Universidad Autónoma De Querétaro

Facultad de Informática

Opción de Titulación: Guía del Maestro

Materia: Redes I

Profesor Titular: M.S.I. Ernesto Ruvalcaba Durán

Alumna: Soraya Lizbeth Sánchez Torres

Generación: 2000

CONTENIDO

RESÙMEN I
ÍNDICE DE FIGURAS VIII
ÍNDICE DE TABLAS XIII
ACRONIMOS XIV
INTRODUCCIÒN XVII
CAPÌTULO I Introducción a las Redes 1
1.1 Conexión a la Internet 2
1.1.1 Requisitos para la conexión a Internet 2
1.1.2 Principios básicos de los PC 3
1.1.3 Tarjeta de interfaz de red 9
1.1.4 Instalación de NIC y módem 10
1.1.5 Descripción general de la conectividad de alta velocidad y de acceso Telefónico 11
1.1.6 Descripción y configuración TCP/IP 11
1.1.7 Probar la conectividad con ping. 12
1.1.8 Navegadores de Web y plug-ins 13
1.1.9 Diagnóstico de los problemas de conexión a Internet 15
1.2 Matemática de redes 15
1.2.1 Representación binaria de datos 15
1.2.2 Bits y bytes 16
1.2.3 Sistema numérico de Base 10 17
1.2.4 Sistema numérico de Base 2 18
1.2.5 Conversión de números decimales en números binarios de 8 bits 20
1.2.6 Conversión de números binarios de 8 bits en números decimales 21
1.2.7 Representación en notación decimal separada por puntos de cuatro octetos de números binarios de 32 bits 22
1.2.8 Hexadecimal. 23
1.2.9 Lógica booleana o binaria 25
1.2.10 Direcciones IP y máscaras de red 27
Resumen 29
CAPITULO 2: Aspectos básicos de Redes 30
2.1 Terminología de Redes 31
2.1.1 Redes de datos 31
2.1.2 Historia de las redes informáticas 34
2.1.3 Dispositivos de Red 36
2.1.4 Topología de red 40
2.1.5 Protocolos de red 42
2.1.6 Redes de área local (LAN) 43
2.1.7 Redes de área amplia (WAN) 43
2.1.8 Redes de área metropolitana (MAN) 44
2.1.9 Redes de área de almacenamiento (SAN) 45
2.1.10 Red privada virtual (VPN) 45
2.1.11 Ventajas de las VPN 46

3.3.6 Señales y ruido en una WLAN 94
3.3.7 Seguridad de la transmisión inalámbrica 95
Resumen 96
CAPITULO 4: Prueba del cable 98
4.1 Información básica para el estudio de pruebas de cables basadas en frecuencia. 99
4.1.1 Ondas 99
4.1.2 Ondas sinoidales y ondas rectangulares 99
4.1.3 Exponentes y logaritmos 100
4.1.4 Decibelios 101
4.1.5 Visualización de señales en tiempo y frecuencia 102
4.1.6 Señales analógicas y digitales en tiempo y frecuencia 103
4.1.7 El ruido en tiempo y frecuencia 103
4.1.8 Ancho de banda 104
4.2 Señales y ruido 104
4.2.1 Señales en cable de cobre y fibra óptica 104
4.2.2 Atenuación y pérdida de inserción en medios de cobre 106
4.2.3 Fuentes de ruido en medios de cobre 107
4.2.4 Tipos de diafonía 108
4.2.5 Estándares de prueba de cables 110
4.2.6 Otros parámetros de prueba 112
4.2.7 Parámetros basados en tiempo 113
4.2.8 Prueba de fibra óptica 114
4.2.9 Un nuevo estándar 114
Resumen 116
CAPÌTULO 5: Cableado de las LAN y las WAN 117
5.1 Cableado LAN 118
5.1.1 Capa física de la LAN 118
5.1.2 Ethernet en el campus 119
5.1.3 Medios de Ethernet y requisitos de conector 120
5.1.4 Medios de conexión 121
5.1.5 Implementación del UTP 121
5.1.6 Repetidores 125
5.1.7 Hubs 126
5.1.8 Redes inalámbricas 126
5.1.9 Puentes 127
5.1.10 Switches 128
5.1.11 Conectividad del host 129
5.1.12 Comunicación de par a par 130
5.1.13 Cliente/servidor 131
5.2 Cableado WAN 133
5.2.1 Capa física de las WAN 133
5.2.2 Conexiones seriales de WAN 133
5.2.3 Conexiones seriales y router 134
5.2.4 Conexiones BRI RDSI y routers 136
5.2.5 Conexiones DSL y routers 138
5.2.6 Conexiones de cable-modem y routers 138

8.1.2 Conmutación a nivel de Capa 2 193
8.1.3 Operación de switches 193
8.1.4 Latencia 194
8.1.5 Modo de conmutación 194
8.1.6 Protocolo de Spaning Tree (árbol de extensión) 195
8.2 Dominios de colisión y de broadcast 196
8.2.1 Entorno de medios compartidos 196
8.2.2 Dominios de colisión 197
8.2.3 Segmentación 199
8.2.4 Broadcasts de Capa 2 201
8.2.5 Dominios de broadcast 203
8.2.6 Introducción al flujo de datos 203
8.2.7 ¿Qué e una segmento de red? 205
Resumen 206
CAPÌTULO 9: Conjunto de protocolos TCP/IP y direccionamiento IP 207
9.1 Introducción a TCP/IP 208
9.1.1 Historia y futuro e TCP/IP 208
9.1.2 La capa de aplicación 208
9.1.3 La capa de transporte 209
9.1.4 La capa de Internet 211
9.1.5 La capa de acceso de red 212
9.1.6 Comparación entre modelos OSI y el TCP/IP 213
9.1.7 Arquitectura de Internet 214
9.2 Dirección de Internet 216
9.2.1 Direccionamiento IP 216
9.2.2 Conversión decimal y binaria 218
9.2.3 Direccionamiento IPv4 219
9.2.4 Direcciones IP Clase, A, B, C, D y E 221
9.2.5 Direcciones IP reservadas 224
9.2. 6 Direcciones IP públicas y privadas 226
9.2.7 Introducción a la división en subredes 229
9.2.8 IPv4 en comparación con IPv6 230
9.3 Obtener una dirección IP 231
9.3.1 Como Obtener una dirección IP 231
9.3.2 Asignación estática de una dirección IP 232
9.3.3 Asignación de direcciones RARP IP 233
9.3.4 Asignación de direcciones BOOTP IP 233
9.3.5 Administración de direcciones DHCPIP 234
9.3.6 Problemas en la resolución de direcciones 234
9.3.7 Protocolo de resolución de direcciones (ARP) 235
Resumen 237
CAPITULO 10: Principios básicos de enrutamiento y subredes 238
10.1 Protocolo enrutado 239
10.1.1 Protocolos enrutables y enrutados 239
10.1.2 IP como protocolo enrutado 239
10.1.3 Propagación y conmutación de los paquetes dentro del Router 240

ÍNDICE DE FIGURAS

Figura 1.1 Muestra grafica de tarjeta madre....4
Figura 1.2 Muestra grafica de Conectores externos....7
Figura 1.3 Conector IEEE....8
Figura 1.4 Tarjeta de red....9
Figura 1.5 Tarjeta PCMCIA....9
Figura 1.6 Modem Interno....10
Figura 1.7 Modem Externo....10
Figura 1.8 PMCIA alambrica....10
Figura 1.9 Adaptador red interno....10
Figura 1.10 Adaptador de red externo....10
Figura 1.11 Comando ping....12
Figura 1.12 Navegador Netscape Navigator....13
Figura 1.13 Navegador Internet Explore (IE)....14
Figura 1.14 Diagrama de conversión de decimal a binario....20
Figura 1.15 Diagrama de conversión de binario a decimal....21
Figura 1.16 compuertas NOT....25
Figura 1.17 Operación NOT....26
Figura 1.18 Operación AND....26
Figura 1.19 Operación OR....26
Figura 1.20 Direcciones de Protocolo de Internet....27
Figura 2.1 Sistema LAN....32
Figura 2.2 Transformación de la LAN....32
Figura 2.3 Dimensiones relativas LAN y WAN.....33
Figura 2.4 Historia de la red Informática.....34
Figura 2.5 Dispositivos de usuario....36
Figura 2.6 Dispositivos de red....36
Figura 2.7 Dispositivo periférico....36
Figura 2.8 Símbolos para dispositivos del usuario....37
Figura 2.9 Dispositivos de Red....37
Figura 2.10 Dispositivo de Red (repetidor)....38
Figura 2.11 Dispositivo de Red (puente)....38
Figura 2.12 Dispositivo de Red (switch)....39
Figura 2.13 Dispositivo de Red (routers)....39
Figura 2.14 Topología física.....40
Figura 2.15 Topología lógica....40
Figura 2.16 Protocolos de comunicación....42
Figura 2.17 Red de área metropolitana (MAN)....44
Figura 2.18 Redes de área de almacenamiento (SAN)....45
Figura 2.19 Red virtual privada (VPN)....46
Figura 2.20 Características de las VPN....46
Figura 2.21 Red Interna y Externa....48
Figura 2.22 Red de tuberías....50

Figura 4.9 Telediafonia 109
Figura 4.10 Paradiafonia 109
Figura 4.11 Estándar Ethernet T568A, T568B 110
Figura 4.12 Mapa de cableado 111
Figura 4.13 Fallas de cableado 111
Figura 4.14 Analizador de Cable Fluke DSP-4100 115
Figura 5.1 Representación de símbolos 118
Figura 5.2 Topología Ethernet 119
Figura 5.3 Especificaciones de cables y conectores (Ethernet) 121
Figura 5.4 código de colores T568A, o T568B 122
Figura 5.5 Cable conexión directa 123
Figura 5.6 Cable conexión cruzada 123
Figura 5.7 Interconexión dispositivos Cisco 124
Figura 5.8 Tipos de categorías de cable UTP 125
Figura 5.9 LAN dividida en segmentos 128
Figura 5.10 Comunicación de par a par. 130
Figura 5.11 Entorno cliente/servidor 131
Figura 5.12 Servidores 132
Figura 5.13 Conexiones seriales en un router 134
Figura 5.14 Conexión de routers 135
Figura 5.15 Routers conectados como DCE 135
Figura 5.16 Interfaces del Router 136
Figura 5.17 Puertos seriales WAN 136
Figura 5.18 Interfaz BRI 137
Figura 5.19 Router ADSL Cisco 827 138
Figura 5.20 Conexión cable uBR905 138
Figura 5.21 Conexión de puerto de consola 139
Figura 6.1 Supcapa MAC y capa fisica 145
Figura 6.2 Envío de datos por Ethernet entre dos estaciones 145
Figura 6.3 Direcciones MAC 147
Figura 6.4 Diagrama de formato de trama 148
Figura 6.5 Estructura de una trama 150
Figura 6.6 Representación de Ethernet 152
Figura 6.7 Representación Token Ring 153
Figura 6.8 Representación de FDDI 153
Figura 6.9 Funciones de Ethernet 154
Figura 6.10 Ethernet y las Colisiones 158
Figura 6.11 Tipo de colisiones 159
Figura 6.12 Señal con colisión 160
Figura 6.13 Los Jabber y las tramas 162
Figura 6.14 Tramas cortas 162
Figura 7.1 Codificación de Manchester, el eje Y es el voltaje; el eje X es el tiempo. 169
Figura 7.2 Máximo dominio de colisión de punta a punta. 170
Figura 7.3 segmento individual de 10BASE2 171
Figura 7.4 Salida de pins conexión 10BASE-T 172
Figura 7.5 Enlace de 10BASE-T 173

Figura 9.25 Direcciones IP públicas 228
Figura 9.25 Creación de direcciones IP en una subred 229
Figura 9.26 Direcciones IPv4 e IPv6 231
Figura 9.26 Direccionamiento estático y dinámico 232
Figura 10.1 Propagación y conmutación de los paquetes 240
Figura 10.2 Enrutamiento capa 3 243
Figura 10.3 Encapsulamiento y desencapsulamiento 244
Figura 10.4 Conmutación 245
Figura 10.5 Tablas ARP de las direcciones MAC de Capa 2 y las tablas de enrutamiento de las direcciones IP de Capa 3 246
Figura 10.6 Tablas de enrutamiento 249
Figura 10.7 División entre redes y Hosts 254
Figura 10.8 Mascara de direcciones clase C 256
Figura 10.9 Tabla de subredes 256
Figura 10.10 Esquema de Subred 258
Figura 10.11 División de redes clase A 258
Figura 10.12 Division de redes clase B 258
Figura 10.13 Cálculo e Subred con Operación “AND” 259
Figura 10.14 Cálculo de una operación AND con una dirección IP 259
Figura 11.1 multiplexión de conversaciones de capas superiores 264
Figura 11.2 Sistemas de emisores y receptores 265
Figura 11.3 Transmisión por segmentos 266
Figura 11.4 Intercambio de señales de tres vías. 267
Figura 11.5 Envío de paquete de datos 268
Figura 11.6 Envío de tres paquetes antes de recibir un ACK (acuse de recibo) 269
Figura 11.7 Emisor que transmite paquetes de datos 270
Figura 11.8 Enumeración de segmentos antes de la transmisión 271
Figura 11.9 campos de un segmento TCP 272
Figura 11.10 Número de asignación de puertos 274
Figura 11.11 Protocolos TCP/IP que admiten transferencias de archivos 275

ACRONIMOS

IP	Internet Protocol
DHCP	Protocolo Configuración Dinámica de Servidor
LAN	Red de Área Local
WAN	Red de Área Amplia
MAN	Red de Área Metropolitana
FTP	Protocolo de Transferencia de Archivos
TFTP	Protocolo de transferencia de archivos trivial
ISO	Modelo de interconexión de sistemas abiertos
CDP	Protocolo de descubrimiento
VPN	Red privada virtual
SPX	Intercambio de Paquetes Secuenciados
IPX	Intercambio de paquetes interred
RIP	protocolo de encaminamiento de información
SAP	Protocolo de Anuncio de Servicio
GNS	Get Nearest Server request
NLSP	NetWare Link Services Protocol
CPD	Centro de Proceso de Datos
PDU	Unidades de datos del protocolo
DTE	Equipo Terminal de Datos
DCE	Equipo de Terminación de Circuito
CSMA/CD	Acceso Múltiple con Detección de Portadora y Detección de Colisiones
MAC	Subcapa de control de acceso al medio
CRC	Verificación de redundancia cíclica
LLC	Subcapa de control de enlace lógico
TCP	Protocolo de Control de Transmisión
SYN	Números de secuencia inicial
UDP	User Datagram Protocol
VLSM	Máscara de Subred de Longitud Variable
NAT	Traducción de Dirección de Red

LMI	Interfaz de administración local
ATM	Modo de Transferencia Asíncrona
RDSI	Red Digital de Servicios Integrados
DDR	Enrutamiento por Llamada Telefónica Bajo Demanda

Los medios de redes constituyen literal y físicamente la columna vertebral de una red. La baja calidad de un cableado de red provocará fallas en la red y un desempeño poco confiable. Todos los medios de redes, de cobre, fibras ópticas e inalámbricas, requieren una prueba para asegurar que cumplen con estrictas pautas de especificación. Estas pruebas se basan en ciertos conceptos eléctricos y matemáticos y expresiones tales como señal, onda, frecuencia y ruido. La comprensión de este vocabulario es útil para el aprendizaje de redes, cableado y prueba de cables.

