xerox, conocido como DIX, fue el primero en implementar ethernet. DIX creó e implementó la primera especificación LAN ethernet, la cual se utilizó como base para la especificación 802.3 del IEEE, publicada en 1980. Más tarde, el IEEE extendió la especificación 802.3 a tres nuevas comisiones conocidas como 802.3u (fast ethernet), 802.3z (gigabit ethernet transmitido en fibra óptica) y 802.3ab (gigabit ethernet en UTP). Los requisitos de la red pueden forzar a la actualización a topologías de ethernet más rápidas. La mayoría de las redes de ethernet admiten velocidades de 10 Mbps y 100 Mbps. La nueva generación de productos para multimedia, imagen y base de datos puede fácilmente abrumar a redes que funcionan a las velocidades tradicionales de ethernet de 10 y 100 Mbps. Los administradores de red pueden considerar proveer gigabit ethernet desde el hasta los usuarios finales. Los costos de instalación de un nuevo cableado y de adaptadores pueden hacer que esto resulte casi imposible. Por el momento, gigabit ethernet en el escritorio no constituye una instalación estándar. Por lo general, las tecnologías ethernet se pueden utilizar en redes de muchas maneras diferentes:

- Se puede utilizar ethernet de 10 Mbps a nivel del usuario para brindar un buen rendimiento. Los clientes o servidores que requieren mayor ancho de banda pueden utilizar ethernet de 100-Mbps. [19]
- Se usa fast ethernet como enlace entre el usuario y los dispositivos de red. Puede admitir la combinación de todo el tráfico de cada segmento ethernet. Para mejorar el rendimiento cliente-servidor a través de la red y evitar los cuellos de botella, se puede utilizar fast ethernet para conectar servidores empresariales. [19]

### 2.1.3 Medios de ethernet y requisitos de conectores

Antes de seleccionar la implementación de ethernet, tenga en cuenta los requisitos de los conectores y medios para cada una de ellas. También tenga en cuenta el nivel de rendimiento que necesita la red. Las especificaciones de los cables y conectores usados para admitir las implementaciones de ethernet derivan del cuerpo de estándares de TIA y EIA. Las categorías de cableado definidas para ethernet derivan del estándar de recorridos y espacios de telecomunicaciones para edificios comerciales EIA/TIA-568 (SP-2840). [19]

### 2.1.4 Medios de conexión

El jack y el conector de jack registrado (RJ-45) son los más comunes. En algunos casos el tipo de conector de la tarjeta de interfaz de red (NIC) no se ajusta al medio al que se tiene que conectar. Puede existir una interfaz para el conector interfaz de unidad de conexión (AUI) de 15 pins. El conector AUI permite que medios diferentes se conecten cuando se usan con el transceptor apropiado. Un transceptor es un adaptador que convierte un tipo de conexión a otra. Por ejemplo, un transceptor convierte un conector AUI en uno RJ-45, coaxial, o de fibra óptica. En ethernet 10BASE5, o thicknet, se utiliza un cable corto para conectar el AUI a un transceptor en el cable principal. (figura7) [19]

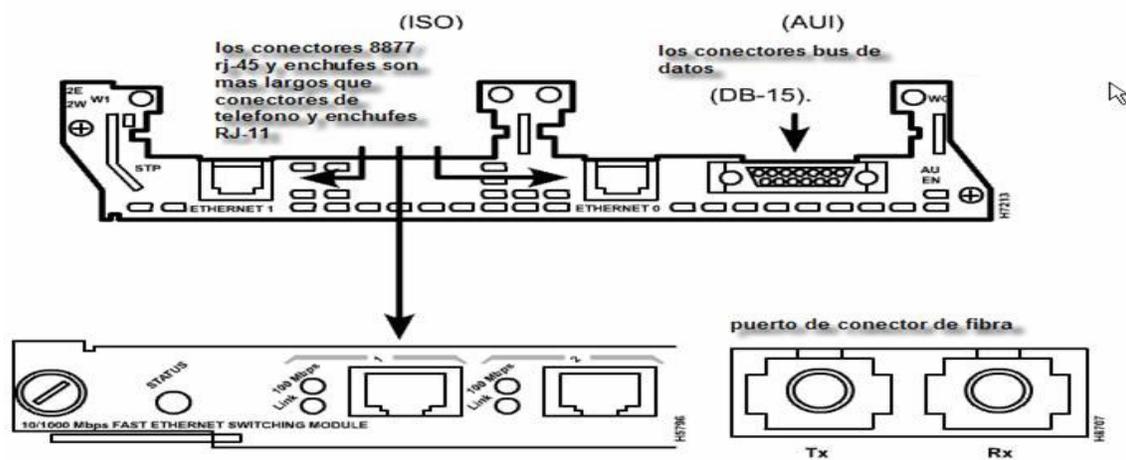


Figura 7 medios de conexión

### 2.1.5 Implementación del UTP

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. El conector transparente RJ-45 muestra ocho hilos de distintos colores. Cuatro de estos hilos conducen el voltaje y se consideran "tip" (punta) (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman "ring" (anillo) (R1 a R4). Tip y ring son términos que surgieron a comienzos de la era de la telefonía. Hoy, estos términos se refieren al hilo positivo y negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente. El conector RJ-45 es el componente macho, engarzado al extremo del cable. Cuando observa el conector macho de frente, las ubicaciones de los pins están numeradas desde 8, a la izquierda, hasta 1, a la derecha. El jack es el componente femenino en un dispositivo de red, toma de pared o panel de conexión. Para que la electricidad fluya entre el conector y el jack, el orden de los hilos debe seguir el código de colores T568A, o T568B recomendado en los estándares EIA/TIA-568-B.1 Identifique la categoría de cableado EIA/TIA correcta que debe usar un dispositivo de conexión, refiriéndose a la documentación de dicho dispositivo, o ubicando alguna identificación en el mismo cerca del jack. Si no se dispone de la documentación o de alguna identificación, use categoría 5E o mayor, dado que las categorías superiores pueden usarse en lugar de las inferiores. Así podrá determinar si va a usar cable straight-through o crossover. Si el orden de los hilos de color es el mismo en cada extremo, entonces el cable es de conexión directa. En un cable de conexión cruzada, los conectores RJ-45 de ambos extremos muestran que algunos hilos de un extremo del cable están cruzados a un pin diferente en el otro extremo del cable. (figura 8). Utilice cables de conexión directa para el siguiente cableado:

- Conmutador a ruteador
- Conmutador a PC o servidor
- Concentrador a PC o servidor

Utilice cables de conexión cruzada para el siguiente cableado:

- Conmutador a conmutador
- Conmutador a concentrador
- Concentrador a concentrador
- Ruteador a ruteador
- PC a PC
- Ruteador a PC. [19]

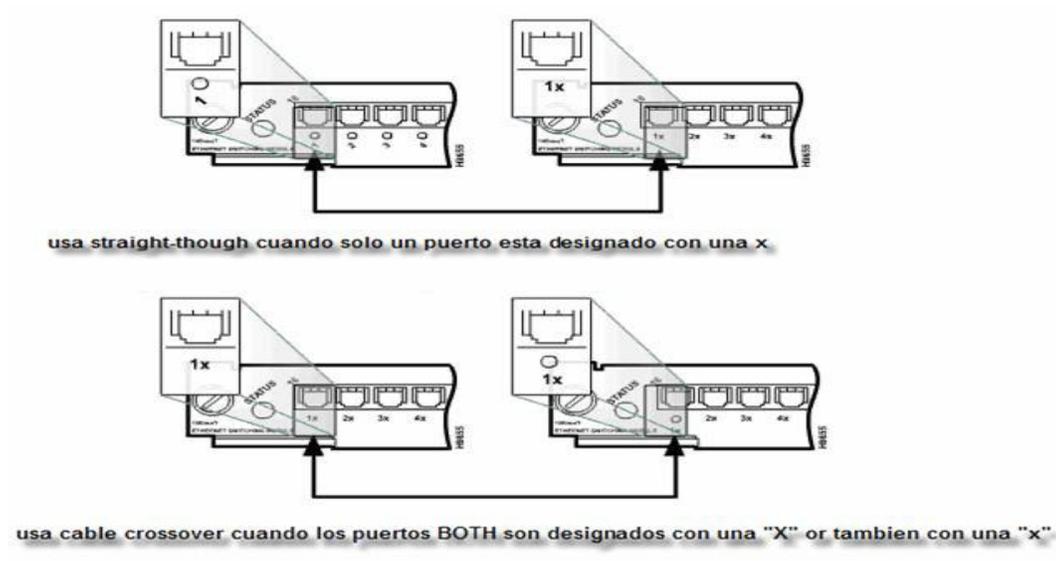


Figura 8 implementaciones UTP

### 2.1.6 Repetidores

Un repetidor recibe una señal, la regenera, y la transmite. El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. En ethernet e IEEE 802.3 se implementa la "regla 5-4-3", en referencia al número de repetidores y segmentos en un de acceso compartido con topología de árbol. La "regla 5-4-3 divide la red en dos tipos de segmentos físicos: Segmentos poblados (de usuarios), y Segmentos no poblados (enlaces). En los segmentos poblados se conectan los sistemas de los usuarios. Los segmentos no poblados se usan para conectar los repetidores de la red entre si. La regla manda que entre cualquiera dos nodos de una red, puede existir un máximo de

cinco segmentos, conectados por cuatro repetidores o concentradores, y solamente tres de los cinco segmentos pueden tener usuarios conectados a los mismos. El protocolo ethernet requiere que una señal enviada en la LAN alcance cualquier parte de la red dentro de una longitud de tiempo especificada. La “regla 5-4-3” asegura que esto pase. Cada repetidor a través del cual pasa la señal añade una pequeña cantidad de tiempo al proceso, por lo que la regla está diseñada para minimizar el tiempo de transmisión de la señal. Demasiada latencia en la LAN incrementa la cantidad de colisiones tardías, haciendo la LAN menos eficiente. [20]

### 2.1.7 Concentradores

En realidad son repetidores multipuerto. En muchos casos, la diferencia entre los dos dispositivos radica en el número de puertos que cada uno posee. Mientras que un repetidor convencional tiene sólo dos puertos, un concentrador por lo general tiene de cuatro a veinticuatro puertos. Por lo general se utilizan en las redes ethernet 10BASE-T o 100BASE-T. El uso de un concentrador hace que cambie la topología de la red desde un bus lineal, donde cada dispositivo se conecta de forma directa al cable, a una en estrella. En un concentrador, los datos que llegan a un puerto del concentrador se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos. Los concentradores vienen en tres tipos básicos:

**Pasivo:** Un concentrador pasivo sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un concentrador pasivo se utiliza sólo para compartir los medios físicos. En sí, un concentrador pasivo no requiere energía eléctrica.

**Activo:** Se debe conectar un concentrador activo a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.

**Inteligente:** A los concentradores inteligentes a veces se los denomina "smart concentradores". Estos dispositivos básicamente funcionan como concentradores activos, pero también incluyen un chip microprocesador y capacidades diagnósticas. Los concentradores inteligentes son más costosos que los concentradores activos, pero resultan muy útiles en el diagnóstico de fallas. [9]

### **2.1.8 Redes inalámbricas**

Se puede crear una red inalámbrica con mucho menos cableado que el necesario para otras redes. Las señales inalámbricas son ondas electromagnéticas que se desplazan a través del aire. Las redes inalámbricas usan radiofrecuencia (RF), láser, infrarrojo (IR), o satélite/microondas para transportar señales de un computador a otro sin una conexión de cable permanente. El único cableado permanente es el necesario para conectar los puntos de acceso de la red. Las estaciones de trabajo dentro del ámbito de la red inalámbrica se pueden trasladar con facilidad sin tener que conectar y reconectar al cableado de la red. (figura 9).

En el centro de la comunicación inalámbrica están los dispositivos llamados transmisores y receptores. El transmisor convierte los datos fuente en ondas electromagnéticas (EM) que pasan al receptor. El receptor entonces transforma de nuevo estas ondas electromagnéticas en datos para el destinatario. Para una comunicación de dos vías, cada dispositivo requiere de un transmisor y un receptor. Muchos de los fabricantes de dispositivos para networking construyen el transmisor y el receptor en una sola unidad llamada transceptor o tarjeta de red inalámbrica. Todos los dispositivos en las LAN inalámbrica (WLAN) deben tener instalada la tarjeta apropiada de red inalámbrica. Las dos tecnologías inalámbricas más comúnmente usadas para networking son IR y RF. Las estaciones de trabajo y los dispositivos digitales deben estar en la línea de vista del transmisor para operar. Las redes basadas en infrarrojo se acomodan a

entornos donde todos los dispositivos digitales que requieren conectividad de red se encuentran en una habitación. La tecnología IR de networking se puede instalar rápidamente, pero las personas que cruzan la habitación, o el aire húmedo pueden debilitar u obstruir las señales de datos. La tecnología de radiofrecuencia permite que los dispositivos se encuentren en habitaciones o incluso en edificios diferentes. El rango limitado de señales de radio restringe el uso de esta clase de red. La tecnología de RF puede utilizar una o varias frecuencias. Una radiofrecuencia única está sujeta a interferencias externas y a obstrucciones geográficas. Además, una sola frecuencia es fácil de monitorear, lo que hace que la transmisión de datos no sea segura. La técnica del espectro disperso evita el problema de la transmisión insegura de datos porque usa múltiples frecuencias para aumentar la inmunidad al ruido y hace que sea más difícil que intrusos intercepten la transmisión de los datos. En la actualidad se utilizan dos enfoques para implementar el espectro disperso para transmisiones de WLAN. Uno es el espectro disperso por salto de frecuencia (FHSS) y el otro es el espectro disperso de secuencia directa (DSSS). [21]

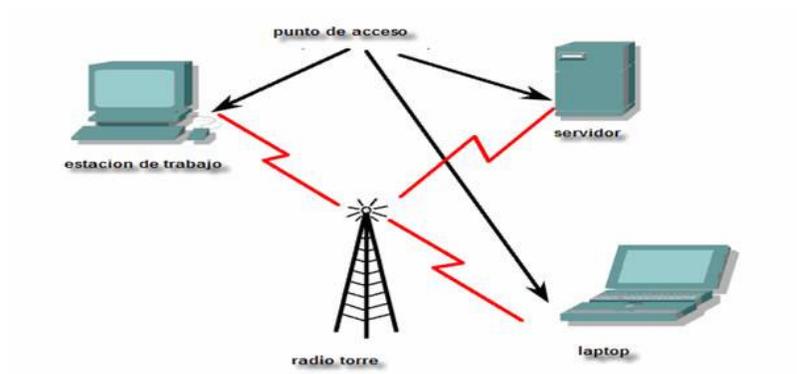


Figura 9 redes inalámbricas

### 2.1.9 Puentes

La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red. Cuando un puente recibe una trama a través de la red, se busca la dirección MAC destino en la tabla de puenteo para determinar si hay que filtrar, inundar, o copiar la trama en otro

segmento. El proceso de decisión tiene lugar de la siguiente forma: Si el dispositivo destino se encuentra en el mismo segmento que la trama, el puente impide que la trama vaya a otros segmentos. Este proceso se conoce como filtrado. Si el dispositivo destino está en un segmento distinto, el puente envía la trama hasta el segmento apropiado. Si el puente desconoce la dirección destino, el puente envía la trama a todos los segmentos excepto aquel en el cual se recibió. Este proceso se conoce como inundación. Si se ubica de forma estratégica, un puente puede mejorar el rendimiento de la red de manera notoria. [22]