La atenuación, que es el deterioro de la señal, y el ruido, que es la interferencia que sufre la señal, pueden causar problemas en las redes porque los datos enviados pueden ser interpretados incorrectamente o no ser reconocidos en absoluto después de haber sido recibidos. La terminación correcta de los conectores de cables y la instalación correcta de cables son importantes. Si se siguen los estándares durante la instalación, se deberían minimizar las reparaciones, los cambios, la atenuación y los niveles de ruido. Una vez instalado el cable, un instrumento de certificación de cables puede verificar que la instalación cumple las especificaciones TIA/EIA. Aunque cada red de área local es única, existen muchos aspectos de diseño que son comunes a todas las LAN. Por ejemplo, la mayoría de las LAN siguen los mismos estándares y tienen los mismos componentes. En la actualidad, están disponibles varias conexiones de red de área amplia (WAN). Éstas incluyen desde el acceso telefónico hasta acceso de banda ancha, y difieren en el ancho de banda, costo y equipo necesario.

Ethernet es ahora la tecnología LAN dominante en el mundo. Ethernet no es una tecnología sino una familia de tecnologías LAN que se pueden entender mejor utilizando el modelo de referencia OSI. Todas las LAN deben afrontar el tema básico de cómo denominar a las estaciones individuales (nodos) y Ethernet no es la excepción. Las especificaciones de Ethernet admiten diferentes medios, anchos de banda y demás variaciones de la Capa 1 y 2. Sin embargo, el formato de trama básico y el esquema de direccionamiento son igual para todas las variedades de Ethernet.

Para que varias estaciones accedan a los medios físicos y a otros dispositivos de networking, se han inventado diversas estrategias para el control de acceso a los medios. Comprender la manera en que los dispositivos de red ganan acceso a los medios es esencial para comprender y detectar las fallas en el funcionamiento de toda la red.

Ethernet ha sido la tecnología LAN de mayor éxito, en gran medida, debido a la simplicidad de su implementación, cuando se la compara con otras tecnologías. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

Las modificaciones a Ethernet han resultado en significativos adelantos, desde la tecnología a 10 Mbps usada a principios de principios de los 80. El estándar de Ethernet de 10 Mbps no sufrió casi ningún cambio hasta 1995 cuando el IEEE anunció un estándar para Fast Ethernet de 100 Mbps. En los últimos años, un crecimiento aún más rápido en la velocidad de los medios ha generado la transición de Fast Ethernet (Ethernet Rápida) a Gigabit Ethernet (Ethernet de 1 Gigabit).

IPv4, la versión actual de IP, se diseñó antes de que se produjera una gran demanda de direcciones. El crecimiento explosivo de Internet ha amenazado con agotar el suministro de direcciones IP.

La división en subredes, la Traducción de direcciones en red (NAT) y el direccionamiento privado se utilizan para extender el direccionamiento IP sin agotar el suministro. Otra versión de IP conocida como IPv6 mejora la versión actual proporcionando un espacio de direccionamiento mucho mayor, integrando o eliminando los métodos utilizados para trabajar con los puntos débiles del IPv4.

Además de la dirección física MAC, cada computadora necesita de una dirección IP exclusiva, a veces llamada dirección lógica, para formar parte de la Internet. Varios son los métodos para la asignación de una dirección IP a un dispositivo. Algunos dispositivos siempre cuentan con una dirección estática, mientras que otros cuentan con una dirección temporaria que se les asigna cada vez que se conectan a la red. Cada vez que se necesita una dirección IP asignada dinámicamente, el dispositivo puede obtenerla de varias formas.

Para que se produzca un enrutamiento eficiente entre los dispositivos, se deben resolver otros problemas. Por ejemplo, las direcciones IP repetidas pueden detener el eficiente enrutamiento de los datos. El Protocolo de Internet (IP) es el principal protocolo de Internet. El direccionamiento IP permite que los paquetes sean enrutados desde el origen al destino usando la mejor ruta disponible. La propagación de paquetes, los cambios en el encapsulamiento y los protocolos que están orientados a conexión y los que no lo están también son fundamentales para asegurar que los datos se transmitan correctamente a su destino.

La diferencia entre los protocolos de enrutamiento y los enrutados es causa frecuente de confusión entre los estudiantes de networking. Las dos palabras suenan iguales pero son bastante diferentes. Este módulo también introduce los protocolos de enrutamiento que permiten que los Routers construyan tablas a partir de las cuales se determina la mejor ruta a un Host en la Internet.

No existen dos organizaciones idénticas en el mundo. En realidad, no todas las organizaciones pueden adaptarse al sistema de tres clases de direcciones A, B y C. Sin embargo, hay flexibilidad en el sistema de direccionamiento de clases. Esto se denomina división en subredes. La división en subredes permite que los administradores de red determinen el tamaño de las partes de la red con las que ellos trabajan. Después de determinar cómo segmentar su red, ellos pueden utilizar la máscara de subred para establecer en qué parte de la red se encuentra cada dispositivo.

Como su nombre lo indica, la capa de transporte de TCP/IP se encarga de transportar datos entre aplicaciones en dispositivos origen y destino. Es esencial contar con una comprensión absoluta de la operación de la capa de transporte para comprender el manejo de datos en las redes modernas. Este módulo describe las funciones y los servicios de esta capa fundamental del modelo de red TCP/IP. Varias de las aplicaciones de red que se encuentran en la capa de aplicación TCP/IP resultan familiares incluso para los usuarios de red casuales. HTTP, FTP y SMTP, por ejemplo, son siglas que los usuarios de navegadores de Web y los clientes de correo electrónico usan a menudo. Este módulo también describe la función de estas y de otras aplicaciones desde el punto de vista del modelo de red TCP/IP.

1.1 Conexión a la Internet

1.1.1 Requisitos para la conexión a Internet

La Internet es una red de acceso público compuesta por redes de computadoras que transmite datos utilizando IP, el protocolo de Internet. (Tabla 1.1)

Para poder tener conexión a Internet se requiere de tres aspectos principales:

1. **Conexión física:** La cual se realiza 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.

2. **Conexión lógica:** Aplica estándares denominados protocolos.

PROTOCOLO	*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.*

Tabla 1.1 Definición de protocolo

   Como ejemplo tenemos el protocolo de control de transporte/protocolo Internet (TCP/IP) es el principal conjunto de protocolos que se utiliza en Internet. Los protocolos del conjunto TCP/IP trabajan juntos para transmitir o recibir datos e información.

3. **Aplicación que interpreta los datos y muestra la información:** En un formato comprensible ya que 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 Explore 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.

PS/2 para el teclado y el ratón. Además, la tarjeta madre proporciona capacidades de expansión a nuestra PC, a través de los conectores PCI, AGP y PCI Express, que nos permiten agregar componentes para dar nuevas funcionalidades al equipo.

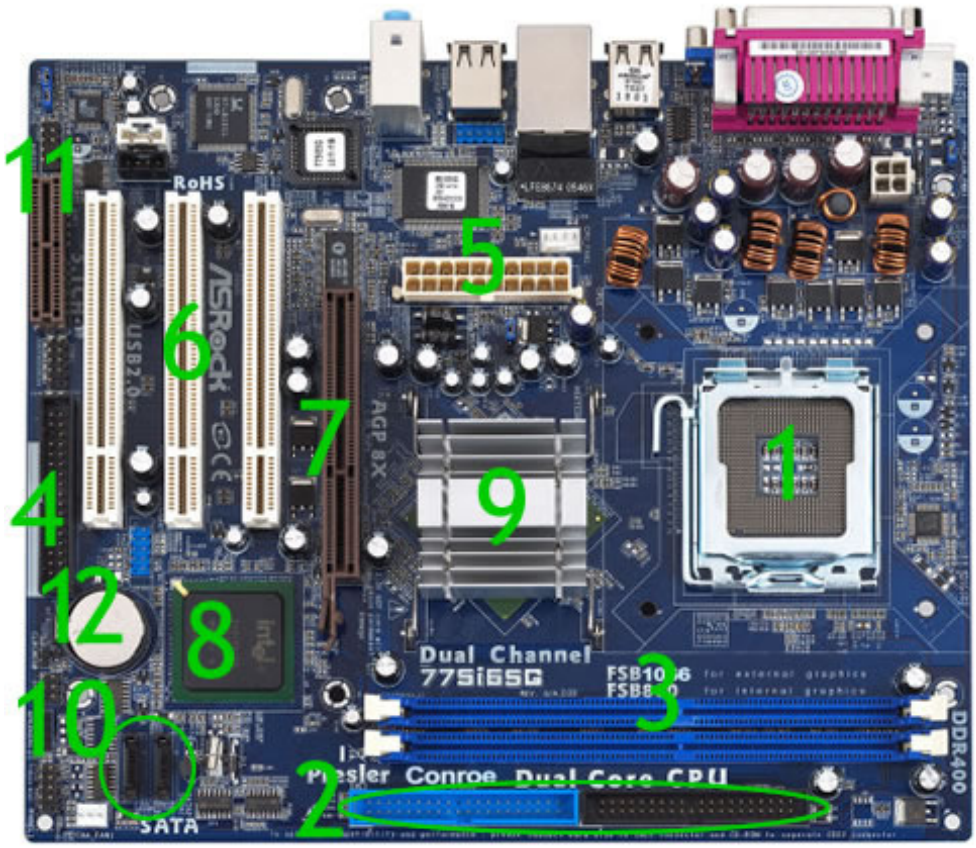


Figura 1.1 Muestra grafica de tarjeta madre

Cabe mencionar, que no todas las tarjetas madres tienen que contar con los elementos mencionados anteriormente, algunas tendrán más o menos conectores que otras, a continuación se da una breve descripción de conectores y sus componentes básicos:

1. Slot del procesador

En este slot se conecta el procesador, y sobre el procesador se conecta el dispersor y el abanico que se encargan de enfriar el procesador y mantenerlo a una temperatura operacional adecuada. Hay que tener en cuenta que hay diferentes tipos de slots y tu tarjeta madre está diseñada para soportar ciertos tipos de procesadores, de modo que no cualquier procesador le queda a tu tarjeta madre, el tipo de slot y los procesadores que soporta se pueden averiguar en el manual de la tarjeta.

7. Slot AGP

Es un conector exclusivo para agregar tarjetas de video dedicadas, funciona a mayor velocidad que los conectores PCI, fue creado para evitar los cuellos de botella que ocurrían antes al conectar tarjetas de video a los slots PCI, ya que con el paso del tiempo, las tarjetas graficas comenzaron a aumentar la velocidad a la que trabajaban y el PCI comenzó a ser insuficiente, de modo que se creó este conector dedicado única y exclusivamente para añadir tarjetas de video.

8. Procesador

El Procesador es el corazón de la motherboard, controla los canales IDE, el canal PCI, el canal AGP, además controla la coordinación memoria-cpu, en resumen, es el encargado de coordinar todos los componentes de la motherboard.

9. Procesador grafico

Si tu tarjeta madre tiene video integrado (es decir que no tiene una tarjeta de video dedicada conectada a un slot PCI, AGP o PCI Express) veras en tu motherboard un dispersor de calor pequeño y en algunos caso un abanico, debajo esta un procesador que se encarga de manejar los gráficos de la computadoraa, de modo que no es necesario invertir mas dinero para tener salida de video en nuestra PC (ya que las tarjetas de video dedicadas son mucho mas caras), por lo general, el video integrado es de bajo desempeño y la memoria de video es compartida con la memoria RAM del sistema.

10. Conector Serial ATA o SATA

Es un conector para los discos duros de tipo Serial, los discos duros tradicionales son Paralelos (ya hablamos que se conectan dos dispositivos por canal IDE). Este tipo de discos duros son mucho más rápidos que los SATA, entre muchos otros beneficios.