#### **2.1.10 Conmutadores**

Un conmutador se describe a veces como un puente multipuerto. El conmutador puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los conmutadores aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los conmutadores utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red. Aunque hay algunas similitudes entre los dos, un conmutador es un dispositivo más sofisticado que un puente. Un conmutador tiene muchos puertos con muchos segmentos de red conectados a ellos. El conmutador elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los conmutadores ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los conmutadores mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda. La conmutación es una tecnología que alivia la congestión en las LAN ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los conmutadores pueden remplazar a los concentradores con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente. Actualmente en la comunicación de

datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. [23]

### **2.1.11 Conectividad del host**

La función de una NIC es conectar un dispositivo host al medio de red. Las NIC se consideran dispositivos Capa 2 porque cada NIC lleva un identificador exclusivo codificado, denominado dirección MAC. Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Posteriormente se suministrarán más detalles acerca de la dirección MAC. Tal como su nombre lo indica, la tarjeta de interfaz de red controla el acceso del host al medio. En algunos casos, el tipo de conector de la NIC no concuerda con el tipo de medios con los que debe conectarse. Un buen ejemplo de ello es el router cisco 2500. En el router, se ve un conector AUI. Ese conector AUI necesita conectarse a un cable ethernet UTP categoría 5 Para hacer esto, se usa un transmisor/receptor, también conocido como transceptor. El transceptor convierte un tipo de señal o conector en otro. [24]

### **2.1.12 Conectividad de par a par**

Los computadores en red actúan como socios en partes iguales, o pares. Como pares, cada computador puede tomar la función de cliente o de servidor. En algún momento, el computador A pedirá un archivo al computador B, el cual responderá entregándole el archivo al computador A. El computador A funciona como cliente, mientras que el B funciona como servidor. Más tarde, los computadores A y B cambiarán de papel. En una red de par a par, los usuarios individuales controlan sus propios recursos. Los usuarios pueden decidir compartir ciertos archivos con otros usuarios. Ya que son los usuarios individuales los que toman estas decisiones, no hay un punto central de control o administración en la red. Además, en caso de fallas, los usuarios individuales deben tener una copia de seguridad de sus sistemas para poder recuperar los datos si estos se pierden. Cuando un computador actúa como servidor, es

posible que el usuario de ese equipo note que el rendimiento es menor, ya que el equipo cumple las peticiones realizadas por otros sistemas. Son relativamente fáciles de instalar y operar. Una red de par a par funciona bien con 10 computadores o menos. [25] (Figura 10).



Figura 10 medio par a par

### 2.1.13 Cliente/servidor

Los servicios de red se ubican en un computador dedicado denominado servidor. El servidor responde a las peticiones de los clientes. El servidor es un computador central que se encuentra disponible de forma continua para responder a las peticiones de los clientes, ya sea de un archivo, impresión, aplicación u otros servicios. La mayoría de los sistemas operativos adoptan la forma de relación cliente/servidor. En general, los computadores de escritorio funcionan como clientes y uno o más computadores con potencia de procesamiento adicional, memoria y software especializado funcionan como servidores. Los servidores están diseñados para cumplir con las peticiones de muchos clientes a la vez. Antes de que un cliente pueda acceder a los recursos del servidor, se debe identificar y obtener la autorización para usar el recurso. Esto se hace asignando a cada cliente un nombre de cuenta y una contraseña que un servicio de autenticación verifica. Con la centralización de las cuentas de los usuarios, de la seguridad, y del control de acceso, las redes basadas en servidores simplifican la administración de grandes redes. [26]

## 2.2 CABLEADO WAN

### 2.2.1 Capa física de las WAN

La implementación de la capa física varía según la distancia que haya entre el equipo y los servicios, la velocidad, y el tipo de servicio en sí. Las conexiones seriales se usan para admitir los servicios WAN tales como líneas dedicadas

arrendadas que usan el PPP o de frame relay La velocidad de estas conexiones va desde los 2400 bits por segundo (bps) hasta el servicio T1 a 1544 Mbps y el servicio E1 a 2048 Mbps. RDSI ofrece conexiones conmutadas por demanda o servicios de respaldo conmutados. (BRI) RDSI está compuesta de dos canales principales de 64 kbps (canales B) para datos, un canal delta (canal D) de 16 kbps que se usa para señalar y para otras tareas de administración del enlace. PPP se utiliza por lo general para transportar datos en los canales B. Con la creciente demanda de servicios residenciales de banda ancha de alta velocidad, las conexiones de DSL y cable módem se están haciendo más populares. Por ejemplo, un servicio DSL residencial puede alcanzar velocidades T1/E1 con la línea telefónica existente. Los servicios de cable utilizan la línea de cable coaxial del televisor. Una línea de cable coaxial provee una conectividad de alta velocidad que iguala o excede aquella de DSL. En un módulo posterior se presentará una explicación detallada de los servicios de DSL y cable módem. [9]

### **2.2.2 Conexiones seriales de WAN**

Para las comunicaciones de larga distancia, las WAN utilizan transmisiones seriales. Este es un proceso por el cual los bits de datos se envían por un solo canal. Este proceso brinda comunicaciones de larga distancia confiables y el uso de un rango específico de frecuencias ópticas o electromagnéticas. Las frecuencias se miden en términos de ciclos por segundo y se expresan en Hercios (Hz). Las señales que se transmiten a través de las líneas telefónicas de grado de voz utilizan 4 (KHz). Para un ruteador, existen dos tipos de conexiones seriales que proveen la conectividad física en las instalaciones del cliente. El primer tipo de conexión serial es el conector de 60 pins. El segundo es un conector más compacto conocido como "smart serial". El conector utilizado por el proveedor varía de acuerdo con el tipo de equipo de servicios. Si la conexión se hace directamente con el proveedor de servicio, o con un dispositivo que provee señal de temporización tal como (CSU/DSU), el ruteador

será un (DTE) y usará cable serial DTE. Sin embargo, hay situaciones en las que se requiere que el ruteador local brinde la temporización y entonces utilizará un cable para equipo de comunicación de datos (DCE). [9]

### 2.2.3 Conexiones seriales del ruteador

Los ruteadores son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Al armar un escenario de ruteadores conectados espalda contra espalda en un ámbito de prueba, uno de los ruteadores debe ser DTE y el otro DCE. Al cablear ruteadores para obtener conectividad serial, los ruteadores tendrán puertos fijos o modulares. El tipo de puerto que se utilice afectará la sintaxis que se use posteriormente para configurar cada interfaz. Las interfaces de los ruteadores que tienen puertos seriales fijos están rotuladas según tipo y número de puerto. Las interfaces de los ruteadores que tienen puertos seriales modulares se rotulan según el tipo de puerto, ranura y número de puerto. (figura 11). [9]

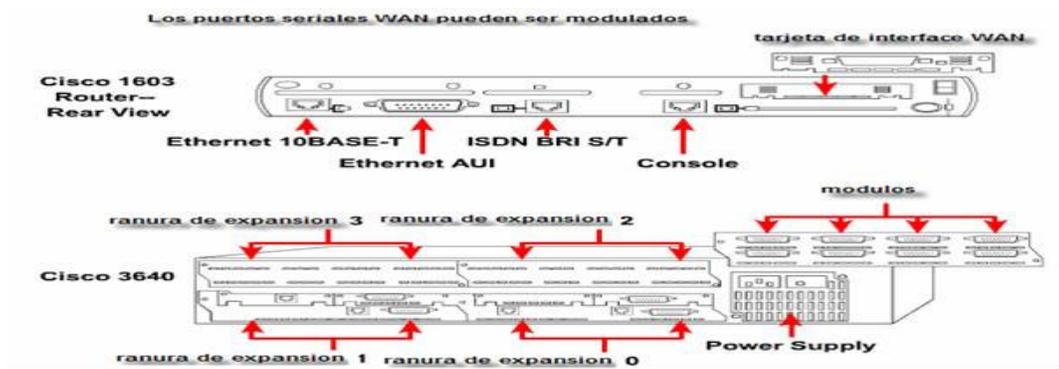


Figura 11 ruteador de cisco 1603 y 3640.

### 2.2.4 Conexiones BRI RDSI y ruteadores

Se pueden utilizar dos tipos de interfaces para BRI RDSI: BRI S/T y BRI U. Un NT1 es un dispositivo intermedio ubicado entre el ruteador y el conmutador del proveedor de servicios RDSI. Se utiliza NT1 para conectar el cableado de cuatro hilos del abonado con el loop local de dos hilos convencional. Puede ser

necesario colocar un NT1 externo si el dispositivo no está integrado al router. Una interfaz BRI con un NT1 integrado tiene el rótulo BRI U mientras que la interfaz BRI sin un NT1 integrado tiene el rótulo BRI S/T. Debido a que los routers pueden tener muchos tipos de interfaz RDSI, es necesario determinar qué tipo de interfaz se necesita al comprar el router. Se puede determinar el tipo de interfaz BRI al mirar el rótulo del puerto. Para interconectar el puerto BRI RDSI al dispositivo del proveedor de servicios, utilice un cable de conexión directa UTP de categoría 5. Es importante que inserte el cable que va desde un puerto BRI RDSI a un jack RDSI o conmutador RDSI solamente. BRI RDSI utiliza voltajes que pueden dañar seriamente los dispositivos que no son de RDSI. [26]

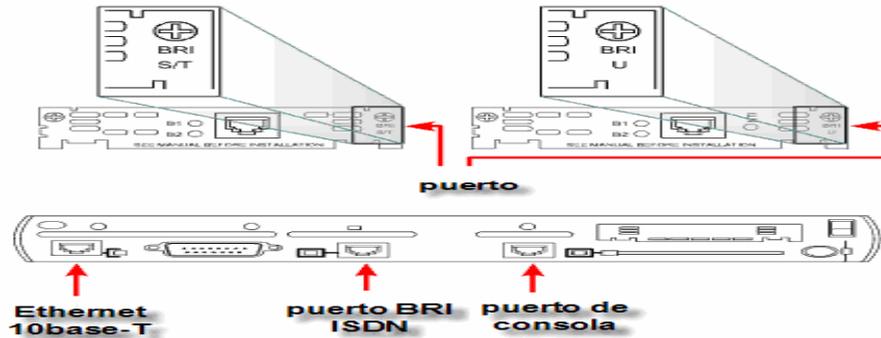


Figura 12 para interconectar el puerto BRI al dispositivo del proveedor del servicio.

### 2.2.5 Conexiones DSL y routers

Para conectar una línea ADSL al puerto ADSL de un router, conecte el cable del teléfono al puerto ADSL en el router y conecte el otro extremo del cable del teléfono al jack telefónico. Para conectar el router y obtener servicio DSL, utilice un cable del teléfono con conectores RJ-11. DSL funciona sobre líneas telefónicas comunes usando los pins 3 y 4 en un conector estándar RJ-11. [27]

### 2.2.6 Conexiones de cable-modem y routers

El router de acceso al cable uBR905 ofrece la posibilidad de tener acceso a una red de alta velocidad a usuarios residenciales, de pequeñas oficinas y de oficinas hogareñas (SOHO) usando el sistema de televisión por cable. El

ruteador uBR905 tiene una interfaz de cable coaxial, o de conector F, que se conecta directamente al sistema de cable. El cable coaxial y el conector F se usan para conectar el ruteador y el sistema de cable. Siga los siguientes pasos:

- Verifique que el ruteador no esté conectado a la alimentación eléctrica.
- Ubique el cable coaxial de RF que sale de la toma de pared para cable coaxial (de TV).
- Instale el divisor de señal/ acoplador direccional, si fuera necesario, para separar las señales para uso del televisor y del computador. Si fuera necesario, también instale un filtro de paso alto para evitar las interferencias entre las señales de TV y del computador.
- Conecte el cable coaxial al conector F del ruteador. Ajuste el conector con los dedos, luego apriétalo dándole un 1/6 de vuelta con una llave.
- Asegúrese de que todos los otros conectores del cable coaxial, todos los divisores intermedios, acopladores, o conexiones a tierra, estén bien ajustados desde la distribución hasta el ruteador uBR905.
- No ajuste el conector excesivamente. [9]

### 2.2.7 Configuración de las conexiones de la consola

El cable que se utiliza entre la terminal y el puerto de consola es el cable transpuesto, con conectores RJ-45. También conocido como cable de consola, tiene una disposición de pins diferente que la de los cables de conexión directa o conexión cruzada RJ-45 usados en ethernet o BRI RDSI. La disposición de pins para un cable transpuesto es la siguiente:

1	a	8
2	a	7
3	a	6
4	a	5
5	a	4
6	a	3
7	a	2
8	a	1

Tabla 2 La disposición de pins para un cable transpuést

### **3. PRINCIPIOS BÁSICOS DE ETHERNET**

#### **3.1 Principios básicos de ethernet**

- 3. 1. 1 Introducción a Ethernet
- 3. 1. 2 Reglas del IEEE para la denominación de Ethernet
- 3. 1. 3 Ethernet y el modelo OSI
- 3. 1. 4 Denominación
- 3. 1. 5 Entramado de la Capa 2
- 3. 1. 6 Estructura de la trama de Ethernet
- 3. 1. 7 Campos de la trama de Ethernet

#### **3.2 Operación de ethernet**

- 3. 2. 1 Control de acceso al medio (MAC)
- 3. 2. 2 Reglas de MAC y detección de la colisión de la retransmisión
- 3. 2. 3 Temporización de Ethernet
- 3. 2. 4 Espacio entre las tramas y postergación
- 3. 2. 5 Manejo de los errores
- 3. 2. 6 Tipos de colisiones
- 3. 2. 7 Errores de Ethernet
- 3. 2. 8 FCS y más allá
- 3. 2. 9 Auto-negociación de Ethernet

### **3 PRINCIPIOS BÁSICOS DE ETHERNET**

#### **3.1 Introducción a ethernet**

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. En 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. El 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. 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 (Km). Este tipo de cable coaxial se conocía como thicknet (red con cable grueso) y tenía el ancho aproximado de un dedo pequeño. 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. Por este motivo, se considera que ethernet es muy escalable. [28]

### **3.1.2 Reglas del IEEE para la denominación de ethernet**

Ethernet no es una tecnología para networking, sino una familia de tecnologías para networking 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. 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 bandabase, 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 se considera ahora obsoleto. 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. El IEEE no puede forzar a los fabricantes de equipamiento para networking a cumplir con todas las particularidades de ningún estándar. IEEE espera que se logre lo siguiente:

- Proporcionar la información de ingeniería necesaria para fabricar dispositivos que cumplan con los estándares de ethernet.
- Promover que los fabricantes introduzcan innovaciones. [29]

### **3.1.3 Ethernet y el modelo OSI**

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física. Para mover datos entre una estación ethernet y otra, a menudo, estos pasan a través de un repetidor. Todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor. Los problemas que se originan en una parte del dominio de colisión generalmente tienen impacto en todo el dominio. Un repetidor es responsable de enviar todo el tráfico al resto de los puertos. El tráfico que el repetidor recibe nunca se envía al puerto por el cual lo recibe. Se enviará toda señal que el repetidor detecte. Si la señal se degrada por atenuación o ruido, el repetidor intenta reconstruirla y regenerarla. Los estándares garantizan un mínimo ancho de banda y operabilidad especificando el máximo número de estaciones por segmento, la longitud máxima del mismo, el máximo número de repetidores entre estaciones, etc. 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 de ethernet 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. 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. [9]

### 3.1.4 Denominación

Para permitir el envío local de las tramas en ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar los computadores 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 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 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. Todos los dispositivos conectados a la LAN de ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, ruteadores y conmutadores. (Figura 13). [30]

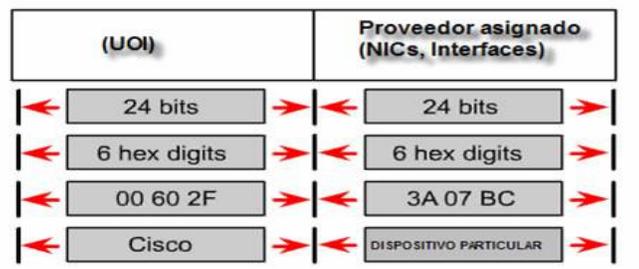


Figura 13 OUI Y proveedor asignado (NICs, Interfaces).

### 3.1.5 Entramado de la capa 2

Los datos en medios físicos, 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 los datos: 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. Se podría utilizar un gráfico de voltaje en función de tiempo para visualizar los bits. Sin embargo, cuando se trabaja con grandes unidades de datos e información de control y direccionamiento, los gráficos de voltaje en función de tiempo pueden volverse excesivamente grandes y confusos. Otro tipo de diagrama que se puede utilizar es el diagrama de formato de trama, que se basa en los gráficos de voltaje en función de tiempo. Estos diagramas se leen de izquierda a derecha, como un gráfico de osciloscopio. Los diagramas de formato de trama muestran distintas agrupaciones de bits (campos), que ejecutan otras funciones. Hay varios tipos distintos de tramas que se describen en diversos estándares. Una trama genérica tiene secciones denominadas campos, y cada campo está formado por bytes. Los campos son:

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

Cuando los computadores se conectan a un medio físico, debe existir alguna forma de informar a los otros computadores cuando están próximos a enviar una trama. Las diversas tecnologías tienen distintas formas para hacerlo, pero todas las tramas, de cualquier tecnología, tienen una secuencia de señalización de inicio de bytes, contienen información de denominación como, por ejemplo, el nombre del computador origen (dirección MAC) y el nombre del computador destino (dirección MAC). 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 el computador 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. 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. El nodo que transmite los datos debe llamar la atención de otros dispositivos para iniciar una trama y para finalizar la trama. El campo de longitud implica el final y se considera que la trama termina después de la FCS. A veces hay una secuencia formal de bytes que se denomina delimitador de fin de trama. (Figura 14). [31]

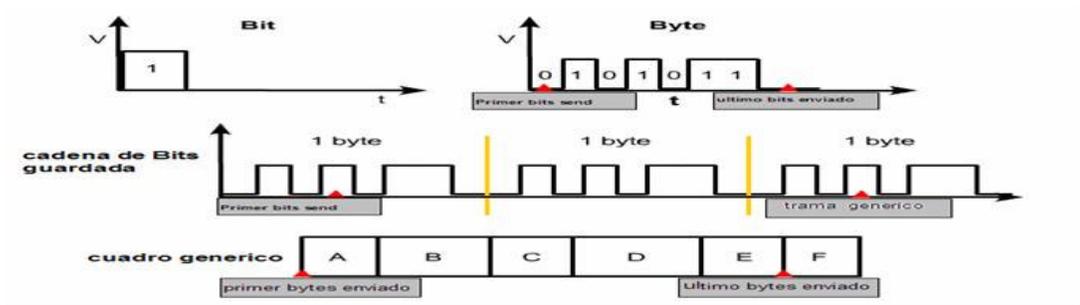


Figura 14 las tres formas principales para calcular el número de secuencia de verificación de trama

### 3.1.6 Estructura de la trama de ethernet

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de ethernet desde 10 Mbps hasta 10000 Mbps. Sin embargo, en la capa física, casi todas las versiones de ethernet son sustancialmente diferentes las unas de las otras, teniendo cada velocidad un juego distinto de reglas de diseño arquitectónico. En la versión de ethernet desarrollada por DIX antes de la adopción de la versión IEEE 802.3 de ethernet, el preámbulo y el delimitador de Inicio de trama (SFD) se combinaron en un solo campo, aunque el patrón binario era idéntico. El campo que se denomina longitud/tipo aparecía como sólo longitud en las primeras versiones de IEEE y sólo como tipo en la versión de DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que el uso que ambos le

daban al campo era común en toda la industria. El campo tipo de la ethernet II se incorporó a la actual definición de trama del 802.3. El nodo receptor debe determinar cuál de los protocolos de capa superior está presente en una trama entrante examinando el campo longitud/tipo. Si el valor de los dos octetos es igual o mayor que el de 0x600 (hexadecimal), 1536 (decimal), entonces el contenido del campo de data es codificado de acuerdo al protocolo indicado. Ethernet II es el formato de trama ethernet utilizado en redes TCP/IP.

### **3.1.7 Campos de la trama de ethernet**

Algunos de los campos que se permiten o requieren en la trama 802.3 de ethernet son:

- Preámbulo
- Delimitador de inicio de trama.
- Dirección destino
- Dirección origen
- Longitud/Tipo
- Datos y relleno
- FCS
- Extensión

El preámbulo es un patrón alternado de unos y ceros que se utiliza para la sincronización de los tiempos en implementaciones de 10 Mbps y menores de ethernet. Las versiones más veloces de ethernet son síncronas y esta información de temporización es redundante pero se retiene por cuestiones de compatibilidad. Un delimitador de Inicio de trama es un campo de un octeto que marca el final de la información de temporización y contiene la secuencia de bits 10101011. El campo de dirección destino contiene la dirección destino MAC. La dirección destino puede ser unicast, multicast o de broadcast. El campo de dirección de origen contiene la dirección MAC de origen. La dirección origen generalmente es la dirección unicast del nodo de transmisión de ethernet. El campo longitud/tipo admite dos usos diferentes. Si el valor es menor a 1536

decimal, 0x600 (hexadecimal), entonces el valor indica la longitud. El valor del tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento de ethernet. La unidad máxima de transmisión (MTU) para ethernet es de 1500 octetos, de modo que los datos no deben superar dicho tamaño. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud. Una FCS contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. La cobertura de la FCS se auto-incluye. [32]

## **3.2 OPERACIÓN DE ETHERNET**

### **3.2.1 Control de acceso al medio (MAC)**

MAC se refiere a los protocolos que determinan cuál de los computadores de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la capa 2 del modelo OSI. Tanto MAC como LLC son subcapas de la capa 2. Hay dos categorías amplias de control de acceso al medio: determinística (por turnos) y la no determinística (el que primero llega, primero se sirve). 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) (fig.15). [9]

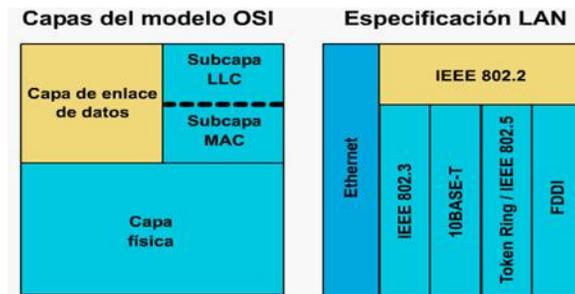


Figura 15 similitudes y diferencias entre las capas 1 y 2 del modelo OSI

### 3.2.2 Reglas de MAC y detección de la colisión/postergación de la retransmisión

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en ethernet ejecuta tres funciones: Transmitir y recibir 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 networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo.

Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar. Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking. Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos. [33]

### **3.2.3 Temporización de ethernet**

Cuando se produce un problema en ethernet, a menudo resulta difícil determinar el origen. Debido a la arquitectura común en bus de ethernet, también descrita como punto único de falla distribuido, el alcance del problema a menudo abarca a todos los dispositivos del dominio de colisión. En los casos en que se utilizan repetidores, esto puede incluir dispositivos separados hasta por cuatro segmentos. 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. 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 de la pila del protocolo. Las versiones de 10 Mbps y más lentas de ethernet son asíncronas. Asíncrona significa que cada estación receptora utiliza los ocho octetos de la información de temporización para sincronizar el circuito receptor con los datos entrantes y luego los descarta. Las implementaciones de 100 Mbps y de mayor velocidad de ethernet son síncronas. Síncrona significa que la información de temporización no es necesaria, sin embargo, por razones de compatibilidad, el preámbulo y la SFD (Delimitador de Inicio de Trama) están presentes. [34]

#### **3.2.4 Espacio entre las tramas 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. Se espera que un repetidor regenere los 64 bits completos de información de temporización, que es el preámbulo y la SFD, al inicio de cualquier trama. [9]

### 3.2.5 Manejo de los errores

El estado de error más común en redes ethernet son las colisiones. Las colisiones son el mecanismo para resolver la contención del acceso a la red. Unas pocas colisiones proporcionan una forma simple y sin problemas, 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 que la impone. Esto se hace de manera que se corrompen por completo los datos transmitidos y todas las estaciones tienen la posibilidad de detectar la colisión. El patrón de datos que se observa con mayor frecuencia para una señal de congestión es 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. 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. (figura 16). [9]

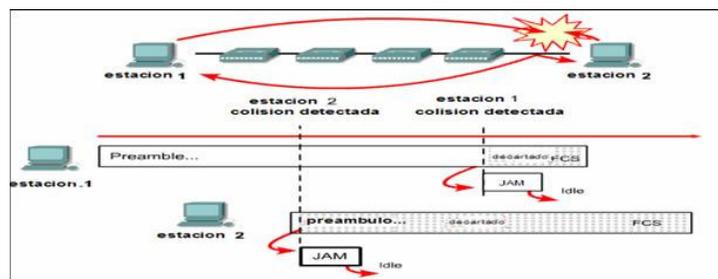


Figura 16 la prueba de longitud mínima como la prueba de la checksum de FCS

### 3.2.6 Tipos de colisiones

Por lo general, las colisiones se producen cuando dos o más estaciones de ethernet transmiten al mismo tiempo dentro de un dominio de colisión. 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, entonces, detectada por todas las estaciones en el segmento local del cable como una colisión. En el cable UTP, como por ejemplo 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. 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. 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. [34]

### 3.2.7 Errores de ethernet

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 concuerdan.

**Fantasma o jabber:** Preámbulo inusualmente largo o evento de congestión. Mientras las colisiones locales o remotas se consideran parte normal de la operación de Ethernet, las colisiones tardías son un error. El estándar 802.3, en varios lugares, define al jabber como una transmisión de al menos 20.000 a 50.000 tiempos de bit de duración. Sin embargo, la mayoría de las herramientas de diagnóstico informan de la presencia de jabber siempre que se detecta una transmisión que excede el tamaño máximo legal de la trama, que es considerablemente menor a 20.000 a 50.000 tiempos de bit. [35]

### 3.2.8 FCS y más allá

Una trama recibida que tiene una secuencia de verificación de trama incorrecta, también conocido como error de CRC o de checksum, 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 corrupción en los controladores 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 concentrador defectuoso o a ruido inducido en el sistema de cables. Un mensaje que no termina en un límite de octeto se conoce como error de alineamiento. Una trama con un valor válido en el campo "longitud" pero que no concuerda con el número real de octetos contabilizados en el campo de datos de la trama recibida recibe el nombre de error de rango. Este error también aparece cuando el valor del campo de longitud es menor que el tamaño mínimo legal fluke networks ha acuñado el término fantasma para referirse a la energía (ruido) que se detecta en el cable y que parece ser una trama, pero que carece de un SFD válido. Para ser considerada fantasma, la trama debe tener una longitud de al menos 72 octetos, incluyendo el preámbulo. De lo contrario, se clasifica como colisión remota. Las mallas a tierra y otros problemas de cableado son normalmente la causa de los fantasmas. [9] (Figura 17).

preambulo	SFD	destinatario	fuelle	tipo de longitud	dato	FCS
7	1	6	6	2	46 to 1500	4

Figura 17 una trama con error de FCS

### 3.2.9 Auto-negociación de ethernet

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 red 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) (ver figura 18), 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. (ver figura 18) [36]



Figura 18. La ráfaga de pulsos FLP está hecha de múltiples en NLP.