11. Slot PCI Express (puede o no tenerlo)

Es la evolución del slot PCI, aunque actualmente se utiliza solo para tarjetas graficas de gama alta y no para otros dispositivos como el slot PCI. Lógicamente, la velocidad de bus de este conector es mayor que la del PCI y que la del AGP. Dependiendo de la velocidad del conector (1x, 4x, 8x, 16x) varía el tamaño del mismo.

4. Puerto paralelo

Principalmente se usa para conectar impresoras a nuestro equipo, aunque hay otros dispositivos que se pueden conectar ahí. En la actualidad la mayoría de las impresoras se conectan por USB, pero impresoras matriciales aun utilizan este conector. Lo podemos identificar por su color rosa.

5. Puertos USB

Son conectores para conectar toda clase de dispositivos a nuestra PC como: Discos Duros externos, memorias USB, cámaras web, Mouse, teclados, etc. Sus siglas significan Universal Serial Bus (Bus Serial Universal) y con universal se refiere a que cualquier cosa se puede conectar ahí, además tiene la característica de que lo que conectes es reconocido de inmediato por la computadora a (el famoso Plug and Play), aunque en ocasiones requerirás de drivers.

6. Conector Ethernet (RJ-45)

Es el conector de red, nos sirve para conectar el MODEM para tener servicio de Internet, o para formar parte de una red casera o de un equipo de trabajo, que a su vez pueden o no darnos servicio de Internet.

7. Conectores de audio

Proporcionan salida de audio (para conectar las bocinas), entrada de audio (para poder grabar audio en tu computadora y conector para el micrófono, están identificados por colores siendo el color rosa para la entrada del micrófono, el verde para la salida de audio (bocinas) y azul para la entrada de audio.

Conector IEEE 1394 o Firewire

Es un conector de alta velocidad, se usa principalmente para conectar cámaras de video y transferir video de alta calidad. Figura 1.3

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

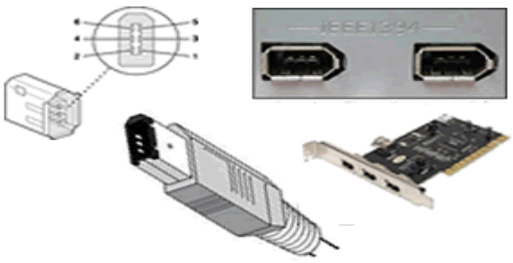


Figura 1.3 Conector IEEE

1.1.4 Instalación de NIC y módem

La conectividad a Internet requiere una tarjeta adaptadora, que puede ser un módem o NIC. Un módem, o modulador-demodulador, es un dispositivo que ofrece la computadora conectividad a una línea telefónica. El módem convierte (modula) los datos de una señal digital en una señal analógica compatible con una línea telefónica estándar. El módem en el extremo receptor demodula la señal, convirtiéndola nuevamente en una señal digital. Los módems pueden ser internos Figura 1.6 o bien, pueden conectarse externamente al computadora una interfaz de puerto serie ó USB Figura 1.7.

Figura 1.6 Modem Interno

Figura 1.7 Modem Externo

La instalación de una NIC, que proporciona la interfaz para un host a la red, es necesaria para cada dispositivo de la red. Se encuentran disponibles distintos tipos de NIC según la configuración del dispositivo específico. Las computadoras notebook pueden tener una interfaz incorporada o utilizar una tarjeta PCMCIA. La Figura 1.8 muestra una PCMCIA alámbrica, tarjetas de red inalámbricas, y un adaptador Ethernet USB (Universal Serial Bus /Bus Serial Universal). Los sistemas de escritorio pueden usar un adaptador de red interno Figura 1.9 llamado NIC, o un adaptador de red externo Figura 1.10 que se conecta a la red a través del puerto USB.

Figura 1.8 PMCIA alambrica

Figura 1.9 Adaptador red interno

Figura 1.10 Adaptador de red externo

Las situaciones que requieren la instalación de una NIC incluyen las siguientes:

- Instalación de una NIC en un PC que no tiene una.
- Reemplazo de una NIC defectuosa.
- Actualización desde una NIC de 10 Mbps a una NIC de 10/100/1000 Mbps.

1.1.7 Probar la conectividad con ping.

Ping es un programa básico que verifica que una dirección IP particular existe y puede aceptar solicitudes. El acrónimo computacional ping es la sigla para Packet Internet or Inter-Network Groper. El nombre se ajustó para coincidir el término usado en la jerga de submarinos para el sonido de un pulso de sonar que retorna desde un objeto sumergido.

El comando **ping** funciona enviando paquetes IP especiales, llamados datagramas de petición de eco ICMP (Internet Control Message Protocol/Protocolo de mensajes de control de Internet) 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** (figura 1.11) se utiliza para probar la función de transmisión/recepción de la NIC, la configuración TCP/IP y la conectividad de red. Se pueden ejecutar los siguientes tipos de comando ping:

• **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** *direcciónc IP dla computadora host*: Un ping a un PC host verifica la configuración de la dirección TCP/IP para el host local y la conectividad al host.

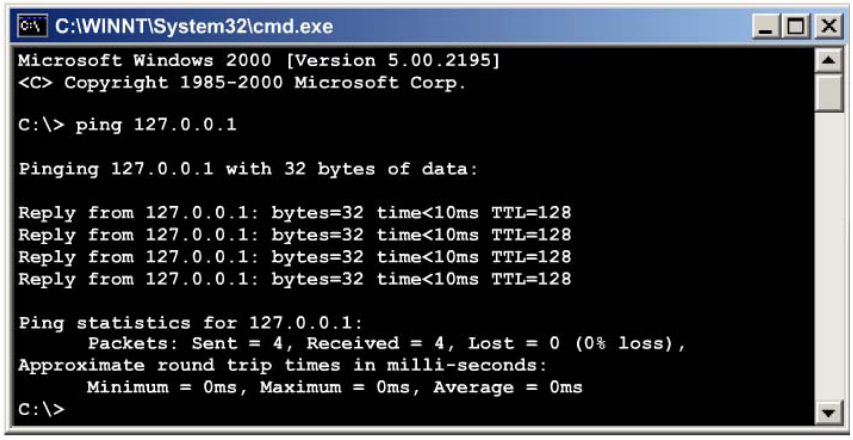


Figura 1.11 Comando ping

• **ping** *dirección IP de gateway por defecto*: Un ping al gateway por defecto verifica si se puede alcanzar el router 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.

Internet Explorer (IE): (Figura 1.13)

• Sólidamente integrado con otros productos de Microsoft
• Ocupa más espacio en disco
• Pone en pantalla archivos HTML, realiza transferencias de correo electrónico y de archivos y Desempeña otras funciones

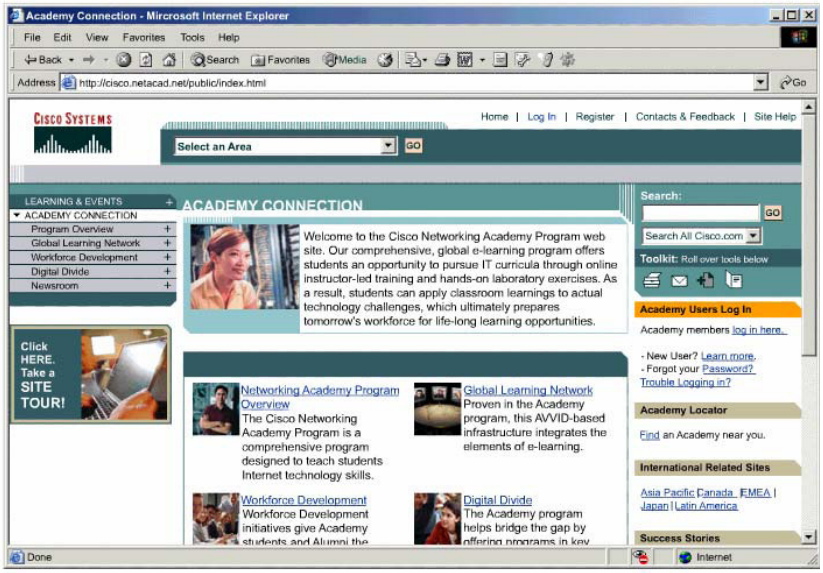


Figura 1.13 Navegador Internet Explore (IE)

También existen algunos tipos de archivos especiales, o propietarios, que no se pueden visualizar con los navegadores de Web estándar. Para ver estos archivos, el navegador debe configurarse para utilizar aplicaciones denominadas plug-in. Estas aplicaciones trabajan en conjunto con el navegador para iniciar el programa que se necesita para ver los archivos especiales.

• **Flash:** Reproduce archivos multimediales, creados con Macromedia Flash
• **Quicktime:** Reproduce archivos de video; creado por Apple
• **Real Player:** Reproduce archivos de audio

Para instalar el plug-in de Flash, siga estos pasos:

1. Vaya al sitio Web de Macromedia.
2. Descargue el archivo .exe. (flash32.exe)
3. Ejecute e instale en Netscape o Internet Explorer (IE).
4. Verifique la instalación y la correcta operación accediendo al sitio Web de la Academia Cisco

que están en este formato binario, o sea, de dos estados. Los unos y los ceros se usan para representar los dos estados posibles de un componente electrónico de un computadora. Se denominan dígitos binarios o bits. Los 1 representan el estado ENCENDIDO, y los 0 representan el estado APAGADO.

El Código americano normalizado para el intercambio de información (ASCII) es el código que se usa más a menudo para representar los datos alfanuméricos de un computadora. ASCII usa dígitos binarios (Tabla 1.3) para representar los símbolos que se escriben con el teclado. Cuando los computadoras envían estados de ENCENDIDO/APAGADO a través de una red, se usan ondas eléctricas, de luz o de radio para representar los unos y los ceros. Observe que cada carácter tiene un patrón exclusivo de ocho dígitos binarios asignados para representar al carácter.

Teclado	Códigos binarios
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000

Tabla 1.3 Códigos binario

Debido a que los computadoras están diseñados para funcionar con los interruptores ENCENDIDO/APAGADO, los dígitos y los números binarios les resultan naturales. Los seres humanos usan el sistema numérico decimal, que es relativamente simple en comparación con las largas series de unos y ceros que usan los computadoras. De modo que los números binarios dla computadora se deben convertir en números decimales.

A veces, los números binarios se deben convertir en números Hexadecimales (hex), lo que reduce una larga cadena de dígitos binarios a unos pocos caracteres hexadecimales. Esto hace que sea más fácil recordar y trabajar con los números.

1.2.2 Bits y bytes

Un número binario 0 puede estar representado por 0 voltios de electricidad (0 = 0 voltios).

Un número binario 1 puede estar representado por +5 voltios de electricidad (1 = +5 voltios).

Las computadoras están diseñados para usar agrupaciones de ocho bits. Esta agrupación de ocho bits se denomina byte. En un computadora, un byte representa una sola ubicación de almacenamiento direccionable. Estas ubicaciones de almacenamiento representan un valor o

El sistema numérico decimal se basa en potencias de 10. Cada posición de columna de un valor, pasando de derecha a izquierda, se multiplica por el número 10, que es el número de base, elevado a una potencia, que es el exponente. La potencia a la que se eleva ese 10 depende de su posición a la izquierda de la coma decimal. Cuando un número decimal se lee de derecha a izquierda, el primer número o el número que se ubica más a la derecha representa 100 (1), mientras que la segunda posición representa 101 (10 x 1= 10) La tercera posición representa 102 (10 x 10 =100). La séptima posición a la izquierda representa 106 (10 x 10 x 10 x 10 x 10 x 10 =1.000.000). Esto siempre funciona, sin importar la cantidad de columnas que tenga el número.

Ejemplo:

2134 = (2x103) + (1x102) + (3x101) + (4x100)

Hay un 4 en la posición correspondiente a las unidades, un 3 en la posición de las decenas, un 1 en la posición de las centenas y un 2 en la posición de los miles. Este ejemplo parece obvio cuando se usa el sistema numérico decimal. Es importante saber exactamente cómo funciona el sistema decimal, ya que este conocimiento permite entender los otros dos sistemas numéricos, el sistema numérico de Base 2 y el sistema numérico hexadecimal de Base 16. Estos sistemas usan los mismos métodos que el sistema decimal.

1.2.4 Sistema numérico de Base 2

Valor de posición	128 64 32 16 8 4 2 1
Base$^{\text{Exponente}}$	$2^7 = 128 \quad 2^3 = 8$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Cantidad de símbolos	10
Símbolos	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Razonamiento	Número típico de dedos igual a diez

Tabla 1.6 Sistema numérico base 2

1.2.5 Conversión de números decimales en números binarios de 8 bits

Existen varios métodos para convertir números decimales en números binarios. El diagrama de flujo que se muestra en la Figura 1.14 describe uno de los métodos. El proceso intenta descubrir cuáles de los valores de la potencia de 2 se suman para obtener el número decimal que se desea convertir en un número binario. Este es uno de varios métodos que se pueden usar. Es mejor seleccionar un método y practicarlo hasta obtener siempre la respuesta correcta.

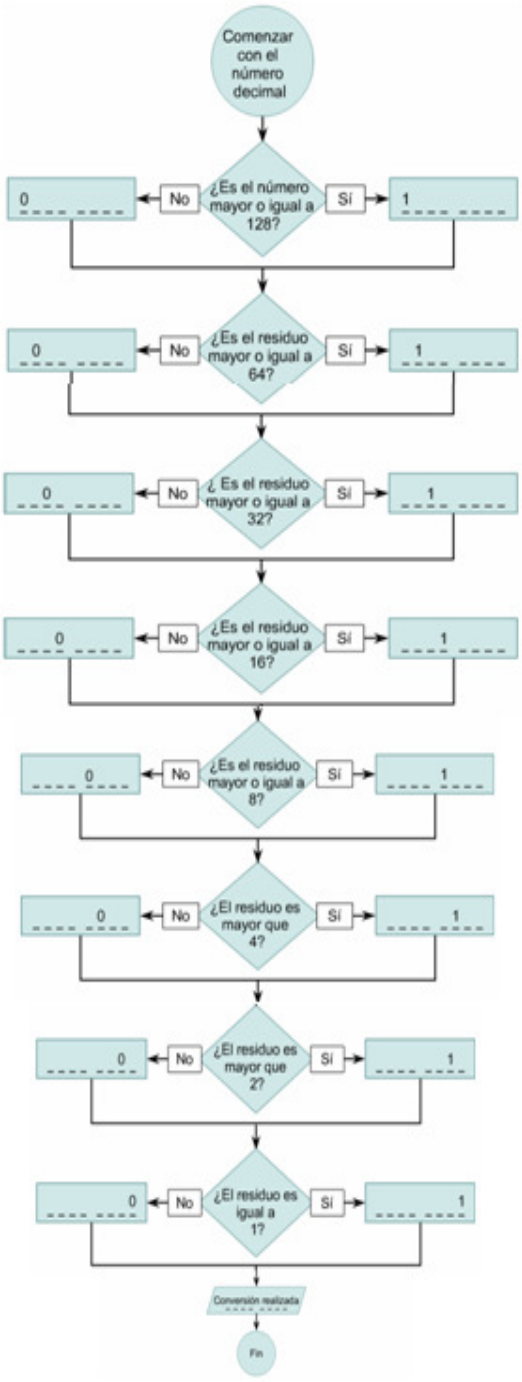


Figura 1.14 Diagrama de conversión de decimal a binario

Ejercicio de conversión

Utilice el ejemplo siguiente para convertir el número decimal 168 en un número binario.

• 128 entra en 168. De modo que el bit que se ubica más a la izquierda del número binario es un 1. 168 - 128 es igual a 40.

• 64 no entra en 40. De modo que el segundo bit desde la izquierda es un 0.

• 32 entra en 40. De modo que el tercer bit desde la izquierda es un 1. 40 - 32 es igual a 8.

• 16 no entra en 8, de modo que el cuarto bit desde la izquierda es un 0.

• 8 entra en 8. De modo que el quinto bit desde la izquierda es un 1. 8 - 8 es igual a 0. De modo que, los bits restantes hacia la derecha son todos ceros.

Resultado: Decimal 168 = 10101000

Para adquirir más práctica, trate de convertir el decimal 255 en un número binario. La respuesta correcta es 11111111.

1.2.7 Representación en notación decimal separada por puntos de cuatro octetos de números binarios de 32 bits

Actualmente, las direcciones que se asignan a los computadoras en Internet son números binarios de 32 bits. Para facilitar el trabajo con estas direcciones, el número binario de 32 bits se divide en una serie de números decimales. Para hacer esto, se divide el número binario en cuatro grupos de ocho dígitos binarios.

Luego, se convierte cada grupo de ocho bits, también denominados octetos, en su equivalente decimal.

Haga esta conversión exactamente como se indica en la explicación de conversión de binario a decimal que aparece en el siguiente cuadro. (Tabla 1.7)

Binario	11001000	01110010	00000110	00110011
Decimal	200 ·	114 ·	6 ·	51
	Numero punto	Numero punto	Numero punto	numero

Tabla 1.7 Conversión de binario a decimal

Una vez que está escrito, el número binario completo se representa como cuatro grupos de dígitos decimales separados por puntos. Esto se denomina notación decimal separada por puntos y ofrece una manera compacta y fácil de recordar para referirse a las direcciones de 32 bits. Esta representación se usará frecuentemente con posterioridad durante este curso, de modo que es necesario comprenderla bien.

Al realizar la conversión de binario a decimal separado por puntos, recuerde que cada grupo, que está formado por uno a tres dígitos decimales, representa un grupo de ocho dígitos binarios. Si el número decimal que se está convirtiendo es menor que 128, será necesario agregar ceros a la izquierda del número binario equivalente hasta que se alcance un total de ocho bits.

Al igual que los sistemas binario, decimal y el sistema hexadecimal se basa en el uso de símbolos, potencias y posiciones Tabla 1.9. Los símbolos que se usan en hexadecimal son los números 0 - 9 y las letras A, B, C, D, E y F. Tabla 1.10.

BINARIO	HEXADECIMAL	BINARIO	HEXADECIMAL
0000	0	1000	8
0001	1	1001	9
0010	2	1010	A
0011	3	1011	B
0100	4	1100	C
0101	5	1101	D
0110	6	1110	E
0111	7	1111	F

Tabla 1.9 Sistema numérico

BINARIO	HEXADECIMAL	DECIMAL	BINARIO	HEXADECIMAL	DECIMAL
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	A	10
0011	3	3	1011	B	11
0100	4	4	1100	C	12
0101	5	5	1101	D	13
0110	6	6	1110	E	14
0111	7	7	1111	F	15

Tabla 1.10 Símbolos del sistema Hexadecimal

Observe que todas las combinaciones posibles de cuatro dígitos binarios tienen sólo un símbolo hexadecimal, mientras que en el sistema decimal se utilizan dos. La razón por la que se utiliza el sistema hexadecimal es que dos dígitos hexadecimales, al contrario de lo que ocurre en el sistema decimal que requiere hasta cuatro dígitos, pueden representar eficientemente cualquier combinación de ocho dígitos binarios. Al permitir que se usen dos dígitos decimales para representar cuatro bits, el uso de decimales también puede provocar confusiones en la lectura de un valor. Por ejemplo, el número binario de ocho bits 01110011 sería 115 si se convirtiera en dígitos decimales. ¿Eso significa 11-5 ó 1-15? Si se usa 11-5, el número binario sería 10110101, que no es el número que se convirtió originalmente. Al usar hexadecimales, la conversión da como resultado 1F, que siempre se vuelve a convertir en 00011111.

La lógica booleana es una lógica binaria que permite que se realice una comparación entre dos números y que se genere una elección en base a esos dos números. Estas elecciones son las operaciones lógicas AND, OR y NOT. Con la excepción de NOT, las operaciones booleanas tienen la misma función. Aceptan dos números, que pueden ser 1 ó 0, y generan un resultado basado en la regla de lógica.

La operación NOT toma cualquier valor que se le presente, 0 ó 1, y lo invierte, Figura 1.17. El uno se transforma en cero, y el cero se transforma en uno. Recuerde que las compuertas lógicas son dispositivos electrónicos creados específicamente con este propósito. La regla de lógica que siguen es que cualquiera sea la entrada, el resultado será lo opuesto.

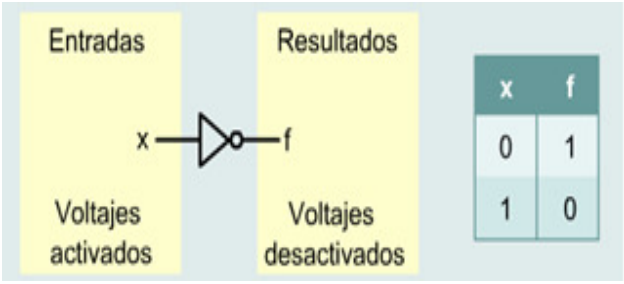


Figura 1.17 Operación NOT

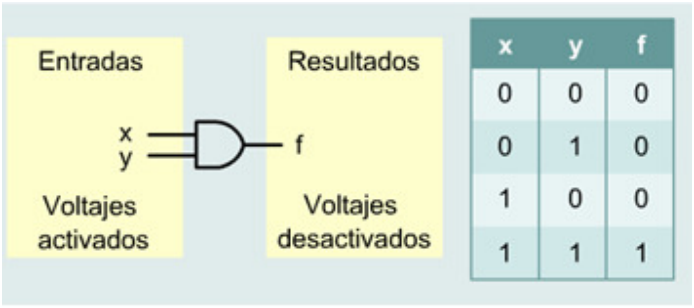


Figura 1.18 Operación AND

La operación AND toma dos valores de entrada. Si ambos valores son 1, la compuerta lógica genera un resultado de 1. De lo contrario, genera un 0 como resultado. Hay cuatro combinaciones de valores de entrada. Tres de estas combinaciones generan un 0, y sólo una combinación genera un 1. Figura 1.18.

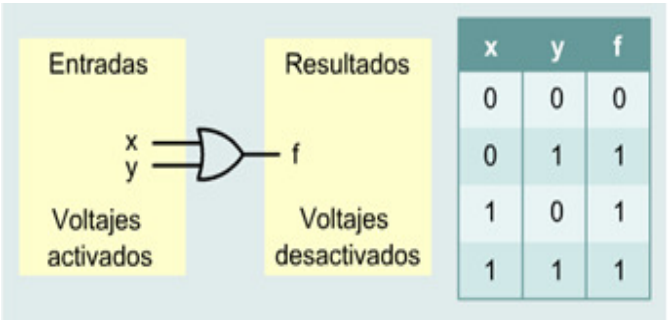


Figura 1.19 Operación OR

Figura 1.19. La operación OR también toma dos valores de entrada FIGURA 4. Si por lo menos uno de los valores de entrada es 1, el valor del resultado es 1. Nuevamente, hay cuatro combinaciones de valores de entrada. Esta vez tres combinaciones generan un resultado de 1 y la cuarta genera un resultado de 0

A continuación se suministran algunos ejemplos de máscaras de subred:

11111111000000000000000000000000 escrito en notación decimal separada por puntos es 255.0.0.0

O bien,

11111111111111110000000000000000 escrito en notación decimal separada por puntos es 255.255.0.0

En el primer ejemplo, los primeros ocho bits desde la izquierda representan la parte de red de la dirección y los últimos 24 bits representan la parte de host de la dirección. En el segundo ejemplo, los primeros 16 bits representan la parte de red de la dirección y los últimos 16 bits representan la parte de host de la dirección.

La conversión de la dirección IP 10.34.23.134 en números binarios daría como resultado lo siguiente:

00001010.00100010.00010111.10000110

La ejecución de una operación AND booleana de la dirección IP 10.34.23.134 y la máscara de subred 255.0.0.0 da como resultado la dirección de red de este host:

00001010.00100010.00010111.10000110
11111111.00000000.00000000.00000000
00001010.00000000.00000000.00000000

00001010.00100010.00010111.10000110
11111111.11111111.00000000.00000000
00001010.00100010.00000000.00000000

Convirtiendo el resultado a una notación decimal separada por puntos, se obtiene 10.0.0.0 que es la parte de red de la dirección IP cuando se utiliza la máscara 255.0.0.0. La ejecución de una operación AND booleana de la dirección IP 10.34.23.134 y la máscara de subred 255.255.0.0 da como resultado la dirección de red de este host:

Convirtiendo el resultado a una notación decimal separada por puntos, se obtiene 10.34.0.0 que es la parte de red de la dirección IP cuando se utiliza la máscara 255.255.0.0.

La siguiente es una ilustración breve del efecto que tiene la máscara de red sobre una dirección IP. La importancia de las máscaras se hará mucho más evidente a medida que se trabaje más con las direcciones IP. Por el momento, sólo hay que comprender el concepto de lo que es una máscara.

CAPITULO 2: Aspectos básicos de Redes

En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de las computadoras en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. (Figura 2.1)

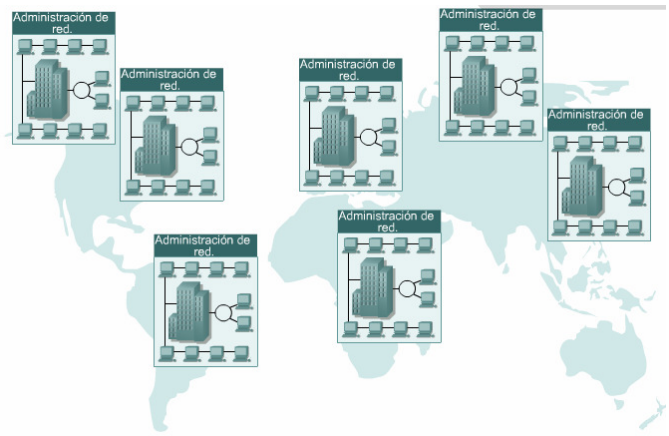


Figura 2.1 Sistema LAN

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra (Figura 2.2).