### **CAPÍTULO 4 INTRODUCCIÓN A ETHERNET**

#### **4.1 Ethernet de 10Mbps y 100-Mbps**

- 4. 1. 1 Ethernet de 10Mbps
- 4. 1. 2 10BASE5
- 4. 1. 3 10BASE2
- 4. 1. 4 10BASE-T
- 4. 1. 5 Cableado y arquitectura de 10BASE-T
- 4. 1. 6 Ethernet De 100-Mbps
- 4. 1. 7 100-BASE-TX
- 4. 1. 8 100-BASE-FX
- 4. 1. 9 Arquitectura da la fase ethernet

#### **4.2 Ethernet Gigabit y 10-Gigabit**

- 4. 2. 1 ethernet dde 1000-Mbps
- 4. 2. 2 1000BASE-T
- 4. 2. 3 Arquitectura de gigabit ethernet
- 4 . 2 . 4 10-gigabit ethernet
- 4 . 2 . 5 Arquitecturas de 10-gigabit ethernet

## **4.1 ETHERNET DE 10-MBPS Y 100-MBPS**

### **4.1.1 Ethernet de 10-Mbps**

Las ethernet de 10BASE5, 10BASE2 y 10BASE-T se consideran implementaciones antiguas de ethernet. Las cuatro 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 10BASE5, 10BASE2 y 10BASE-T todas comparten los mismos parámetros de temporización. 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"). La SQE es una transmisión del transceptor de respuesta al controlador para indicarle sobre la funciónabilidad de los circuitos de detección de colisiones. La SQE es conocida como "latido de corazón". La señal SQE fue diseñada para corregir el problema en versiones anteriores de ethernet, en las cuales el host desconocía si el transceptor estaba conectado. El SQE siempre se utiliza en half-duplex. Es posible utilizar el SQE en una operación en full-duplex pero no es necesario. La codificación manchester se basa en la dirección de la transición de borde en la mitad de la ventana de temporización para determinar el valor binario para dicho período de bits. 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. [9]

### **4.1.2 10BASE5**

Los sistemas 10BASE5 son económicos y no requieren de configuración, pero componentes básicos tales como las NIC son muy difíciles de encontrar así como el hecho de que es sensible a las reflexiones de señal en el cable. También representan un único punto de falla. Hace uso de la codificación

manchester. Tiene un conductor central sólido. Cada uno de los cinco segmentos máximos de coaxial grueso puede medir hasta 500 m (1640,4 pies) de largo. El cable es grueso, pesado y difícil de instalar. Sin embargo, las limitaciones de distancia eran favorables y esto prolongó su uso en ciertas aplicaciones. Debido a que el medio es un solo cable coaxial, solamente una estación puede transmitir al mismo tiempo, de lo contrario, se produce una colisión. Por lo tanto, 10BASE5 sólo transmite en half-duplex produciendo un máximo de 10 Mbps de transferencia de datos. [9]

#### **4.1.3 10BASE2**

Usa la codificación manchester también. Los computadores en la LAN se conectaban entre sí con una serie de tendidos de cable coaxial sin interrupciones. Se usaban conectores BNC para unir estos tendidos a un conector en forma de T en la NIC. 10BASE2 tiene un conductor central trenzado. Cada uno de los cinco segmentos máximos de cable coaxial delgado puede tener hasta 185 metros de longitud y cada estación se conecta directamente al conector BNC con forma de "T" del cable coaxial. Sólo una estación puede transmitir a la vez, de lo contrario, se produce una colisión. 10BASE2 usa half-duplex. La máxima velocidad de transmisión de 10BASE2 es de 10 Mbps. Puede haber hasta 30 estaciones en cada segmento individual de 10BASE2. De los cinco segmentos consecutivos en serie que se encuentran entre dos estaciones lejanas, sólo tres pueden tener estaciones conectadas. [9]

#### **4.1.4 10BASE-T**

10BASE-T fue introducido en 1990. 10BASE-T utilizaba cable de cobre (UTP) de par trenzado, no blindado de categoría 3 que era más económico y más fácil de usar que el cable coaxial. La explosión de popularidad de ethernet desde mediados hasta fines de los 90 se produjo cuando ethernet comenzó a dominar la tecnología de LAN. 10BASE-T usa la codificación manchester también. Un cable UTP para 10BASE-T tiene un conductor sólido para cada hilo en un cable

horizontal con una longitud máxima de 90 metros. El cable UTP utiliza conectores RJ-45 de ocho pins. Aunque el cable de categoría 3 es apto para uso en redes de 10BASE-T, se recomienda que cualquier nueva instalación de cables se realice con cables de categoría 5e o superior. Los cuatro pares de hilos deberían utilizarse ya sea con la disposición de salida de los pins del cable T568-A o bien la T568-B. Este tipo de instalación de cables admite el uso de protocolos múltiples sin necesidad de volver a cablear. [9]

#### 4.1.5 Cableado y arquitectura de 10BASE-T

Generalmente consisten en una conexión entre la estación y un concentrador o conmutador. Los concentradores son repetidores multipuertos y cuentan en el número límite de repetidores entre las estaciones lejanas. Los concentradores no dividen los segmentos de la red en distintos dominios de colisión. Como los concentradores o repetidores solamente extienden la longitud de una red dentro de un solo dominio de colisión, existe un límite respecto de cuántos concentradores pueden ser utilizados en dicho segmento. Los puentes y los conmutadores dividen un segmento en dominios de colisión individuales, dejando que las limitaciones de los medios determinen la distancia entre los conmutadores. 10BASE-T limita la distancia entre los conmutadores a 100 m (328 pies). Esto contribuye a evitar que se exceda el límite de retardo máximo entre las estaciones lejanas. Cuando se requiera del uso de múltiples concentradores, es recomendable organizarlos de forma jerárquica, para así crear una estructura en forma de árbol. Mejorará el rendimiento si pocos repetidores separan las estaciones. [37] (figura 19).

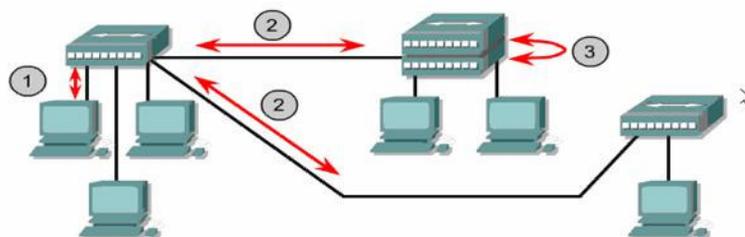


Figura 19 Cableado y Arquitectura de 10BASE-T

#### 4.1.6 Ethernet de 100-Mbps

Ethernet de 100-Mbps también se conoce como fast ethernet (ethernet rápida). Las dos tecnologías que han adquirido relevancia son 100BASE-TX, que es un medio UTP de cobre y 100BASE-FX, que es un medio multimodo de fibra óptica. Tres 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. Tenga en cuenta que 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 responder a estos problemas, ethernet de 100-Mbps utiliza dos distintos pasos de codificación. (Figura 20). [9]

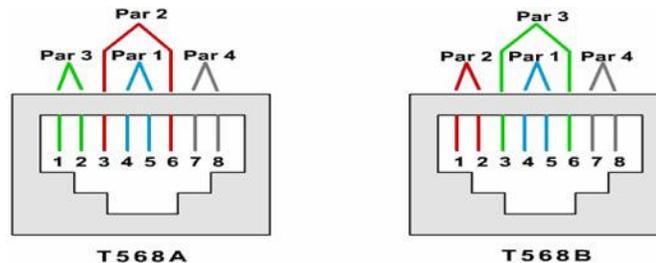


Figura 20 tomacorriente/Conector de telecomunicaciones de par trenzado balanceado de 100 ohms.

#### 4.1.7 100BASE-TX

En 1995, 100BASE-TX con un cable UTP categoría 5 fue el estándar que se convirtió en un éxito comercial. Sin embargo, en 1997, ethernet se expandió para incluir capacidad de full duplex permitiendo que más de un PC transmitiera al mismo tiempo en una red. Cada vez más, los conmutadores reemplazaban los concentradores. Estos conmutadores tenían la capacidad de transmitir en full duplex y de manejar rápidamente las tramas de ethernet. 100BASE-TX usa codificación 4B/5B, que luego es mezclada y convertida a 3 niveles de

transmisión multinivel o MLT-3. 100BASE-TX transporta 100 Mbps de tráfico en modo half-duplex. En modo full-duplex, 100BASE-TX puede intercambiar 200 Mbps de tráfico. [38]

#### **4.1.8 100BASE-FX**

Sin embargo, 100BASE-FX, utiliza la codificación NRZI. La cresta de la onda no presenta ninguna transición, lo cual indica un 0 binario. La segunda forma de la onda muestra una transición en el centro de la ventana de temporización. La transición representa el binario 1. En la tercera forma de onda hay una secuencia binaria alternada. En este ejemplo, resulta más obvio que la ausencia de una transición indica un binario 0 y la presencia de una transición, un binario 1. La transmisión a 200 Mbps es posible debido a las rutas individuales de transmisión (Tx) y recepción (Rx) de fibra óptica de 100BASE-FX. [38]

#### **4.1.9 Arquitectura de la fast ethernet**

Generalmente consisten en una conexión entre la estación y el concentrador. Los concentradores se consideran repetidores multipuerto y los conmutadores, puentes multipuerto. Estos están sujetos a la limitación de 100 m de distancia de los medios UTP. Un repetidor clase 1 puede introducir hasta 140 tiempos de bit de latencia. Todo repetidor que cambie entre una implementación de ethernet y otra es un repetidor clase 1. Un repetidor clase II está restringido a menores retardos, 92 tiempos de bit, debido a que inmediatamente repite la señal entrante al resto de los puertos sin proceso de translación. Para lograr menor latencia, los repetidores clase II deben conectarse a tipos de segmentos que usen la misma técnica de señalización. Tal como sucede con las versiones de 10 Mbps, es posible modificar algunas de las reglas de arquitectura para las versiones de 100 Mbps. Sin embargo, no se permite casi ningún retardo adicional. La modificación de las reglas de arquitectura para 100BASE-TX no es recomendable. El cable para 100BASE-TX entre repetidores clase II no puede superar los 5 metros. [38]

## 4.2 ETHERNET GIGABIT Y 10-GIGABIT

### 4.2.1 Ethernet de 1000-mbps

Los estándares para ethernet de 1000-Mbps o gigabit ethernet representan la transmisión a través de medios ópticos y de cobre. El estándar para 1000BASE-X, IEEE 802.3z, especifica una conexión full duplex de 1 Gbps en fibra óptica. El estándar para 1000BASE-T, IEEE 802.3ab, especifica el uso de cable de cobre balanceado de categoría 5, o menor. Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización, Utilizan 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. La transmisión de datos se realiza de manera más eficiente utilizando códigos para representar el corriente binario 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. Los símbolos 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 del concepto 4B/5B. (Figura 21). [38]



Figura 21 subcapa de control de enlace lógica

### 4.2.2 1000BASE-T

Al instalar fast ethernet para aumentar el ancho de banda de las estaciones de trabajo, se comenzaron a crear cuellos de botella corriente arriba en la red. 1000BASE-T (IEEE 802.3ab) se desarrolló para proporcionar ancho de banda adicional a fin de ayudar a aliviar estos cuellos de botella. Proporcionó mayor desempeño a dispositivos tales como s dentro de los edificios, enlaces entre los conmutadores, servidores centrales y otras aplicaciones de armarios para cableado así como conexiones para estaciones de trabajo de nivel superior. Fast ethernet se diseñó para funcionar en los cables de cobre cat 5 existentes y esto requirió que dicho cable aprobara la verificación de la cat 5e. Uno de los atributos más importantes del estándar para 1000BASE-T es que es interoperable con 10BASE-T y 100BASE-TX. Como el cable cat 5e puede transportar, de forma confiable, hasta 125 Mbps de tráfico, obtener 1000 Mbps (gigabit) de ancho de banda fue un desafío de diseño. El primer paso para lograr una 1000BASE-T es utilizar los cuatro pares de hilos en lugar de los dos pares tradicionales utilizados para 10BASE-T y 100BASE-TX. Esto se logra mediante un sistema de circuitos complejo que permite las transmisiones full duplex en el mismo par de hilos. Esto proporciona 250 Mbps por par. Con los cuatro pares de hilos, proporciona los 1000 Mbps esperados. Como la información viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor. La codificación de 1000BASE-T con la codificación de línea 4D-PAM5 se utiliza en UTP de cat 5e o superior. Esto significa que la transmisión y recepción de los datos se produce en ambas direcciones en el mismo hilo a la vez. Como es de esperar, esto provoca una colisión permanente en los pares de hilos. Estas colisiones generan patrones de voltaje complejos. Mediante los complejos circuitos integrados que usan técnicas tales como la cancelación de eco, la corrección del error de envío capa 1 (FEC) y una prudente selección de los niveles de voltaje, el sistema logra una tasa de transferencia de 1 gigabit. En los períodos de inactividad, son nueve los niveles de voltaje que se encuentran

en el cable y durante los períodos de transmisión de datos son 17. Con este gran número de estados y con los efectos del ruido, la señal en el cable parece más analógica que digital. Como en el caso del analógico, el sistema es más susceptible al ruido debido a los problemas de cable y terminación. Los datos que provienen de la estación transmisora se dividen cuidadosamente en cuatro corrientes paralelas; luego se codifican, se transmiten y se detectan en paralelo y finalmente se reensamblan en una sola corriente de bits recibida. [38]

#### **4.2.3 Arquitectura de gigabit ethernet**

Las limitaciones de distancia de los enlaces full-duplex están restringidas sólo por el medio y no por el retardo de ida y vuelta. Como la mayor parte de gigabit ethernet está conmutada, Las topologías de cadena de margaritas, de estrella y de estrella extendida están todas permitidas. El problema entonces yace en la topología lógica y el flujo de datos y no en las limitaciones de temporización o distancia. Un cable UTP de 1000BASE-T es igual que un cable de una 10BASE-T o 100BASE-TX, excepto que el rendimiento del enlace debe cumplir con los requisitos de mayor calidad de ISO Clase D (2000) o de la categoría 5e. No es recomendable modificar las reglas de arquitectura de 1000BASE-T. A los 100 metros, 1000BASE-T opera cerca del límite de la capacidad de su hardware para recuperar la señal transmitida. Cualquier problema de cableado o de ruido ambiental podría dejar un cable, que en los demás aspectos cumple con los estándares, inoperable inclusive a distancias que se encuentran dentro de la especificación. Se recomienda que todos los enlaces existentes entre una estación y un concentrador o conmutador estén configurados para auto-negociación para así permitir el mayor rendimiento conjunto. [39]

#### **4.2.4 10-Gigabit ethernet**

Se adaptó el IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. Las similitudes básicas entre 802.3ae y 802.3, ethernet original son notables. Esta ethernet de 10-Gigabit (10GbE) está evolucionando

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 red existente. Un importante cambio conceptual en ethernet surge con 10GbE. 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. 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. Es posible que 10GbE compita con la ATM en ciertas aplicaciones.

En resumen, ¿cómo se compara 10GbE con otras variedades de Ethernet? El formato de trama es el mismo, permitiendo así la interoperabilidad entre todos los tipos de tecnologías antiguas, fast, gigabit y 10 gigabit, sin retramado o conversiones de protocolo. El tiempo de bit es ahora de 0,1 nanosegundos. Todas las demás variables de tiempo caen en su correspondiente lugar en la escala. Como sólo se utilizan conexiones de fibra en full-duplex, el CSMA/CD no es necesario. Las subcapas de IEEE 802.3 dentro de las capas OSI 1 y 2 se preservan en su mayoría, con pocos agregados para dar lugar a enlaces en fibra de 40 Km. e interoperabilidad con las tecnologías SONET/SDH. Entonces, es posible crear redes de ethernet flexibles, eficientes, confiables, a un costo de punta a punta relativamente bajo. El TCP/IP puede correr en redes LAN, MAN y WAN con un método de transporte de capa 2. El estándar básico que rige el CSMA/CD es IEEE 802.3. Un suplemento al IEEE 802.3, titulado 802.3ae, rige la familia de las 10GbE. Como es típico para las nuevas tecnologías, se están considerando una variedad de 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 multiplexación 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. [40]

#### 4.2.5 Arquitecturas de 10-gigabit ethernet

Cada bit de datos dura 0,1 nanosegundos. Esto significa que habría 1000 bits de datos en GbE en el mismo tiempo de bit que un bit de datos en una corriente de datos en ethernet de 10-Mbps. Las transmisiones de datos en 10 GbE dependen de la temporización exacta de bit para separar los datos de los efectos del ruido en la capa física. Este es el propósito de la sincronización. Corrientes complejas de bits en serie se utilizan para todas las versiones de 10GbE excepto en 10GBASE-LX4, que utiliza la amplia multiplexión por división de longitud de Onda (WWDM) para multiplexar corrientes de datos simultáneas de cuatro bits en cuatro longitudes de onda de luz lanzada a la fibra a la vez. En la actualidad, la mayoría de los productos de 10GbE tienen forma de módulos, o tarjetas de línea, para agregar a los conmutadores y a los ruteadores de nivel superior. Una creciente variedad de componentes para la transmisión de señales. A medida que evolucionen las tecnologías ópticas, se incorporarán mejores transmisores y receptores a estos productos, tomando ventaja adicional de la modularidad. 10GbE utilizan medios de fibra óptica. Los tipos de fibra incluyen fibra monomodo de 10 $\mu$  y fibras multimodo de 50 $\mu$  y 62.5 $\mu$ . Admiten un rango de características de dispersión y de atenuación de la fibra, pero limitan las distancias de operación. [40]

### **5 CONMUTACIÓN DE ETHERNET**

#### **5.1 CONMUTACIÓN DE ETHERNET**

- 5.1.1 Punteo de Capa 2
- 5.1.2 Conmutación a nivel de Capa 2
- 5.1.3 Operación de conmutadores
- 5.1.4 Latencia
- 5.1.5 Modos de conmutación

#### **5.2 Dominios de colisión y de broadcast**

- 5.2.1 Entorno de medios compartidos
- 5.2.2 Dominios de colisión
- 5.2.3 Segmentación
- 5.2.4 Broadcasts de capa 2
- 5.2.5 Dominios de broadcast

## 5.1 CONMUTACIÓN DE ETHERNET

### 5.1.1 Puenteo de capa 2

A medida que se agregan más nodos al segmento físico de ethernet, aumenta la contención de los medios. Ethernet es un medio compartido, lo que significa que sólo un nodo puede transmitir datos a la vez. Al agregar más nodos, se aumenta la demanda sobre el ancho de banda disponible y se impone una carga adicional sobre los medios. Cuando aumenta el número de nodos en un solo segmento, aumenta la probabilidad de que haya colisiones, y esto causa más retransmisiones. Una solución al problema es dividir un segmento grande en partes y separarlo en dominios de colisión aislados. Para lograr esto, un puente guarda una tabla de direcciones MAC y sus puertos asociados. El puente luego envía o descarta tramas basándose en las entradas de su tabla. Los pasos siguientes ilustran el modo de operación de un puente: El host A está haciendo ping hacia el host B. Como los datos se transmiten por todo el segmento del dominio de colisión, tanto el puente como el host B procesan el paquete. El puente agrega la dirección origen de la trama a su tabla de puenteo. Como la dirección se encontraba en el campo de dirección origen y se recibió la trama en el puerto 1, la trama debe estar asociada con el puerto 1 de la tabla. La dirección de destino de la trama se compara con la tabla de puenteo. Ya que la dirección no se encuentra en la tabla, aunque está en el mismo dominio de colisión, la trama se envía a otro segmento. La dirección del host B no se registró aún ya que sólo se registra la dirección origen de una trama. El host B procesa la petición del ping y transmite una respuesta ping de nuevo al host A. El dato se transmite a lo largo de todo el dominio de colisión. Tanto el host A como el puente reciben la trama y la procesan. El puente agrega la dirección origen de la trama a su tabla de puenteo. Debido a que la dirección de origen no estaba en la tabla de puenteo y se recibió en el puerto 1, la dirección origen de la trama debe estar asociada con el puerto 1 de la tabla. La dirección de destino de la trama se compara con la tabla de puenteo para verificar si su entrada está allí. Debido a que la dirección se encuentra en la tabla, se verifica la asignación

del puerto. La dirección del host A está asociada con el puente por el que la trama llegó, entonces la trama no se envía. El host A ahora va a hacer ping hacia el host C. Ya que los datos se transmiten en todo el segmento del dominio de colisión, tanto el puente como el host B procesan la trama. El host B descarta la trama porque no era el destino establecido. El puente agrega la dirección origen de la trama a su tabla de puenteo. Debido a que la dirección ya estaba registrada en la tabla de puenteo, simplemente se renueva. La dirección de destino de la trama se compara con la tabla de puenteo para verificar si su entrada está allí. Debido a que la dirección no se encuentra en la tabla, se envía la trama a otro segmento. La dirección del host C no se registró aún, ya que sólo se registra la dirección origen de una trama. El host C procesa la petición del ping y transmite una respuesta ping de nuevo al host A. El dato se transmite a lo largo de todo el dominio de colisión. Tanto el host D como el puente reciben la trama y la procesan. El host D descarta la trama porque no era el destino establecido. El puente agrega la dirección origen de la trama a su tabla de puenteo. Ya que la dirección se encontraba en el campo de dirección origen y la trama se recibió en el puerto 2, la trama debe estar asociada con el puerto 2 de la tabla. La dirección destino de la trama se compara con la tabla de puenteo para verificar si su entrada está allí. La dirección se encuentra en la tabla pero está asociada con el puerto 1, entonces la trama se envía al otro segmento. Cuando el Host D transmite datos, su dirección MAC también se registrará en la tabla de puenteo. Esta es la manera en que el puente controla el tráfico entre los dominios de colisión. (Figura 22). [9]

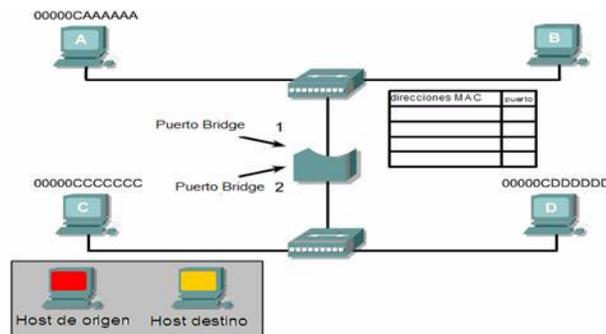


Figura 22 Esta es la manera en que el puente controla el tráfico entre los dominios de colisión.

### 5.1.2 Conmutación a nivel de capa 2

Por lo general, un puente sólo tiene dos puertos y divide un dominio de colisión en dos partes. Todas las decisiones que toma el puente se basan en un direccionamiento MAC o de Capa 2 y no afectan el direccionamiento lógico o de capa 3. Así, un puente dividirá el dominio de colisión pero no tiene efecto sobre el dominio lógico o de broadcast. No importa cuántos puentes haya en la red, a menos que haya un dispositivo como por ejemplo un ruteador que funciona en el direccionamiento de capa 3, toda la red compartirá el mismo espacio de dirección lógica de broadcast. Un puente creará más dominios de colisión pero no agregará dominios de broadcast. Un conmutador es básicamente un puente rápido multipuerto, que puede contener docenas de puertos. En vez de crear dos dominios de colisión, cada puerto crea su propio dominio de colisión. En una red de veinte nodos, existen veinte dominios de colisión si cada nodo está conectado a su propio puerto de conmutador. Si se incluye un puerto uplink, un conmutador crea veintiún dominios de colisión de un solo nodo. Un conmutador crea y mantiene de forma dinámica una tabla de memoria de contenido direccionable (CAM), que contiene toda la información MAC necesaria para cada puerto. (Figura 23) [41]

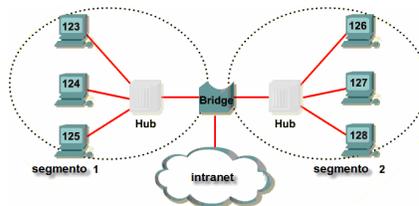


Figura 23 broadcast de dominio

### 5.1.3 Operación de conmutadores

Cuando sólo un nodo está conectado a un puerto de conmutador, el dominio de colisión en el medio compartido contiene sólo dos nodos. Los dos nodos en este segmento pequeño, o dominio de colisión, constan del puerto de conmutador y el host conectado a él. Estos segmentos físicos pequeños son llamados microsegmentos. Otra capacidad emerge cuando sólo dos nodos se

conectan. En una red que utiliza cableado de par trenzado, un par se usa para llevar la señal transmitida de un nodo al otro. Un par diferente se usa para la señal de retorno o recibida. Es posible que las señales pasen a través de ambos pares de forma simultánea. La mayoría de los conmutadores son capaces de admitir full duplex, como también lo son las NIC. En el modo full duplex, no existe contención para los medios. Así, un dominio de colisión ya no existe. En teoría, el ancho de banda se duplica cuando se usa full duplex. Un circuito integrado de aplicación específica (ASIC) es un dispositivo formado de compuertas lógicas no dedicadas que pueden programarse para realizar funciones a velocidades lógicas. Las operaciones que antes se llevaban a cabo en software ahora pueden hacerse en hardware usando ASIC. El uso de estas tecnologías redujo enormemente los retardos causados por el procesamiento del software y permitió que un conmutador pueda mantenerse al ritmo de la demanda de los datos de muchos microsegmentos y velocidades de bits altas. [42]

#### **5.1.4 Latencia**

La latencia es el retardo que se produce 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. Existe una gran variedad de 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. [43]

### 5.1.5 Modos de conmutación

Se conmuta una trama a su puerto de destino es una compensación entre la latencia y la confiabilidad. Un conmutador puede comenzar a transferir 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 conmutador. Sin embargo, no se puede verificar la existencia de errores. En el otro extremo, el conmutador puede recibir toda la trama antes de enviarla al puerto destino. Si se descubre que la trama es inválida, se descarta en este conmutador en vez de hacerlo en el destino final. Al usar conmutación por métodos de corte, tanto el puerto origen como el destino deben operar a la misma velocidad de bit para mantener intacta la trama. Esto se denomina conmutación síncrona. 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. En la conmutación asimétrica se debe usar el método de almacenamiento y envío. 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. [9]

## 5.2 DOMINIOS DE COLISIÓN Y DE BROADCAST

### 5.2.1 Entorno de medios compartidos

Comprender los dominios de colisión requiere de la comprensión de lo que son las colisiones y cómo se originan. Algunas redes se conectan directamente y todos los hosts comparten la capa 1. Algunos ejemplos:

**Entorno de medios compartidos:** Ocurre cuando varios hosts tienen acceso al mismo medio. Por ejemplo, si varios PC 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 networking 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 hogareño. Se trata de un entorno de networking compartido en el que un dispositivo se conecta a un dispositivo solamente, como por ejemplo un computador al proveedor de servicios de Internet por cable módem y línea telefónica. 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. (ver figura 24) [45]

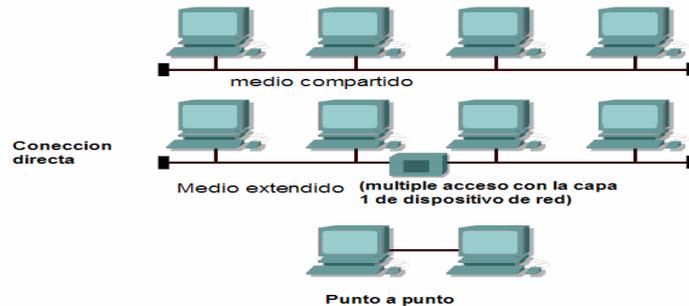


Figura 24 medio compartido, medio extendido, punto a punto.

### 5.2.2 Dominios de colisión

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. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de 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, tales como los repetidores y concentradores, tienen la función primaria de extender los segmentos de cable de ethernet. Al extender la red se pueden agregar más hosts, 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. El resultado final es el deterioro del rendimiento de la red, que será mayor si todos los computadores en esa red exigen anchos de banda elevados. En fin, 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. La regla de los cuatro repetidores en ethernet establece que no puede haber más de cuatro repetidores o concentradores repetidores entre dos computadores 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, 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 notablemente. Una colisión tardía es una colisión que se produce después de la transmisión de los primeros 64 bytes de la trama. 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 deteriora el rendimiento de la red. La regla 5-4-3-2-1 requiere que se cumpla con las siguientes pautas:

- Cinco segmentos de medios de red.
- Cuatro repetidores o concentradores
- Tres segmentos de host de red

- Dos secciones de enlace (sin hosts)
- Un dominio de colisión grande. ver (figura 25).

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.  
[45]

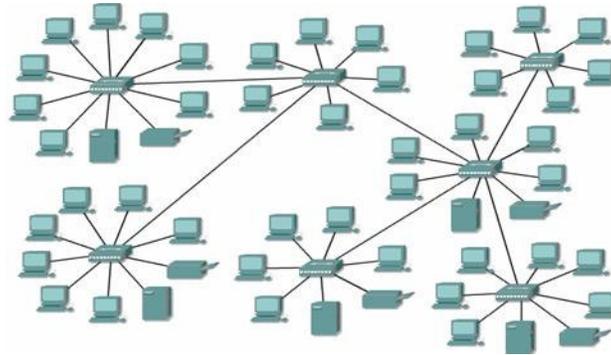


Figura 25 La regla 5-4-3-2-1

### 5.2.3 Segmentación

En realidad, el protocolo de ethernet se basa en el protocolo aloha. Una habilidad importante de todo profesional de networking, es la capacidad de reconocer los dominios de colisión. Conectar varios computadores a un solo medio de acceso compartido que no tiene ningún otro dispositivo de networking conectado, crea un dominio de colisión. Esta situación limita el número de computadores que pueden utilizar el medio, también llamado segmento. Los dispositivos de capa 1 amplían pero no controlan los dominios de colisión. 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 y conmutadores, 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 conmutadores, 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. Cuanto 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 desacelerar 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 en una red produce el efecto de dividir los dominios de colisión en dominios menores. Los dispositivos de capa 3 tienen más funciones que sólo las de dividir los dominios de colisión. Los dispositivos de capa 3 y sus funciones se tratarán con mayor profundidad en la sección sobre dominios de broadcast. [46]

#### **5.2.4 Broadcasts de capa 2**

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 de cada host. Los dispositivos de capa 2 deben inundar todo el tráfico de broadcast y multicast. La 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. Como se ve en los resultados, los broadcasts que inundan la red efectivamente pueden desconectar una estación de trabajo IP. Aunque parezca extremo, durante las tormentas de broadcast, se han observado picos de miles de broadcasts por segundo. Pruebas en un entorno controlado con una variedad de broadcasts y multicasts de la red mostraron una degradación del sistema mensurable a tan sólo 100 broadcasts o multicasts por segundo. La mayoría de las veces, el host no se beneficia al procesar el broadcast, ya que no es el destino buscado. Los niveles elevados de radiación de broadcast pueden degradar el rendimiento del host de manera considerable. Las tres fuentes de broadcasts y multicasts en las redes IP son las estaciones de trabajo, los ruteadores y las aplicaciones multicast. Las estaciones de trabajo envían en broadcast una petición de protocolo de resolución de direcciones (ARP) cada vez que necesitan ubicar una dirección MAC que no se encuentra en la tabla ARP. 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. Eso significa que 2000 estaciones terminales IP producen cerca de 14 ARP por segundo. Los protocolos de enrutamiento que están configurados en la red pueden aumentar el tráfico de broadcast de modo significativo. [47]

### **5.2.5 Dominios 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 posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, 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. En otras palabras, 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 ruteadores no envían broadcasts. Los ruteadores, en realidad, funcionan en las capas 1, 2 y 3. Ellos, al igual que los dispositivos de capa 1, poseen una conexión física y transmiten datos a los medios. Ellos 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 ruteador segmente dominios de broadcast. Para que un paquete sea enviado a través del ruteador, el dispositivo de capa 2 debe ya 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.