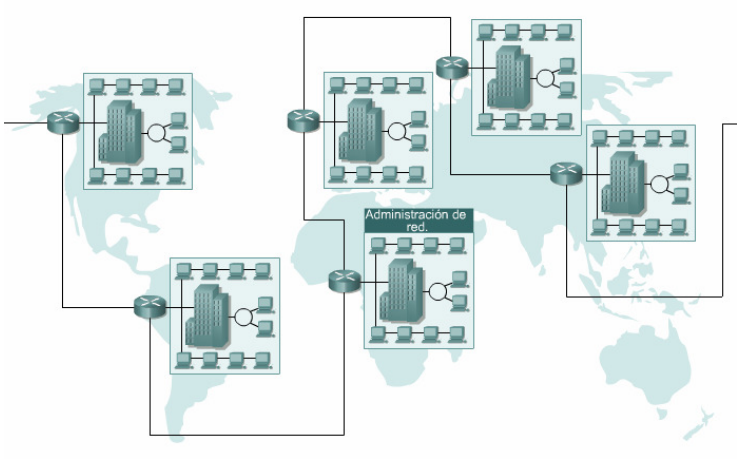


Figura 2.2 Transformación de la LAN

2.1.2 Historia de las redes informáticas

La historia de networking informática es compleja. Participaron en ella muchas personas de todo el mundo a lo largo de los últimos 35 años. Presentamos aquí una versión simplificada de la evolución de la Internet. Figura 2.4

Cronograma histórico de Internet	
Antes de 1900	Comunicaciones de larga distancia a través de mensajeros, jinetes, señales de humo, palomas mensajeras, telégrafo óptico, telégrafo eléctrico
Década de 1890	Bell inventa el teléfono; el servicio telefónico se expande rápidamente.
1901	Primera transmisión inalámbrica transatlántica de Marconi
Década de 1920	Radio AM
1939	Radio FM
Década de 1940	La Segunda Guerra Mundial provoca el auge de la radio y el desarrollo de las microondas.
1947	Shockley, Barden y Brittain inventan el transistor de estado sólido (semiconductor).
1948	Claude Shannon publica "Teoría matemática de la comunicación".
Década de 1950	Invención de los circuitos integrados.
1957	El Departamento de Defensa de Estados Unidos crea ARPA.
Década de 1960	Computadoras Mainframe
1962	Paul Baran de RAND trabaja en redes de "conmutación de paquetes".
1967	Larry Roberts publica el primer informe sobre ARPANET.
1969	ARPANET se establece en UCLA, UCSB, U-Utah y Stanford
Década de 1970	Uso generalizado de circuitos digitales integrados; advenimiento de las PC digitales.
1970	La Universidad de Hawaii desarrolla ALOHANET.
1972	Ray Tomlinson crea un programa de correo electrónico para enviar mensajes.
1973	Bob Kahn y Vint Cerf empiezan a trabajar en lo que posteriormente se transformaría en TCP/IP. La red ARPANET pasa a ser internacional con conexiones a la University College en Londres, Inglaterra, y el Establecimiento Real de Radar en Noruega.
1974	BBN abre Telnet, la primera versión comercial de la red ARPANET.
Década de 198	Uso generalizado de las computadoras personales y de las minicomputadoras basadas en Unix.
1981	Se asigna el término Internet a un conjunto de redes interconectadas.
1982	ISO lanza el modelo y los protocolos OSI; los protocolos desaparecen pero el modelo tiene gran influencia
1983	El Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) se transforma en el lenguaje universal de la Internet. ARPANET se divide en ARPANET y MILNET.
1984	Se funda Cisco Systems; comienza el desarrollo de gateways y routers. Se introduce el Servicio de Denominación de Dominio. La cantidad de hosts de Internet supera los 1000.
1986	Se crea NSFNET (con una velocidad de backbone 56 KBps).
1987	La cantidad de hosts de Internet supera los 10.000.
1988	DARPA forma el Equipo de Respuesta de Emergencia Informática (CERT).
1989	La cantidad de hosts de Internet supera los 100.000.
1990	ARPANET se transforma en la Internet.
1991	Se crea la World Wide Web (WWW). Tim Berners-Lee desarrolla el código para la WWW.
1992	Se organiza la Internet Society (ISOC). La cantidad de hosts de Internet supera el millón.
1993	Aparece Mosaic, el primer navegador de Web de base gráfica.
1994	Se presenta el navegador de Web Netscape Navigator.
1996	La cantidad de hosts de Internet supera los 10 millones. La Internet abarca a todo el planeta.
1997	Se crea el Registro Americano de Números de Internet (American Registry for Internet Numbers - ARIN). Internet 2 se pone en línea.
Fines de la década de 1990 hasta la actualidad	La cantidad de usuarios de Internet se duplica cada 6 meses (crecimiento exponencial).
1998	Cisco alcanza el 70% de las ventas a través de Internet, se lanzan las Academias de Networking.
1999	La red de backbone Internet 2 implanta IPv6. Las empresas más importantes se lanzan a la convergencia entre video, voz y datos.
2001	La cantidad de hosts de Internet supera los 110 millones.

Figura 2.4 Historia de la red Informática.

2.1.3 Dispositivos de Red

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 está compuesto por los dispositivos de usuario final.

Los dispositivos de usuario final incluyen las computadoras, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario. (Figura 2.5). El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación (Figura 2.6).

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. Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computadora, o puede ser un dispositivo periférico. (Figura 2.7) También se denomina adaptador de red. Las NIC para computadoras portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. Cada NIC individual tiene un código único, denominado dirección de control de acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Hablaremos más sobre la dirección MAC más adelante. Tal como su nombre lo indica, la NIC controla el acceso del host al medio.

Figura 2.5 Dispositivos de usuario

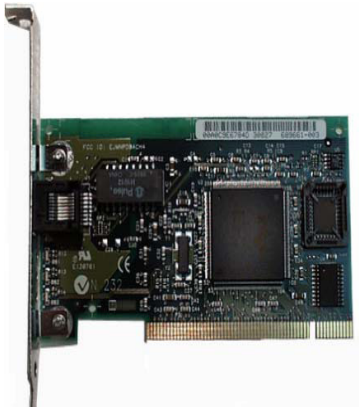


Figura 2.6 Dispositivos de red

Figura 2.7 Dispositivo periférico

Un repetidor (figura 2.10) es un dispositivo de red que se utiliza para regenerar una señal. Los repetidores regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. Un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

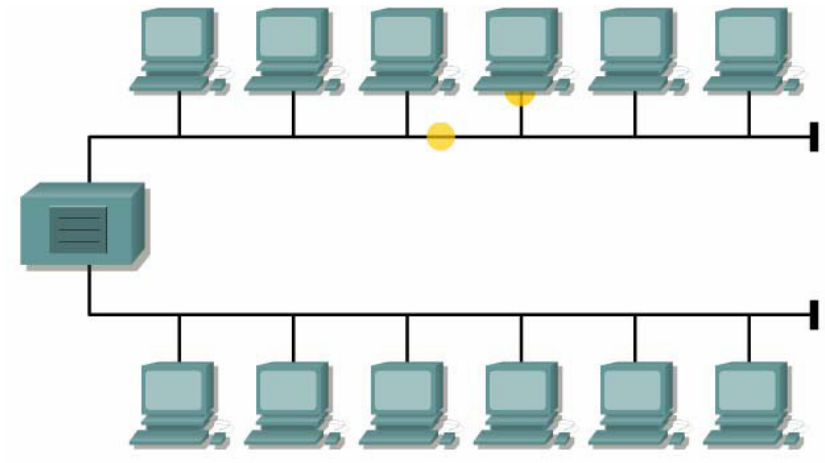


Figura 2.10 Dispositivo de Red (repetidor)

Los hubs concentran las conexiones. En otras palabras, permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

Los puentes convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos (Figura 2.11). Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

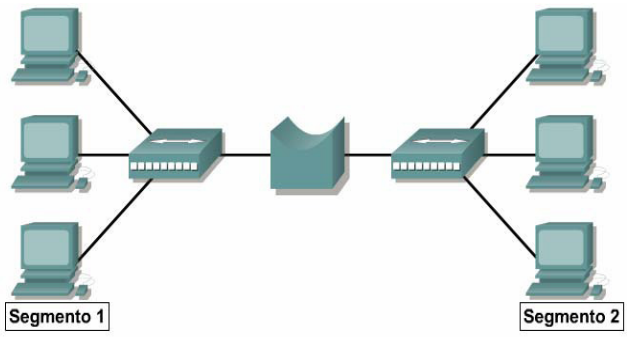


Figura 2.11 Dispositivo de Red (puente)

2.1.4 Topología de red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías físicas más comúnmente usadas son las siguientes: Figuras 2.14 y 2.15.

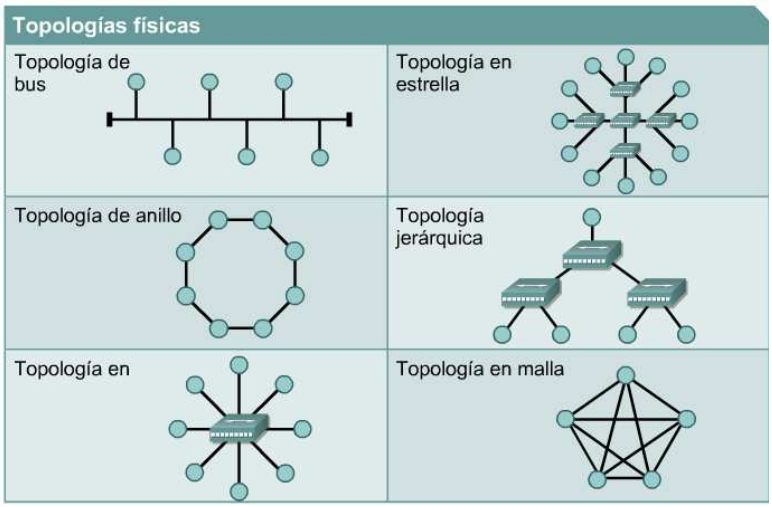


Figura 2.14 Topología física.

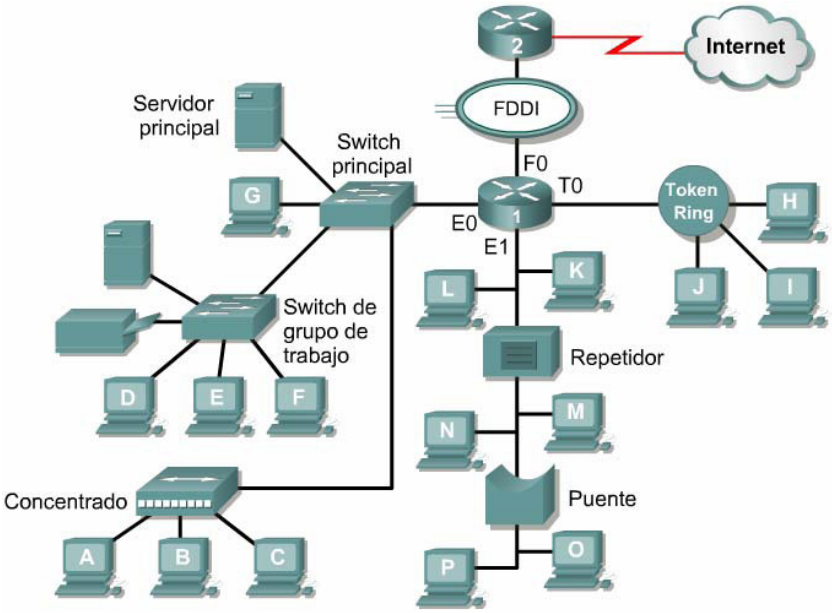


Figura 2.15 Topología lógica

2.1.5 Protocolos de red

Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí.

Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, la computadora no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computadora. Figura 16.

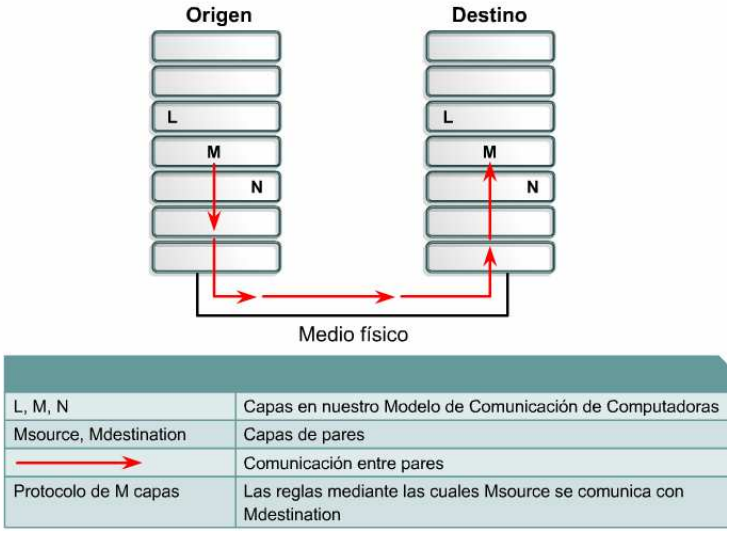


Figura 2.16 Protocolos de comunicación

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo las computadoras 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 organizaciones y comités.

Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

Algunas de las tecnologías comunes de WAN son:

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

2.1.8 Redes de área metropolitana (MAN)

La MAN (Figura 2.17) es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

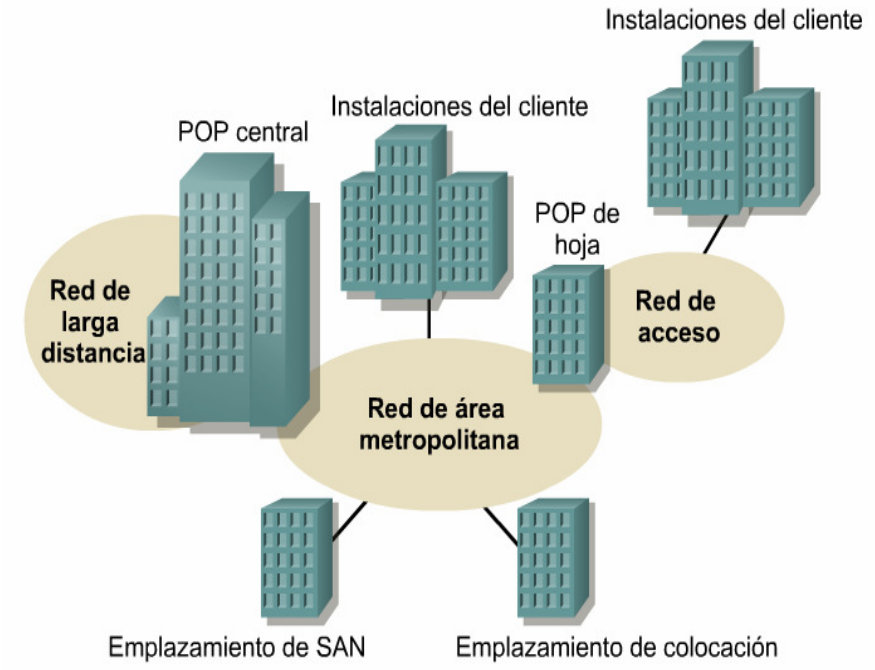


Figura 2.17 Red de área metropolitana (MAN)

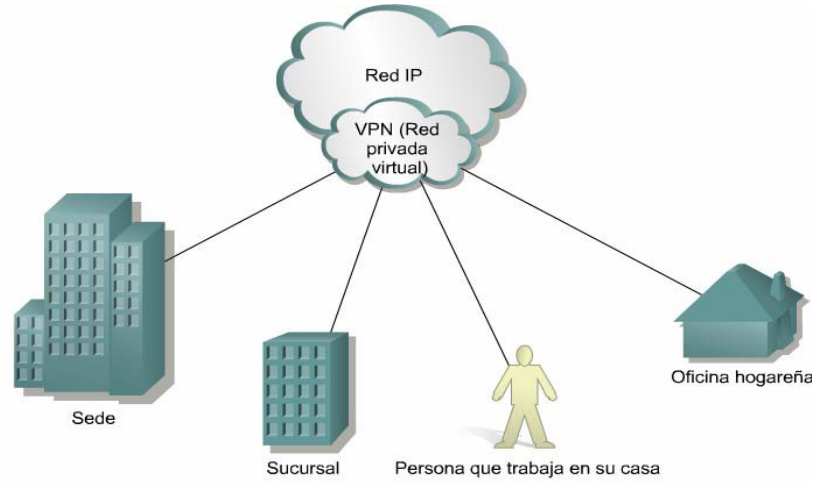
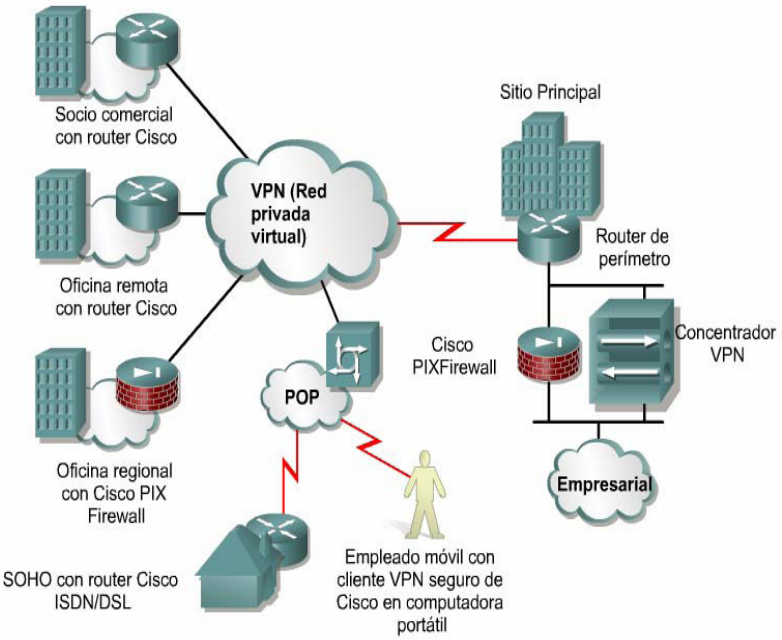


Figura 2.19 Red virtual privada (VPN)

2.1.11 Ventajas de las VPN



Los productos Cisco admiten la más reciente tecnología de VPN. La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la 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. (Figura 2.20).

Figura 2.20 Características de las VPN

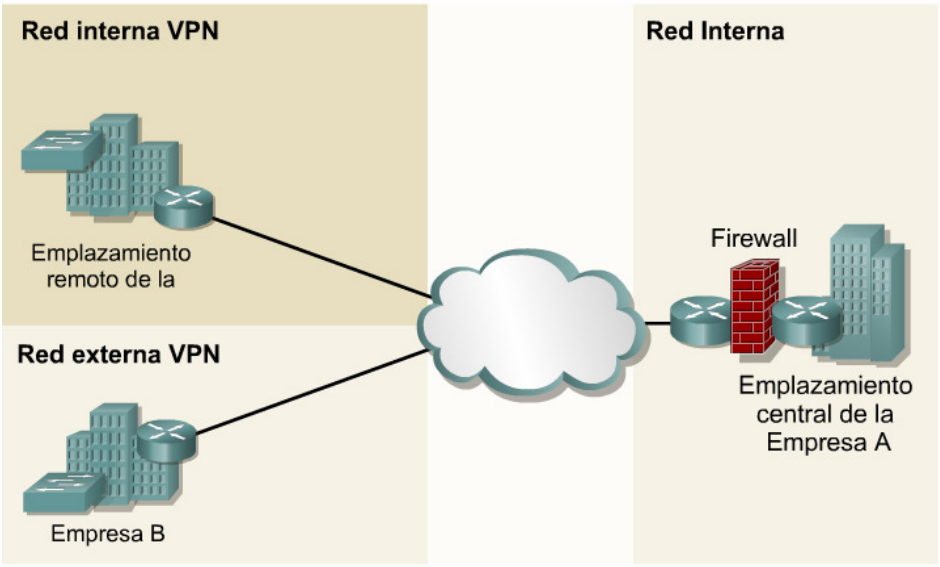


Figura 2.21 Red Interna y Externa.

2.2 Ancho de banda

2.2.1 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:

1. **El ancho de banda es finito.** En otras palabras, independientemente del medio que se utilice para construir la red, 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. Por ejemplo, el ancho de banda de un módem convencional está limitado a alrededor de 56 kpbs por las propiedades físicas de los cables telefónicos de par trenzado y por la tecnología de módems. No obstante, las tecnologías empleadas por DSL utilizan los mismos cables telefónicos de par trenzado, y sin embargo DSL ofrece un ancho de banda mucho mayor que los módems convencionales. Esto demuestra que a veces es difícil definir los límites impuestos por las mismas leyes de la física. La fibra óptica posee el potencial físico para proporcionar un ancho de banda prácticamente ilimitado. Aun así, el ancho de banda de la fibra óptica no se puede aprovechar en su totalidad, en tanto no se desarrollen tecnologías que aprovechen todo su potencial.

Figura 2.22 Red de tuberías

2. **El ancho de banda también puede compararse con la cantidad de carriles de una autopista** (Figura 2.23).

Una red de caminos sirve a cada ciudad o pueblo. Las grandes autopistas con muchos carriles se conectan a caminos más pequeños con menor cantidad de carriles. Estos caminos llevan a otros aún más pequeños y estrechos, que eventualmente desembocan en las entradas de las casas y las oficinas. Cuando hay poco tráfico en el sistema de autopistas, cada vehículo puede moverse con libertad. Al agregar más tráfico, cada vehículo se mueve con menor velocidad. Esto es particularmente verdadero en caminos con menor cantidad de carriles disponibles para la circulación del tráfico.

Eventualmente, a medida que se suma tráfico al sistema de autopistas, hasta aquéllas con varios carriles se congestionan y vuelven más lentas. Una red de datos se parece mucho al sistema de autopistas. Los paquetes de datos son comparables a los automóviles, y el ancho de banda es comparable a la cantidad de carriles en una autopista.

Cuando uno piensa en una red de datos en términos de un sistema de autopistas, es fácil ver cómo las conexiones con ancho de banda reducido pueden provocar congestiones de tráfico en toda la red.

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental del 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

Figura 2.24 Medición de ancho de banda

2.2.4 Limitaciones

Medios típicos	Ancho de banda máximo teórico	Distancia máxima teórica
Cable coaxial de 50 ohmios (Ethernet 10BASE2, Thinnet)	10 Mbps	185 m
Cable coaxial de 50 ohmios (Ethernet 10BASE5, Thicknet)	10 Mbps	500 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 10BASE-T)	10 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 100BASE-TX)	100 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 1000BASE-TX)	1000 Mbps	100 m
Fibra Óptica Multimodo (62.5/125µm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Fibra Óptica Multimodo (62.5/125µm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Fibra Óptica Multimodo(50/125µm) (1000BASE-SX Ethernet)	1000 Mbps	550 m

Figura 2.25 medios de networking y los límites de distancia y ancho de banda

El ancho de banda varía según el tipo de medio, además de las tecnologías LAN y WAN utilizadas. La física de los medios fundamenta algunas de las diferencias. 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.

Esto sólo podría suceder bajo las circunstancias más ideales. El concepto de tasa de transferencia nos ayudará a entender el motivo.

La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día, usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos.

Desafortunadamente, por varios motivos, la tasa de transferencia a menudo es mucho menor que el ancho de banda digital máximo posible del medio utilizado. A continuación se detallan algunos de los factores que determinan la tasa de transferencia:

• Dispositivos de internetworking
• Tipo de datos que se transfieren
• Topología de la red
• Cantidad de usuarios en la red
• Computadora del usuario
• Computadora servidor
• Estado de la alimentación

El ancho de banda teórico de una red es una consideración importante en el diseño de la red, porque el ancho de banda de la red jamás será mayor que los límites impuestos por los medios y las tecnologías de networking escogidos. No obstante, es igual de importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medir la tasa de transferencia regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de los usuarios de la red. Así la red se podrá ajustar en consecuencia.

2.2.6 Cálculo de la transferencia de datos

A menudo se convoca a los diseñadores y administradores de red para tomar decisiones con respecto al ancho de banda. Una decisión podría ser sobre la necesidad de incrementar el tamaño de la conexión WAN para agregar una nueva base de datos.

Otra decisión podría ser si el ancho de banda del actual backbone de la LAN alcanza para un programa de capacitación con video fluido. Las respuestas a este tipo de problemas no siempre son fáciles de hallar, pero se puede comenzar con un cálculo sencillo de transferencia de datos.

Aplicando la fórmula tiempo de transferencia = tamaño del archivo / ancho de banda (T=Tm/AB), un administrador de red puede estimar varios de los importantes componentes del rendimiento de una red. Si se conoce el tamaño típico de un archivo para una aplicación dada, al dividir el tamaño del archivo por el ancho de banda de la red, se obtiene una estimación del tiempo más rápido en el cual se puede transferir el archivo. (Figura 2.27)

A medida que las ondas de luz y sonido cambian de tamaño y forma, la señal eléctrica que transporta la transmisión cambia proporcionalmente. En otras palabras, las ondas electromagnéticas son análogas a las ondas de luz y sonido. El ancho de banda analógico se mide en función de la cantidad de espectro magnético ocupada por cada señal. La unidad de medida básica del ancho de banda analógico es el hercio (Hz), o ciclos por segundo.

Por lo general, se usan múltiplos de esta unidad de medida básica para anchos de banda analógicos, al igual que para los anchos de banda digitales. Las unidades de medida más comúnmente usadas son el kilohercio (KHz), el megahercio (MHz), y el gigahercio (GHz). Estas unidades se utilizan para describir las frecuencias de los teléfonos inalámbricos, que generalmente operan a 900 MHz o a 2,4 GHz. También son las unidades que se usan para describir las frecuencias de las redes inalámbricas 802.11a y 802.11b, que operan a 5GHz y 2,4 GHz. Figura 31.

Aunque las señales analógicas pueden transportar una amplia gama de información, presentan algunas desventajas significativas en comparación con las transmisiones digitales. La señal de video analógico que requiere una amplia margen de frecuencia para la transmisión, no puede ser comprimida en una banda más pequeña. Por lo tanto, si no se dispone del ancho de banda analógico necesario, no se puede enviar la señal.

En la señalización digital, toda la información se envía como bits, independientemente del tipo de información del cual se trate. Voz, video y datos se convierten todos en corrientes de bits al ser preparados para su transmisión a través de medios digitales.

Este tipo de transmisión confiere al ancho de banda digital una importante ventaja sobre el ancho de banda analógico. Es posible enviar cantidades ilimitadas de información a través de un canal digital con el ancho de banda más pequeño o más bajo.

Independientemente de lo que la información digital demore en llegar a su destino y reensamblarse, puede ser vista, oída, leída o procesada en su forma original.

Es importante comprender las diferencias y similitudes entre el ancho de banda digital y analógico. Ambos tipos de ancho de banda existen en el campo de la tecnología informática. No obstante, como este curso trata principalmente el networking digital, la expresión ‘ancho de banda’ se referirá al ancho de banda digital.

La conversación entre dos personas es un buen ejemplo para aplicar un enfoque en capas para analizar el flujo de información. En una conversación, cada persona que desea comunicarse comienza creando una idea. Luego se toma una decisión respecto de cómo comunicar la idea correctamente. Por ejemplo, una persona podría decidir si hablar, cantar o gritar, y qué idioma usar. Finalmente, la idea es comunicada. Por ejemplo, la persona crea el sonido que transmite el mensaje.

Se puede desglosar este proceso en distintas capas aplicables a todas las conversaciones. La capa superior es la idea que se comunicará. La capa intermedia es la decisión respecto de cómo se comunicará la idea. La capa inferior es la creación del sonido que transmitirá la comunicación.

El mismo método de división en capas explica cómo una red informática distribuye la información desde el origen al destino. Cuando los computadoras envían información a través de una red, todas las comunicaciones se generan en un origen y luego viajan a un destino. Figura 2.30.