[47]

### **6.1 ETHERNET DE 100Mbps, TECNOLOGÍAS COMPETITIVAS Y REDES INALÁMBRICAS 802.11**

#### **6.1. Evolución de ethernet**

- 6.1.2 Tecnología.
- 6.1.3 Aplicaciones y productos.
- 6.1.4 Tecnologías competitivas
- 6.1.5 Ethernet en el futuro
- 6.1.6 Packet bursting

#### **6.2 REDES INALÁMBRICAS 802.11**

- 6.2.1 Wi-Fi
- 6.2.2 Funcionamiento de Internet Turbo Wi-Fi
- 6.2.3 Las redes inalámbricas o WN
- 6.2.4 Redes inalámbricas de consumo
- 6.2.5 Clasificación de las redes inalámbricas - Redes inalámbricas personales
- 6.2.6 Velocidad vs Modulación
- 6.2.7 Topología y Modos de funcionamiento de los dispositivos

## **6 ETHERNET DE 10 MBPS, TECNOLOGÍAS COMPETITIVAS Y REDES INALÁMBRICAS 802.11**

### **6.1 Evolución de ethernet**

Ethernet ha evolucionado desde las primeras tecnologías, a las tecnologías fast, a las de gigabit y a las de multigigabit. Aunque otras tecnologías LAN todavía están instaladas (instalaciones antiguas), ethernet domina las nuevas instalaciones de LAN. A tal punto que algunos llaman a ethernet el "tono de marcación" de la LAN. ethernet ha llegado a ser el estándar para las conexiones horizontales, verticales y entre edificios. Las versiones de ethernet actualmente en desarrollo están borrando la diferencia entre las redes LAN, MAN y WAN. Mientras que ethernet de 1 gigabit es muy fácil de hallar en el mercado, y cada vez es más fácil conseguir los productos de 10 gigabits, el IEEE y la alianza de ethernet de 10 gigabits se encuentran trabajando en estándares para 40, 100 e inclusive 160 Gbps. Las tecnologías que se adopten dependerán de un número de factores que incluyen la velocidad de maduración de las tecnologías y de los estándares, la velocidad de adopción por parte del mercado y el costo. El futuro de los medios para networking tiene tres ramas:

- Cobre (hasta 1000 Mbps, tal vez más)
- Inalámbrico (se aproxima a los 100 Mbps, tal vez más)
- Fibra óptica (en la actualidad a una velocidad de 10.000 Mbps y pronto superior)

Los medios de cobre e inalámbricos presentan ciertas limitaciones físicas y prácticas en cuanto a la frecuencia más alta con la se pueda transmitir una señal. Este no es un factor limitante para la fibra óptica en un futuro predecible. Las limitaciones de ancho de banda en la fibra óptica son extremadamente amplias y todavía no están amenazadas. En los sistemas de fibra, son la tecnología electrónica (por ejemplo los emisores y los detectores) y los procesos de fabricación de la fibra los que más limitan la velocidad. Los adelantos futuros de ethernet probablemente estén dirigidos hacia las fuentes de luz láser y a la fibra óptica monomodo. [48]

### 6.1.2 Tecnología

La primera propuesta, en 1992, por parte del comité IEEE 802.3, responsable de las especificaciones de las redes ethernet, intentó la normalización de una normativa para ethernet de 100 Mbps. Sin embargo, no se llegó a su aprobación, dado que diversos grupos de fabricantes apostaban por diversas soluciones, intentando así forzar la introducción de sus propios productos en el mercado. Básicamente se proponían cuatro soluciones:

**Grand Junction Networks** proponía el uso de las redes actuales, con un esquema de señalización similar al de las redes FDDI de par trenzado, cuya seguridad para la transmisión de datos a 100 Mbps. esta totalmente probado. Es lo que se ha denominado 100BaseX o fast ethernet. Su mayor ventaja es que es totalmente compatible con las redes actuales, dado que sigue utilizando el mismo sistema de control de acceso al medio (MAC), al mismo tiempo que puede seguir usando los mismos cables de par trenzado. Dado que este esquema MAC es totalmente independiente de la velocidad, ello permite la coexistencia de trafico a 1, 10, 100 Mbps. u otras velocidades en la misma red, mediante el uso de puentes (puentes) o tarjetas adaptadoras de dos velocidades, y por tanto la migración de 10 a 100 Mbps. con los menores costes posibles. Otra ventaja es que, dado que la subcapa ANSI X3T9.5 (FDDI PMD) empleada en 100BaseX, soporta diversos tipos de cableado (UTP, STP, fibra), ello implica que 100BaseX puede adaptarse también a una gran variedad de situaciones de cableado ya instalado. Otra gran ventaja de esta tecnología, es que, al usar la capa ANSI PMD de FDDI, sin cambios, ya existen en el mercado muchos circuitos integrados que la implementan, y ello conlleva un período de desarrollo y de implementación de los productos 100BaseX, sensiblemente inferior al de otras propuestas.

**AT&T** y **HP** diseñaron una nueva topología, que reemplazaría el sistema CSMA/CD por otro denominado ("Demand Priority Protocol") (DPP o protocolo

de solicitud de demanda), y que se denominó 100BaseVG. Su objetivo primordial era mantener la compatibilidad con los cableados UTP de categoría 3, al mismo tiempo que se lograban los 100 Mbps. Para ello, la única solución viable consistía en incrementar el número de pares empleados para repartir el ancho de banda. Dado que los cableados UTP empleados en las redes 10BaseT actuales disponen de 4 pares, de los cuales actualmente sólo se emplean dos (transmisión y recepción), se propuso la división del ancho de banda entre los 4 pares, de modo que por cada uno de ellos circularan datos a 25 Mbps. La transmisión de 25 Mbps. en cada par, en lugar de los 10 Mbps. En las redes 10BaseT cada nodo tiene que "escuchar" en la red al mismo tiempo que transmite los paquetes de datos, y por ello requieren pares dedicados a cada función. Las redes 100BaseVG liberan a los nodos de esta función, y la centralizan en el concentrador. Con ello, los nodos pueden utilizar el mismo par (cada uno de los cuatro pares disponibles), para ambas funciones: transmisión y recepción de datos. Además, el concentrador gestiona la prioridad de acceso a la red por parte de los nodos, en función del tipo de datos. IBM y HP añadieron modificaciones que permitían el uso de esta red como "fast token ring", manteniendo cierta compatibilidad con las redes token ring actuales, por lo que a partir de ese momento se denominó 100VG-AnyLAN.

**LANMedia** proponía una variante de 100BaseX, con un esquema de señalización denominado LMC. Por el momento, no parece que tenga muchas posibilidades de éxito.

**Kalpana** y otras empresas diseñaban la cuarta proposición; era un paso relativamente sencillo desde las redes actuales: multiplicaba por dos el ancho de banda ethernet, utilizando dos canales ethernet actuales, logrando así un ancho de banda de 20 Mbps. Es lo que se denomina ethernet full duplex (FDE). Es relativamente fácil de entender: en las redes ethernet actuales, los datos que viajan desde una estación de trabajo (cliente), hasta el servidor, y los datos que

vian en sentido contrario (desde el servidor al cliente), comparten el mismo cable, y por tanto, sólo puede haber tráfico en un sentido en un momento dado. Si permitimos que, por ejemplo, desde un concentrador, hasta el servidor de la red, el ancho de banda sea de 20 Mbps., a través de una tarjeta de red ethernet full duplex (o dos ethernet estándar, con un software adecuado), ello implicaría, sin duda, una gran optimización de los recursos que el servidor es capaz de ofrecer a la red. En Julio de 1993, el comité IEEE 802.0, decidió la creación de dos nuevos grupos de trabajo para la definición de las nuevas "ethernet". El primer grupo, denominado 802.12, se encargará de las redes 100Base-VG, mientras que el segundo, 802.13 u 802.14 [48]

Sin embargo, hay otro tipo de productos que también nos permiten, incluso con redes ethernet estándar (10 Mbps.), incrementar la "velocidad" real del flujo de tráfico en la red. Se trata de los conmutadores básicamente se trata de una forma de bridge o puente. Con ello logramos incrementar las posibilidades de que varios nodos transmitan y reciban datos simultáneamente, siempre y cuando estén situadas en diferentes segmentos de una misma red. Otros emplean una técnica conocida como "store and forward", por medio de la cual examinan el paquete completo, y lo filtran o transmiten, siendo más efectivos y manejables, ya que nos permiten funciones como spanning tree, filtrado en función de protocolo o dirección (destino o fuente) o de parámetros definidos por el usuario. Es decir, son auténticos puentes, y como tales, son capaces de desempeñar idénticas funciones. Por lo general incorporan gestión remota SNMP y otras características adicionales importantes para el adecuado control y administración de la red. La velocidad de filtrado y transmisión de paquetes es muy importante, ya que nos indica el retraso que ocasionan al recibir el paquete de la red, almacenarlo en su memoria interna, analizarlo y filtrarlo o transmitirlo, según el caso. [48]

### **6.1.3 Aplicaciones y productos**

Lo más interesante que podemos deducir es que los conmutadores y las redes ethernet rápidas, son totalmente complementarias: La elección de una u otra, o ambas posibilidades, depende en gran medida de cada situación. En una red con un sólo servidor, en la que los nodos cliente sólo comunican con el servidor y no entre sí, no se requiere un conmutadores, sino mayor ancho de banda. Y por último, cuando existen varios servidores, varios grupos de trabajo, y el tráfico es grande, puede ser conveniente el uso de ambas tecnologías. Claro estás, normas genéricas, y cada caso es único, como hemos indicado antes. De hecho, hay productos como concentradores, con capacidad de conmutación (caso de las redes 100BaseVG). E incluso se ofrecen productos con puertos de 10 Mbps. para los clientes, y enlaces de 20 o 100 Mbps. con el servidor, de modo que varios clientes pueden comunicar entre sí simultáneamente y con el servidor, y a este le puede llegar tráfico simultáneo de varios clientes. Algunas de las empresas que ya comercializan productos cumpliendo con las tecnologías que hemos citado son: grand junction, HP, IBM, interphase, kalpana, lannet, lantronix, y sun. [48]

### **6.1.4 Tecnologías competitivas**

Obviamente, existen tecnologías, algunas de las cuales ya hemos explicado en artículos precedentes, como FDDI/CDDI, u otros como ATM, que pueden, perfectamente, competir con los diversos tipos de "ethernet rápidas". El inconveniente, por lo general, es su costo más elevado, por nodo de la red, e incluso, la complejidad en su instalación y gestión. Por otro lado, es probable que coexistan, si no todos, la mayoría de los sistemas o tecnologías de redes ethernet rápidas, especialmente si tenemos en cuenta que ya hoy, cuando todavía no han sido normalizadas, existen productos 100BaseX, 100BaseVG y FDE. Se trata de un mercado lo suficientemente grande, y en continuo crecimiento como para permitirlo e incluso especializar cada producto en determinados sectores, aunque sólo el tiempo, no mucho, lo confirmará. [48]

### 6.1.5 ethernet en el futuro

Gigabit ethernet deberá ser inter-operable con las redes existentes 802.3, carrier extensión es una ruta del 802.3 que mantiene los tamaños de trama máximos y mínimos con distancias significativas de cableado. Para que el carrier sea extendido dentro de la trama, los símbolos de extensión de no-data son incluidos en la ventana de colisiones, que es, la trama entera extendida considerada por la colisión y caída. Sin embargo, la secuencia de chequeo en la trama (FCS) es calculada solamente en la trama original (sin los símbolos de extensión). Los símbolos de extensión son removidos antes que el FCS sea chequeado por el receptor. Por lo que la capa LLC es ni siquiera avisado de la carrier extensión. (ver figura 26) [49]

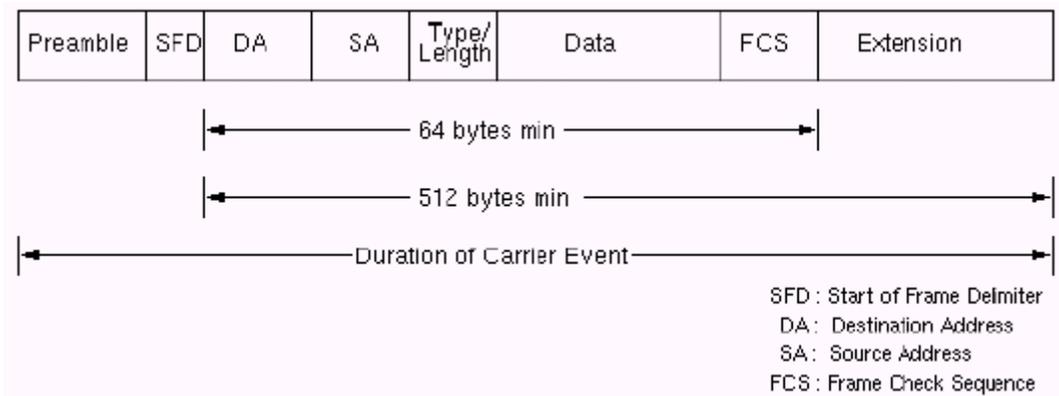


Figura 26 formato de la trama ethernet cuando el carrier extensión es usado.

### 6.1.6 Packet Bursting

Packet bursting es una extensión de carrier extensión. packet bursting es "carrier extensión más unos paquetes agregados" (burst). Cuando una estación tiene un número de paquetes a transmitir, el primer paquete coloca al time slot si es necesario usando carrier extensión. Los siguientes paquetes son transmitidos unos detrás de otro, con el mínimo intervalo inter-packet (IPG) hasta que finalice el tiempo de burst (de 1500 bytes). El packet bursting sustancialmente incrementa el throughput. En la siguiente figura 27 se muestra como trabaja el packet burst. [49]

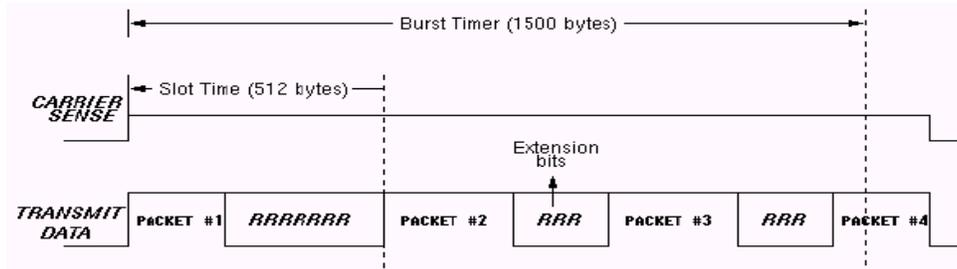


Figura 27 como trabaja el Packet Burst.

gigabit interfase independiente del medio (GMII). La GMII es la interfaz entre la capa MAC y la capa física. Esto permite que algunas de las capas físicas ser usada con la capa MAC. Existe una extensión de la MII (media independent interface) usada en fast ethernet. Este usa la misma interfaz de [gestión](#) como MII. Este soporta transmisión de [datos](#) de 10, 100 y 1000 Mbps. Posee separadamente un receptor de 8-bit de ancho y un trasmisor que agrega datos, tal que puede soportar operaciones como full-duplex y half-duplex. fig. 28. [49]

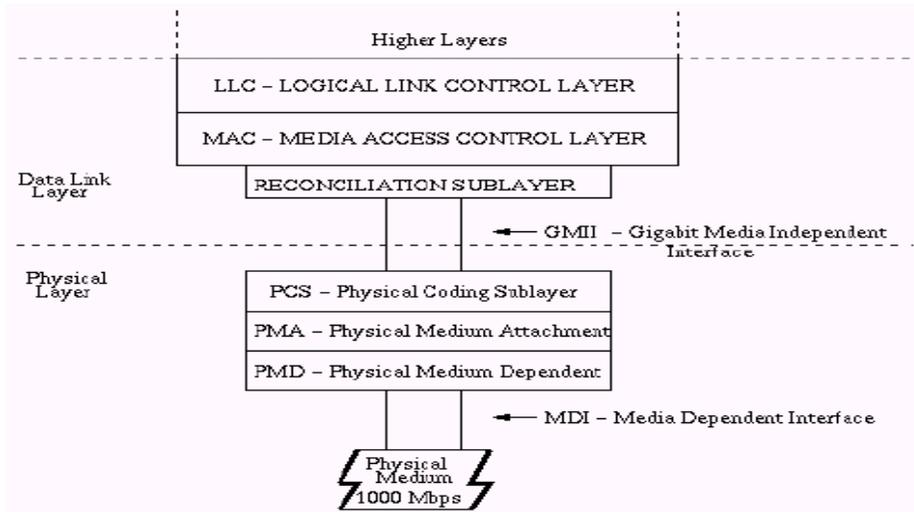


Figura 28 Las diferentes capas de la arquitectura del protocolo Gigabit Ethernet

La GMII posee 2 medios de señales del status: uno indica la presencia del carrier y el otro indica la ausencia de colisión. La sub-capa de reconciliación (RS) proyecta estas señales a señalización física (PLS) primitivas conocida por la sub-capa MAC existente. Con la GMII es posible conectar diferentes tipos de medios tales como cable UTP, [fibra óptica](#) mono-modo y multi-modo, mientras se sigue usando el mismo controlador MAC. La GMII está dividida en 3 sub-

capas: PCS, PMA, PMD. PCS (Physical Coding Sublayer) La PCS es la sub-capas de la capa GMII que provee una interfaz uniforme para la reconciliación de capas por todo el medio físico. Usa [código](#) 8B/10B empleado por canales de fibra. En estos tipos de códigos 8 bits están representados por 10 bits "[grupos de códigos](#)". Algunos grupos de códigos representan datos simbólicos de 8 bits. Otros son símbolos de control. Los símbolos de extensión usados en el carrier extensión son un ejemplo de símbolos de control. Las indicaciones de carrier sense y collision detect son generados por esta sub-capas. Esta sub-capas también maneja los procesos de auto negociación por el cual la tarjeta de red ([NIC](#)) se comunica con la red para determinar la velocidad de la misma (10, 100 o 1000 Mbps) y el modo de operación (half-duplex o full-duplex). PMA (Physical Médium Attachment). Esta sub-capas provista de un medio independiente por la sub-capas PCS para soportar diferentes medios físicos de bit-orientados serialmente. Esta capa forma grupos de códigos seriales por transmisión y desambla los códigos de grupos seriales cuando los bits son recibidos. PMD. Esta sub-capas proyecta el medio físico para la sub-capas PCS. Esta capa define la señalización de la capa físicas usadas por diferentes medios. La MDI, la cual es parte de PMD es actualmente la interfaz de la capa física. Esta capa define la actual capa física de unión, como los conectores de los diferentes medios de transmisión. [49]

## **6.2 REDES INALÁMBRICAS 802.11**

### **6.2.1 Wi-Fi**

Es un conjunto de estándares para redes inalámbricas. Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad, también se utiliza para acceder a Internet como es el caso de internet turbo Wi-Fi.

Ventajas:

- Movilidad, desde cualquier lugar dentro de su cobertura.

- Fácil instalación, más rapidez y simplicidad que si utilizáramos cables
- Flexibilidad, ya que permite el acceso a la red en entornos donde es difícil realizar un cableado.
- Adaptabilidad, porque permite frecuentes cambios en topología de la red y facilita su escalabilidad. Se puede decir que la tecnología Wi-Fi, es una solución que unifica la movilidad y la conectividad, ofreciendo un nuevo esquema de oficina móvil sin cables.

Este servicio combina las tecnologías ADSL y Wi-Fi permitiendo acceder al internet a alta velocidad de manera inalámbrica. Es una solución idónea para dar acceso a Internet tanto a usuarios internos de la empresa como a sus clientes, en este último caso, como un valor agregado en lugares tales como: salas de esperas, aeropuertos, restaurantes, librerías, plazas comerciales, hoteles, centros de convenciones, universidades, entre otros. [50]

### **6.2.2 Funcionamiento de Internet turbo Wi-Fi**

Internet turbo Wi-Fi utiliza un modem inalámbrico que opera con una frecuencia pública (no licenciada) de 2.4 Ghz bajo el estándar 802.11 g. Dicho modem está preparado para transmitir datos a alta velocidad de manera inalámbrica haciendo la función de punto de acceso o hotspot. En una red inalámbrica cada laptop o PDA debe tener integrada la tecnología Wi-Fi o debe disponer de una tarjeta de red inalámbrica. Luego de instalado el servicio, el usuario sólo debe ubicarse dentro de una distancia máxima de 300 pies del modem o punto de acceso, verificar la señal Wi-Fi del servicio en su pantalla y ejecutar el navegador de su preferencia para comenzar a navegar. [50]

### **6.2.3 Las redes inalámbricas o WN**

Básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE. Como suele pasar siempre

que un estándar aparece y los grandes fabricantes se interesan por él, aparecen diferentes aproximaciones al mismo lo que genera una incipiente confusión. Nos encontramos ante tres principales variantes: **802.11a**: fue la primera aproximación a las **WN** y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por punto de acceso. Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma. Sus principales desventajas son su incompatibilidad con los estándares **802.11b** y **g**, la no incorporación a la misma de **QoS** (posibilidades de aseguro de calidad de servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia online), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la **HyperLAN2** y la parcial disponibilidad de la misma en Japón. [50]

#### **6.2.4 Redes inalámbricas de consumo**

Redes CDMA (estándar de telefonía móvil estadounidense) y GSM (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

**802.16** son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (MAN) en la banda de entre los 2 y los 11 Ghz. Estas redes no entran dentro del ámbito del presente documento.

**802.11b**: es la segunda aproximación de las WN. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización del IEEE. Opera dentro de la frecuencia de los 2'4 Ghz. Inicialmente se soportan hasta 32 usuarios por AP.

**802.11a** como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2'4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos bluetooth, lo cual puede provocar interferencias. En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE.

**802.11g**: Es la tercera aproximación a las WN, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps. Funciona dentro de la frecuencia de 2'4 Ghz. Dispone de los mismos inconvenientes que el 802.11b además de los que pueden aparecer por la aún no estandarización del mismo por parte del IEEE (puede haber incompatibilidades con dispositivos de diferentes fabricantes). Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad. [50]

### **6.2.5 Clasificación de las redes inalámbricas-redes inalámbricas personas**

Las redes inalámbricas (WN), se están introduciendo en el mercado de consumo gracias a unos precios populares y a un conjunto de entusiastas, mayoritariamente particulares, Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura). En un futuro cercano se reunificarán todo aquellos dispositivos con los que hoy contamos para dar paso a unos nuevos que perfectamente podrían llamarse terminales internet en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, ordenador portátil y un largo etcétera. Se podría dar lugar a una Internet paralela y gratuita la cual estaría basada en las redes que

altruistamente cada uno de nosotros pondríamos a disposición de los demás al incorporarnos a las mismas como destino y origen de la información. En las grandes ciudades por fin se podría llevar a cabo un control definitivo del tráfico con el fin de evitar atascos, limitando la velocidad máxima y/o indicando rutas alternativas en tiempo real. Las tecnologías que son necesarias para llevar a cabo estos sistemas hoy existen desde ayer, su precio es mínimo o al menos muy accesible y su existencia mañana sólo depende de las estrategias comerciales de las empresas que las poseen. En el mundo wireless existen dos topologías básicas:

- **Topología Ad-Hoc.** Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red par a par, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si.

- **Topología Infraestructura,** en el cual existe un nodo central (punto de acceso WiFi) que sirve de enlace para todos los demás (tarjetas de red Wi-fi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP. Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo: modo managed, es el modo en el que el TR se conecta al AP para que éste último le sirva de "concentrador". El TR sólo se comunica con el AP. Modo master. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida. Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW. [50]

### **6.2.6 Velocidad vs modulación**

802.11g es una unión de los estándares 802.11 "a" y "b". Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, los otros dos operan en la del los 2'4 Ghz. Cuando tenemos una red inalámbrica en la que todos los dispositivos son tipo "a" o "b" no hay problemas en las comunicaciones. Cada AP tipo "a" tendrá sólo TRs tipo "a" y los APs tipo "b" tendrán sólo TRs tipo "b". Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible. En el caso de dispositivos AP 802.11g normalmente estaremos usando la modulación OFDM, que es la óptima para este estándar. Si un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b". Sin embargo el dispositivo "b" no puede escuchar las transmisiones de los otros dispositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez. Para evitar las colisiones, los equipos "b" usan la modulación barker con TRS/CTS, que básicamente significa que deben pedir permiso al AP para transmitir. [50]

### **6.2.7 Topología y Modos de funcionamiento de los dispositivos**

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida. [50]

## CONCLUSIONES

En esta monografía se presentan algunos elementos importantes para conocer los funcionamiento de ethernet es por eso la importancia de tener las bases y el conocimiento adecuado de el funcionamiento de los diferentes tipos de redes de telecomunicaciones, tomando en cuenta sus ventajas y desventajas, sabiendo que la finalidad de esta monografía es arrojar los requerimientos necesarios para obtener el optimo desempeño de las redes ethernet.

Tomando en cuenta la importancia del ancho de banda en networking, el por qué se utilizan modelos divididos en capas para describir la comunicación de datos, identificando cada una de las siete capas del modelo OSI, identificando las cuatro capas del modelo TCP/IP, los dispositivos utilizados en networking, comprendiendo la función de los protocolos en networking, contando con la definición de las redes LAN, WAN, MAN y SAN, las VPN y sus ventajas y desventajas de los repetidores, hubs, puentes, switches, los componentes de una red inalámbrica, la diferencia entre las conexiones WAN seriales, de red digital de servicios integrados (RDSI), de línea digital del suscriptor (DSL), y de cable módem. Así como las reglas de denominación de la tecnología de ethernet, tanto como el proceso de entramado de ethernet y la estructura de la trama, y por ultimo las características del CSMA/CD y definir los errores y las colisiones de ethernet, así como la descripción de las similitudes y diferencias entre las redes ethernet.

Por lo tanto a medida que se tornen económicos, se deben implementar fast ethernet o gigabit en las redes de telecomunicaciones para lograr los óptimos resultados deseados

## GLOSARIO

**ACL:** Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

**Activo:** Se debe conectar un concentrador activo a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.

**Ancho de banda:** La capacidad de datos de un enlace. En general, se prefiere un enlace Ethernet de 10 Mbps. a una línea arrendada de 64 kbps.

**Asíncrona** significa que cada estación receptora utiliza los ocho octetos de la información de temporización para sincronizar el circuito receptor con los datos entrantes y luego los descarta.

**Backbone** Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene, y se destina a, otras redes.

**Backbone colapsada** Backbone no distribuida en la que todos los segmentos de red se encuentran interconectados mediante un dispositivo de internetworking. Una backbone colapsada puede ser un segmento de red virtual que existe en un dispositivo tal como un hub, un router o un switch.

**Backbone de multicast.** El backbone de multicast de Internet. MBONE es una red de multicast virtual compuesta por LAN de broadcast y los túneles punto a punto que las interconectan.

**Bits de código:** Funciones de control, como configuración y terminación de una sesión.

**Bus:** Un conjunto de pistas eléctricas en la placa madre a través del cual se transmiten señales de datos y temporización de una parte del computador a otra.

**CDMA** estándar de telefonía móvil estadounidense

**Checksum (suma de comprobación):** Suma de comprobación calculada a partir de los campos del encabezado y de los datos.

**Checksum (suma de verificación) de Internet:** Agrega los valores de todos los bits de datos para obtener una suma.

**Checksum del encabezado:** ayuda a garantizar la integridad del encabezado IP, 16 bits.

**Circuito integrado:** Dispositivo fabricado con material semiconductor que contiene varios transistores y realiza una tarea específica.

**CNAC:** Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

**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

**Concentrador:** concentran las conexiones.

**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 enchufa a un puerto o interfaz

**Confiabilidad:** Generalmente se refiere al índice de error de cada enlace de red.

**Datos:** Contiene información de capa superior, longitud variable hasta un de máximo 64 Kb.

**Crossover:** cable de conexión cruzada

**Dirección de destino:** Especifica la dirección IP del nodo receptor, 32 bits.

**Dirección de origen:** Especifica la dirección IP del nodo emisor, 32 bits.

**Error de alineamiento:** Número insuficiente o excesivo de bits transmitidos.

**Error de FCS:** Transmisión dañada.

**Error de intervalo:** El número real y el informado de octetos en una trama no concuerdan.

**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.

**Firewire:** Una norma de interfaz de bus serial que ofrece comunicaciones de alta velocidad y servicios de datos isócronos de tiempo real.