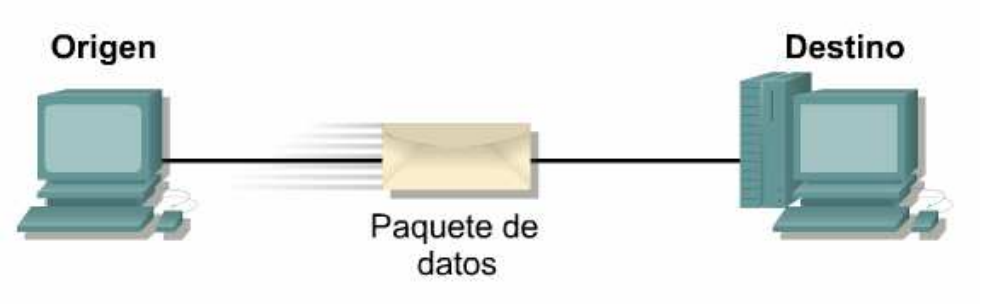


Figura 2.30. Método de división en capas

Generalmente, la información que se desplaza por una red recibe el nombre de datos o paquete. Un paquete es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación.

A medida que los datos atraviesan las capas, cada capa agrega información que posibilita una comunicación eficaz con su correspondiente capa en el otro computadora.

Los modelos OSI y TCP/IP se dividen en capas que explican cómo los datos se comunican de un computadora a otro.

Los modelos difieren en la cantidad y la función de las capas. No obstante, se puede usar cada modelo para ayudar a describir y brindar detalles sobre el flujo de información desde un origen a un destino.

2.3.3 Modelo OSI

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

El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controla todo uso de la tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes. Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes. El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial Figura 2.32.

Figura 2.32 Modelo OSI

Figura 2.36 Capa 4 Transporte

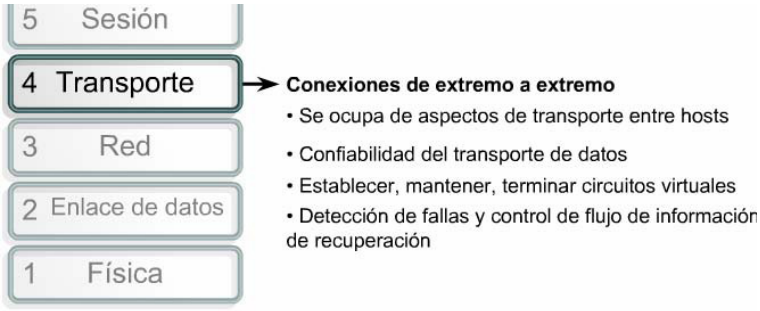


Figura 2.37 Capa 5 Sesión

Figura 2.38 Capa 6 Presentación

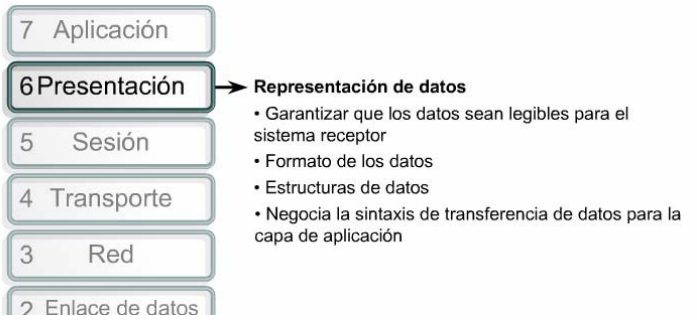


Figura 2.39 Capa 7 Aplicación

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le Puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función.

Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales. Después de que las Capas 7, 6 y 5 han agregado su información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de la Capa 4, se denomina segmento Figura 2.41.

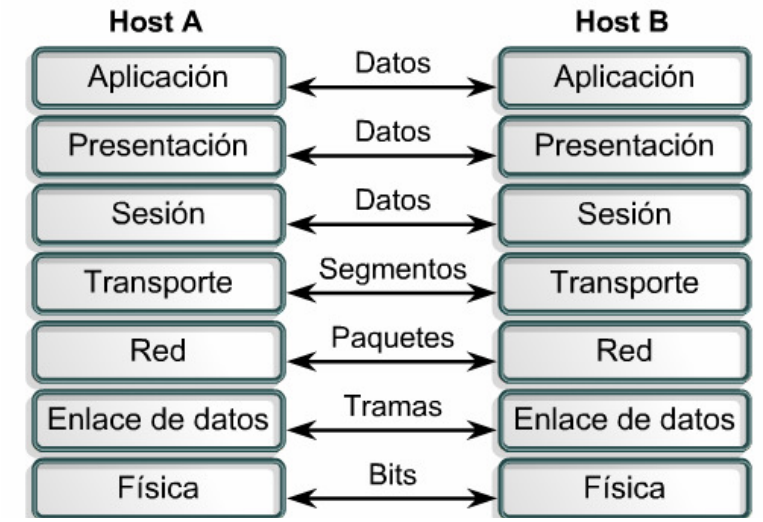


Figura 2.41 Segmento capa 4

La capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (la PDU de la Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como, por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de la Capa 2). El encabezado de trama contiene la información (por ejemplo, las direcciones físicas) que se requiere para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.

TCP es un protocolo orientado a conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a conexión no significa que existe un circuito entre los computadoras que se comunican. Significa que segmentos de la Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. El propósito de la capa Internet es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red. Los paquetes llegan a la red de destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. La relación entre IP y TCP es importante. Se puede pensar en el IP como el que indica el camino a los paquetes, en tanto que el TCP brinda un transporte seguro.

El nombre de la capa de acceso de red es muy amplio y se presta a confusión. También se conoce como la capa de host a red. Esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de networking, y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

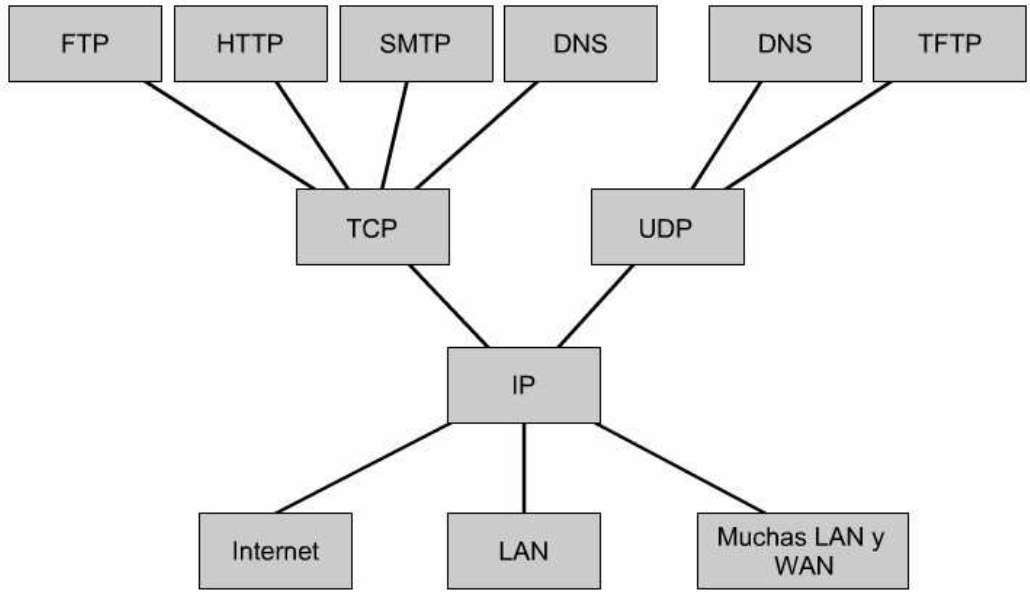


Figura 2.43 Protocolo de TCP/IP

La Figura 2.43 ilustra algunos de los protocolos comunes especificados por las capas del modelo de referencia TCP/IP.

Las similitudes incluyen:

• Ambos se dividen en capas.
• Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
• Ambos tienen capas de transporte y de red similares.
• Ambos modelos deben ser conocidos por los profesionales de networking.
• Ambos suponen que se conmutan paquetes.

Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

• TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.

• TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.

• TCP/IP parece ser más simple porque tiene menos capas.

• Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, este currículum utiliza el modelo OSI por los siguientes motivos:

• Es un estándar genérico, independiente de los protocolos.
• Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
• Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallas.

Los profesionales de networking tienen distintas opiniones con respecto al modelo que se debe usar. Dada la naturaleza de esta industria, es necesario familiarizarse con ambos. A lo largo de todo de esta guia se hará referencia a ambos modelos, el OSI y el TCP/IP. Se hará énfasis en lo siguiente:

• TCP como un protocolo de Capa 4 OSI
• IP como un protocolo de Capa 3 OSI
• Ethernet como una tecnología de Capa 2 y Capa 1

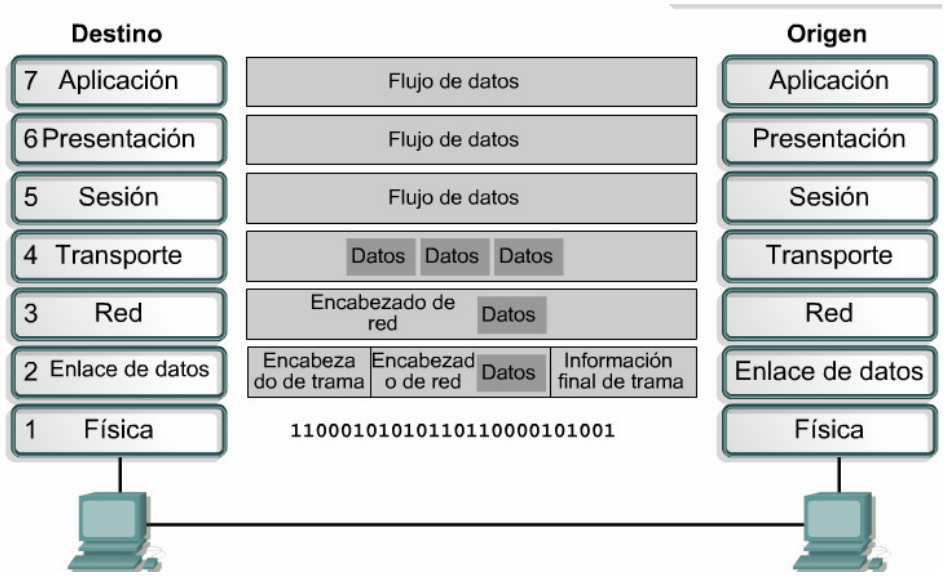


Figura 2.46. Encapsulamiento

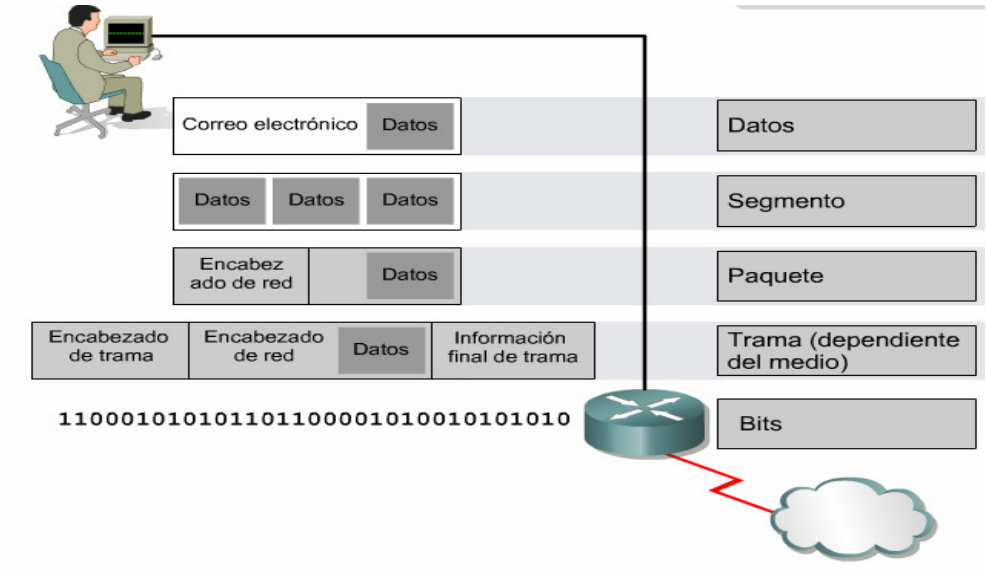


Figura 2.47 Empaquetamiento

Resumen

Se debe haber obtenido una comprensión adecuada de los siguientes puntos clave:

• Comprender que el ancho de banda es esencial en el estudio de networking
• El ancho de banda es finito, cuesta dinero, y su demanda aumenta a diario
• El empleo de analogías como el flujo de agua y de tráfico puede ayudar a entender el ancho de banda
• El ancho de banda se mide en bits por segundo, bps, kbps, Mbps o Gbps
• Las limitaciones del ancho de banda incluyen el tipo de medios utilizados, las tecnologías LAN y WAN, y el equipo de red
• La tasa de transferencia se refiere a la medida real del ancho de banda, que se ve afectada por factores que incluyen la cantidad de usuarios de red, los dispositivos de red, el tipo de datos, la computadora del usuario y el servidor.
• Se puede usar la fórmula T=Tm/AB (tiempo de transferencia = tamaño del archivo /ancho de banda) para calcular el tiempo de transmisión de datos.
• Comparación entre el ancho de banda analógico y digital
• Un enfoque dividido en capas resulta efectivo para analizar problemas
• La comunicación de red se describe mediante modelos divididos en capas
• Los modelos OSI y TCP/IP son los dos modelos más importantes de comunicación de red
• La Organización Internacional de Normalización desarrolló el modelo OSI para resolver los problemas de incompatibilidad entre redes.
• Las siete capas de OSI son aplicación, presentación, sesión, transporte, red, enlace de datos y física
• Las cuatro capas de TCP/IP son aplicación, transporte, internet y acceso a red
• La capa de aplicación de TCP/IP es equivalente a las capas de aplicación, presentación y sesión de OSI
• Las LAN y las WAN se desarrollaron en respuesta a necesidades informáticas comerciales y gubernamentales
• Los dispositivos fundamentales de networking son los hubs, puentes, switches y routers
• Las disposiciones topológicas físicas incluyen las de bus, de anillo, en estrella, en estrella extendida, jerárquica y de malla
• Una WAN consiste en una o más LAN que abarcan un área geográfica común.
• Una SAN brinda un mejor rendimiento del sistema, es escalable y tiene incorporada tolerancia al desastre
• Una VPN es una red privada construida dentro de una estructura de red pública
• Los tres principales tipos de VPN son acceso, red interna, y red externa
• Las redes internas están diseñadas para estar disponibles para usuarios con privilegios de acceso a la red interna de la organización.
• Las redes externas están diseñadas para distribuir aplicaciones y servicios basados en la red interna, utilizando un acceso extendido y seguro a usuarios o empresas externas.