**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).

**Flash:** Reproduce archivos multimediales, creados con Macromedia Flash

**Flexibilidad:** un algoritmo de enrutamiento debe adaptarse rápidamente a una

**Full duplex:** La capacidad de comunicación en ambas direcciones al mismo tiempo

**GMII** es la interfaz entre la capa MAC y la capa física.gran variedad de cambios en la red.

**GSM** estándar de telefonía móvil europeo y asiático

**Identificación:** Contiene un número entero que identifica el datagrama actual, 16 bits. Este es el número de secuencia.

**IEEE 802.3ab**, especifica el uso de cable de cobre balanceado de categoría 5, o menor.

**IEEE 802.3z**, especifica una conexión full duplex de 1 Gbps en fibra óptica.

**IGRP** es un protocolo de enrutamiento por vector-distancia desarrollado por cisco.

**Inteligente:** A los hubs inteligentes a veces se los denomina "smart hubs".

**jabber:** Transmisión excesiva o ilegalmente larga.

**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 el computador 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 del computador 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.

**Microprocesador:** Un microprocesador es un procesador que consiste en un chip de silicio diseñado con un propósito especial y físicamente muy pequeño.

**Módem**, o modulador-demodulador, es un dispositivo que ofrece al computador conectividad a una línea telefónica.

**Número de secuencia:** El número que se usa para asegurar el secuenciamiento correcto de los datos entrantes.

**Optimización:** la optimización describe la capacidad del algoritmo de enrutamiento de seleccionar la mejor ruta.

**OSA** (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP.

**OSPF** es un protocolo de enrutamiento de estado de enlace desarrollado por la Fuerza de tareas de ingeniería de Internet (IETF) en 1988.

**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.

**Pasivo:** Un hub pasivo sirve sólo como punto de conexión física. No requiere energía eléctrica.

**PCMCIA:** es el acrónimo para Personal Computer Memory Card International Association (Asociación Internacional de Tarjetas de Memoria de Computadores Personales). Las tarjetas PCMCIA también se conocen como tarjetas PC.

**Ping** es un programa básico que verifica que una dirección IP particular existe y puede aceptar solicitudes.

**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.

**Protocolo:** indica cuál es el protocolo de capa superior, por ejemplo, TCP o UDP, que recibe el paquete entrante luego de que se ha completado el procesamiento IP, ocho bits.

**Puentes** convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos.

**Puerto serial:** Interfaz que se puede utilizar para la comunicación serial, en la cual sólo se puede transmitir un BIT a la vez.

**Ranura de expansión:** Un receptáculo en la placa madre donde se puede insertar una placa de circuito impreso para agregar capacidades al computador y AGP.

**Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas.

**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.

**Relleno:** se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits.

**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.

**Repetidor:** es un dispositivo de red que se utiliza para regenerar una señal.

**RIP Versión 2 (RIPv2)** ofrece un prefijo de enrutamiento y envía información de la máscara de subred en sus actualizaciones.

**Reservado:** Establecido en cero.

**Retardo:** la cantidad de tiempo requerido para transportar un paquete a lo largo de cada enlace desde el origen hacia el destino.

**Ring:** Anillo

**RIP** es un protocolo de enrutamiento vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier enlace en internetwork.

**Síncrona** significa que la información de temporización no es necesaria, sin embargo, por razones de compatibilidad, el Preámbulo y la SFD (Delimitador de Inicio de Trama) están presentes.

**SKA** Es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

**SOHO**-Small Office/Home Office brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña

**SSID.** Service Set Identifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

**Straight-through** cable de conexión directa

**Switches** de grupos de trabajo agregan inteligencia a la administración de transferencia de datos.

**Tipos de medios:** Cable de par trenzado, cable coaxial, inalámbrico o fibra óptica.

**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).

**Topología broadcast:** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red.

**Topología lógica de una red** es la forma en que los hosts se comunican a través del medio.

**Trama corta, fragmento de colisión o runt:** Transmisión ilegalmente corta.

**Unidad de CD-ROM:** Unidad de disco compacto con memoria de sólo lectura, que puede leer información de un CD-ROM. transcurrido la ranura temporal.

**Transmisión de tokens:** controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial.

**Unidad de disco duro:** Un dispositivo de almacenamiento computacional que usa un conjunto discos rotatorios con cubierta magnética para almacenar datos o programas.

**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.

**Unidad de procesamiento central (CPU):** La parte de un computador 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 del sistema:** La parte principal del PC, que incluye el armazón, el microprocesador, la memoria principal, bus y puertos.

**Versión:** Especifica el formato del encabezado de IP.

**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.

**WEP:** Fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos.

**Wi-Fi,** Abreviatura de Wireless Fidelity, es un conjunto de estándares para redes inalámbricas.

## SIGLARÍO

**ANSI** Instituto nacional americano de normalización  
**ARP** Protocolo de resolución de direcciones  
**ASIC** Circuito integrado de aplicación específica  
**BGP** Protocolo de gateway fronterizo.  
**BRI** Interfaz de acceso básico  
**CAM** Tabla de memoria de contenido direcciónable  
**CCITT** Comité consultivo internacional telegráfico y telefónico  
**CRC** Verificación por redundancia cíclica  
**CSU/DSU** Unidad de servicio de canal/datos  
**DHCP** Protocolo de configuración dinámica del host  
**DNS** Sistema de denominación de dominios.  
**DSL** Línea de suscripción digital  
**DSSS** Espectro disperso de secuencia directa  
**DTE** Equipo terminal de datos  
**EGP** Protocolos de enrutamiento de gateway exterior  
**EIA** Asociación de industrias electrónicas  
**FDE** Ethernet full duplex  
**FHSS** Espectro disperso por salto de frecuencia  
**FTP** Protocolo de Transferencia de Archivos.  
**GMII** Gigabit interfase independiente del Medio  
**HTTP** Protocolo de transferencia de hipertexto.  
**ICMP** Protocolo de mensajes de control de Internet  
**IEEE** Instituto de ingeniería eléctrica y electrónica  
**IGP** Protocolos de enrutamiento de gateway interior  
**IRQ** Petición de interrupción  
**LEAP** Protocolo liviano de autenticación extensible  
**LLC** Protocolo de control de enlace lógico  
**MAN** Redes de área metropolitana

**MDI** Medium dependent interface  
**NIC** Tarjetas de interfaz de red.  
**NMS** Sistema de administración de la red.  
**NRZ** Simple codificación de línea sin retorno a cero.  
**OUI** Identificador exclusivo organizacional.  
**PCS** Physical coding sublayer  
**PING** Packet internet or inter-network groper  
**PLS** Señalización física  
**PMA** Physical médium attachment  
**PMD** Physical medium dependent  
**PPP** Protocolo punto a punto  
**RIP** Protocolo de información de enrutamiento  
**RS** Sub -capa de reconciliación  
**SAN:** Redes de área de almacenamiento.  
**SDH** Redes síncronas de jerarquía digital  
**SFD** Delimitador de Inicio de trama  
**SMTP** Protocolo simple de transferencia de correo  
**SNMP** Protocolo simple de administración de red.  
**SONET** Red óptica síncrona  
**SQE** Señal de error de calidad de señal.  
**TCP** Protocolo para el control del transporte  
**TFTP:** Protocolo trivial de transferencia de archivos.  
**TIA** Asociación de la industria de las telecomunicaciones  
**TRS/CTS** Request to send / clear to send  
**UDP** Protocolo de datagrama de usuario.  
**UIT** Unión internacional de telecomunicaciones  
**URL** Localizador de recursos uniforme.  
**VPN** Red privada virtual  
**WAN** Redes de área amplia.  
**WWDM** Amplia multiplexión por división de longitud de onda

## REFERENCIAS BIBLIOGRÁFICAS

[1] José Luís Raya y Cristina Raya Pérez, 2000 redes locales y tcp/ip, edición original publicada por RA-MA, editorial Madrid, España.

[2] Revista pc magazine numero 80, año 1995.

## REFERENCIAS BIBLIOGRÁFICAS

- [3]<http://library.albany.edu/Internet/connect.html>, 2003, USA.
- [4]<http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/nic.html>, 2003, USA.
- [5]<http://calvin.linfield.edu/~darnett/helpages/NICinstall/NICStar.html>, 2003, USA.
- [6][http://www.windowsnetworking.com/j\\_helmig/tcpip.htm](http://www.windowsnetworking.com/j_helmig/tcpip.htm), 2003, USA.
- [7]<http://www.chami.com/tips/internet/060298l.html>, Copyright © 1995-2005 Chami.com. All Rights Reserved.USA.
- [8]<http://www.howstuffworks.com/category.htm?cat=Hardwar>, 2003, USA.
- [9][www.cisco.netacad.net](http://www.cisco.netacad.net), todo el contenido copyright@2003, cisco System, Inc. todos los derechos educación mundial, USA.
- [10]<http://www.protocols.com/pbook/tcpip1.htm> 2003, USA.
- [11][http://searchnetworking.techtarget.com/sDefinition/0,sid7\\_gci214083,00.html](http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci214083,00.html), 2003, USA.
- [12][http://www.gcn.com/21\\_16/guide/19055-1.html](http://www.gcn.com/21_16/guide/19055-1.html) 2006 Post-Newsweek Media, Inc. All Rights Reserved.
- [13]<http://aplawrence.com/Basics/vpn.html>, 2003, USA.
- [14][http://www.clavister.com/manuals/ver8x/manual/vpn/vpn\\_overview.htm](http://www.clavister.com/manuals/ver8x/manual/vpn/vpn_overview.htm), Copyright(c) 1997-2002 Clavister AB. All rights reserved.

- [15]<http://www.intrack.com/intranet/faqbasic.cfm>, 2003, USA.
- [16]<http://www.jegsworks.com/Lessons/lessonintro.html>, 2003
- [17][http://english.peopledaily.com.cn/200105/18/eng20010518\\_70356.html](http://english.peopledaily.com.cn/200105/18/eng20010518_70356.html), 2003, USA.
- [18]<http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/phy.html>, 2003.
- [19]<http://www.kan.org/networking/nethardware.html>, 2003, USA.
- [20][http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci212890,00.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212890,00.html).  
All Rights Reserved, Copyright 2000 - 2006.
- [21][http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci213380,00.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213380,00.html).  
All Rights Reserved, Copyright 2000 - 2006.
- [22][http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci211705,00.htm](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211705,00.htm). All Rights Reserved, Copyright 2000 - 2006.
- [23][http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci213079,00.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213079,00.html).  
All Rights Reserved, Copyright 2000 - 2006.
- [24][http://searchnetworking.techtarget.com/searchSystemsManagement\\_redirect/0,294431,sid7,00.html](http://searchnetworking.techtarget.com/searchSystemsManagement_redirect/0,294431,sid7,00.html). All Rights Reserved, Copyright 2000 - 2006.
- [25][http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci212769,00.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html).  
All Rights Reserved, Copyright 2000 - 2006.
- [26] <http://www.ralphb.net/ISDN/intro.html>, 2003, USA.

[27] <http://www.faqs.org/faqs/datacomm/xdsl-faq/2003>, USA.

[28] [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ethernet.htm#xtocid2](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm#xtocid2), 2003, USA.

[29] <http://www.ieee802.org/> 2003, USA.

[30] <http://standards.ieee.org/regauth/oui/index.shtml>, Copyright ©2005 IEEE-SA, USA.

[31] [http://www.ee.usyd.edu.au/ecsl/CAP/USYDmodules/EBUS3001\\_m1\\_det.html](http://www.ee.usyd.edu.au/ecsl/CAP/USYDmodules/EBUS3001_m1_det.html), 2003, USA.

[32] <http://www.wildpackets.com/compendium/EN/EN-FrFmt.html>, 2003, USA.

[33] [http://www.cisco.com/en/US/tech/tk389/tk214/tk125/tech\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk389/tk214/tk125/tech_protocol_home.html), 2003, USA.

[34] <http://www.networkcomputing.com/netdesign/t15errors.html>, TechWeb is brought to you by CMP Media LLC, Copyright © 2005, USA.

[35] <http://www.networkcomputing.com/netdesign/t15errors.html>, Copyright © 2005

[36] <http://www.cites.uiuc.edu/network/autosense.html>, Últimas modificaciones en diciembre 30, 2003, USA.

[37] <http://www.webopedia.com/TERM/1/10BaseT.htm>, USA.

[38] [http://www.ethermanage.com/ethernet/100quickref/ch10qr\\_1.html](http://www.ethermanage.com/ethernet/100quickref/ch10qr_1.html), 2003, USA.

[39][http://www.bostontech.net/assets/files/articles/TechBrief1\\_P1.pdf](http://www.bostontech.net/assets/files/articles/TechBrief1_P1.pdf),2003,USA.

[40][http://www.cisco.com/en/US/tech/tk389/tk214/tk771/tech\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk389/tk214/tk771/tech_protocol_home.html),  
USA.

[41][http://www.ctr.columbia.edu/~dimitri/teaching/E6761/Lecture7/switching\\_bridging.pdf](http://www.ctr.columbia.edu/~dimitri/teaching/E6761/Lecture7/switching_bridging.pdf), 2003, USA.

[42]<http://msridhar.freeshell.org/switching.html>, 2003, USA.

[43][http://whatis.techtarget.com/definition/0,,sid9\\_gci212456,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci212456,00.html)

[44][http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/lanswtch.html](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/lanswtch.html), All  
contents are Copyright © 1992--2002 Cisco Systems, Inc. All rights reserved.

[45][http://www.transition.com/TransitionNetworks/Resources/en/PDF/colldom\\_wp.pdf](http://www.transition.com/TransitionNetworks/Resources/en/PDF/colldom_wp.pdf), 2003, USA.

[46][http://www.oreillynet.com/pub/a/network/2001/03/16/net\\_2nd\\_lang.html](http://www.oreillynet.com/pub/a/network/2001/03/16/net_2nd_lang.html)

[47]<http://www.howstuffworks.com/lan-switch3.html>, 2003, USA.

[48][http://www.consulintel.es/Html/Tutoriales/Articulos/eth\\_y\\_c.html](http://www.consulintel.es/Html/Tutoriales/Articulos/eth_y_c.html)

[49][www.tolosa.go.cc](http://www.tolosa.go.cc), Fuente: Dpto. de Ciencias de la Computación, Universidad de Ohio.

[50]<http://www.tricom.net/int009.html>.