3.1 Medios de cobre

3.1.1 Átomos y electrones

Toda la materia del universo está constituida por átomos. La Tabla Periódica de los Elementos enumera todos los tipos conocidos de átomos y sus propiedades, El átomo está compuesto de tres partículas básicas:

Electrones: Partículas con carga negativa que giran alrededor del núcleo
Protones: Partículas con carga positiva
Neutrones: Partículas sin carga (neutras).

Los protones y los neutrones se combinan en un pequeño grupo llamado núcleo.

Una de las leyes de la naturaleza, denominada Ley de la Fuerza Eléctrica de Coulomb, especifica que las cargas opuestas reaccionan entre sí con una fuerza que hace que se atraigan. Las cargas de igual polaridad reaccionan entre sí con una fuerza que hace que se repelan. Figura 3, En el caso de cargas opuestas y de igual polaridad, la fuerza aumenta a medida que las cargas se aproximan.

La fuerza es inversamente proporcional al cuadrado de la distancia de separación. Cuando las partículas se encuentran muy cerca una de la otra, la fuerza nuclear supera la fuerza eléctrica de repulsión y el núcleo se mantiene unido. Por esta razón, las partículas del núcleo no se separan.

Ley de Coulomb: Las cargas opuestas se atraen y las cargas iguales se repelen.

Modelo de Bohr: Los protones tienen cargas positivas y los electrones tienen cargas negativas. Hay más de 1 protón en el núcleo.

Se denomina electricidad estática a los electrones libres que permanecen en un lugar, sin moverse y con una carga negativa. Si estos electrones estáticos tienen la oportunidad de saltar hacia un conductor, se puede producir una descarga electrostática (ESD).

La ESD, aunque por lo general no es peligrosa para las personas, puede producir graves problemas en los equipos electrónicos sensibles. Una descarga electrostática puede dañar los chips o los datos dla computadora, o ambas cosas, de forma aleatoria.

Los circuitos lógicos de los chips de la computadora son sumamente sensibles a las descargas electrostáticas. Tenga cuidado al trabajar en el interior de un computadora, router u otro dispositivo.

Los conductores eléctricos, generalmente llamados simplemente conductores, son materiales que permiten que los electrones fluyen a través de ellos con gran facilidad. Pueden fluir con facilidad porque los electrones externos están unidos muy débilmente al núcleo y se liberan con facilidad. A temperatura ambiente, estos materiales poseen una gran cantidad de electrones libres que pueden proporcionar conducción. La aplicación de voltaje hace que los electrones libres se desplacen, lo que hace que la corriente fluya.

3.1.4 Corriente

La corriente eléctrica es el flujo de cargas creado cuando se mueven los electrones. En los circuitos eléctricos, la corriente se debe al flujo de electrones libres. Cuando se aplica voltaje, o presión eléctrica, y existe un camino para la corriente, los electrones se desplazan a lo largo del camino desde la terminal negativa hacia la terminal positiva. JLL a terminal negativa repele los electrones y la terminal positiva los atrae. La letra "I" representa la corriente. La unidad de medición de la corriente es el Amperio (A). Un Amperio se define como la cantidad de cargas por segundo que pasan por un punto a lo largo de un trayecto.

3.1.5 Circuitos

La corriente fluye en bucles cerrados denominados circuitos. Estos circuitos deben estar compuestos por materiales conductores y deben tener fuentes de voltaje. El voltaje hace que la corriente fluya, mientras que la resistencia y la impedancia se oponen a ella. La corriente consiste en electrones que fluyen alejándose de las terminales negativas y hacia las terminales positivas. El conocimiento de estos hechos permite controlar el flujo de la corriente.

La electricidad fluye naturalmente hacia la tierra cuando existe un recorrido. La corriente también fluye a lo largo de la ruta de menor resistencia. Si el cuerpo humano provee la ruta de menor resistencia, la corriente pasará a través de él. Cuando un artefacto eléctrico tiene un enchufe con tres espigas, una de las tres espigas sirve como conexión a tierra, o de cero voltios. La conexión a tierra proporciona una ruta conductora para que los electrones fluyan a tierra, ya que la resistencia que presenta el cuerpo suele ser mayor que la resistencia que opone la vía que conduce directamente a tierra. Por lo general, una conexión a tierra significa un nivel cero de voltios, al realizar las mediciones eléctricas. El voltaje se crea mediante la separación de las cargas, lo que significa que las mediciones de voltaje se deben realizar entre dos puntos.

La analogía del sistema de suministro de agua ayuda a explicar los conceptos de la electricidad. Cuanto mayor sea la altura del agua, y cuanto mayor sea la presión, mayor será el flujo de agua. La corriente de agua también depende del tamaño del espacio que debe atravesar. De igual manera, cuanto mayor sea el voltaje y cuanto mayor sea la presión eléctrica, más corriente se producirá. La corriente eléctrica se encuentra entonces con una resistencia que, al igual que el grifo, reduce el flujo.

Las líneas representan un conductor, que por lo general es un cable de cobre. Se puede considerar a un interruptor como dos extremos de un solo cable que se puede abrir o interrumpir para evitar que los electrones fluyan. Cuando los dos extremos están cerrados, fijos o puestos en cortocircuito, los electrones pueden fluir. Por último, la lamparilla presenta resistencia al flujo de electrones, lo que hace que liberen energía, en forma de luz. Los circuitos que participan en networking usan una versión mucho más compleja de este simple circuito. En los sistemas eléctricos de CA y CC, los electrones siempre fluyen desde una fuente con una carga negativa hacia una fuente con una carga positiva. Sin embargo, para que se produzca un flujo controlado de electrones, es necesario que haya un circuito completo. La Figura 3.2, muestra parte de un circuito eléctrico que lleva energía a un hogar u oficina.

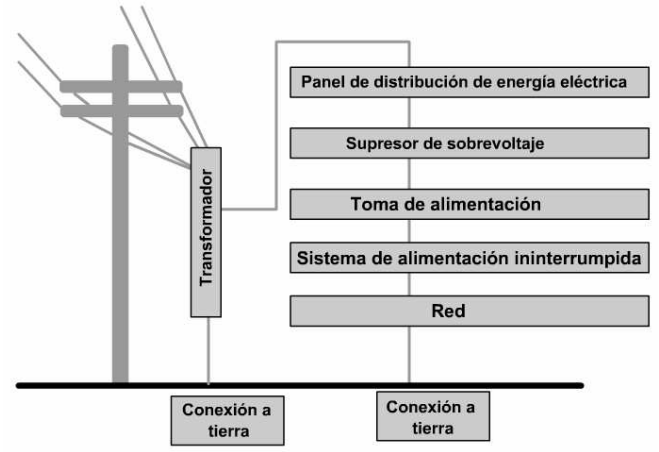


Figura 3.2 Circuito eléctrico común de un hogar u oficina

3.1.6 Especificaciones de cables

Los cables tienen distintas especificaciones y generan distintas expectativas acerca de su rendimiento.Algunos ejemplos de las especificaciones de Ethernet que están relacionadas con el tipo de cable son:

- 10BASE-T
- 10BASE5
- 10BASE2

10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.

10BASE5 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 5 representa la capacidad que tiene el cable para permitir que la señal recorra aproximadamente 500 metros antes de que la atenuación interfiera con la capacidad del receptor de interpretar correctamente la señal recibida.

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

3.1.8 Cable STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Figura 3.4, Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Según se especifica para el uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como, por ejemplo, el acoplamiento de par a par y la diafonía. El STP también reduce el ruido electrónico desde el exterior del cable, como, por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.

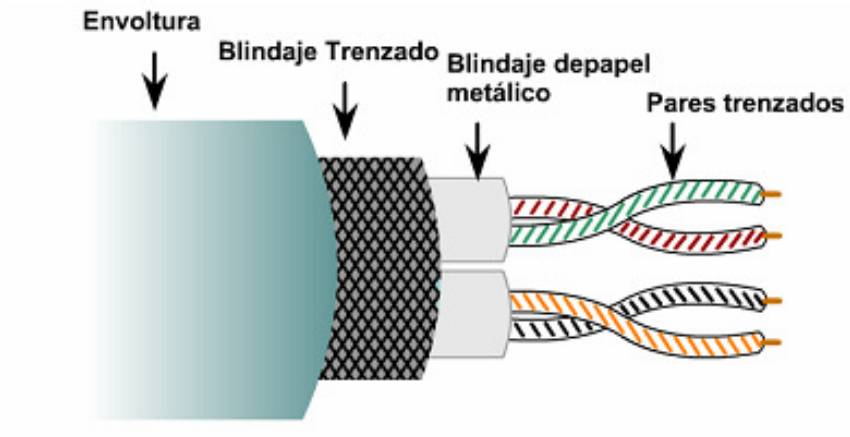


Figura 3.4 Cable de par trenzado

El cableado de par trenzado presenta ciertas desventajas. El cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios para networking y la distancia que puede abarcar la señal sin el uso de repetidores es menor para UTP que para los cables coaxiales y de fibra óptica. En una época, el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre.

Para que sea posible la comunicación, la señal transmitida por la fuente debe ser entendida por el destino. Esto es cierto tanto desde una perspectiva física como en el software. La señal transmitida necesita ser correctamente recibida por la conexión del circuito que está diseñada para recibir las señales. El pin de transmisión de la fuente debe conectarse en fin al pin receptor del destino. A continuación se presentan los tipos de conexiones de cable utilizadas entre dispositivos de internetwork.

En la Figura 3.6, un switch de LAN se conecta a un computadora. El cable que se conecta desde el puerto del switch al puerto de la NIC de la computadora recibe el nombre de cable directo. Figura 3.7.

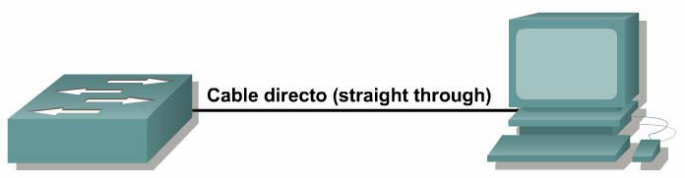


Figura 3.6 Switch de LAN

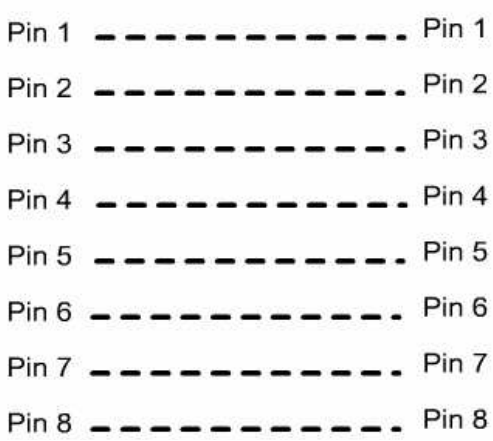


Figura 3.7 Configuración cable directo

Los cables están definidos por el tipo de conexiones o la disposición de pines, de un extremo al otro del cable. Ver imágenes 4, 6 y 8. Un técnico puede comparar ambos extremos de un mismo cable poniendo uno al lado del otro, siempre que todavía no se haya embutido el cable en la pared.

El técnico observa los colores de las dos conexiones RJ-45 colocando ambos extremos con el clip en la mano y la parte superior de ambos extremos del cable apuntando hacia afuera. En un cable directo, ambos extremos deberían tener idénticos patrones de color.

Al comparar los extremos de un cable de conexión cruzada, el color de los pins nº 1 y nº 2 aparecerán en el otro extremo en los pins nº 3 y nº 6, y viceversa. Esto ocurre porque los pins de transmisión y recepción se encuentran en ubicaciones diferentes. En un cable transpuesto, la combinación de colores de izquierda a derecha en un extremo debería ser exactamente opuesta a la combinación de colores del otro extremo. Figura 3.11.

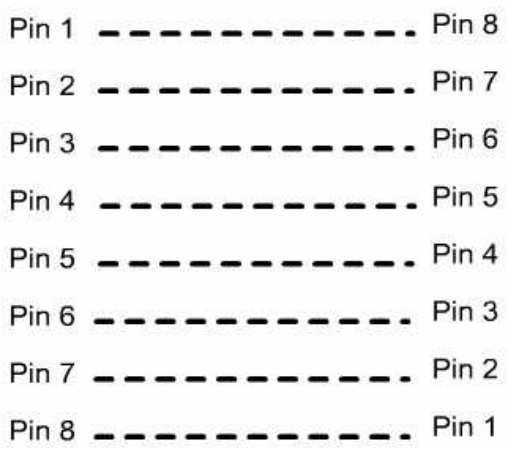


Figura 3.11. Configuracion cable transpuesto

3.2 Medios de fibra óptica

3.2.1 El espectro de fibra óptica

La luz que se utiliza en las redes de fibra óptica es un tipo de energía electromagnética. Cuando una carga eléctrica se mueve hacia adelante y hacia atrás, o se acelera, se produce un tipo de energía denominada energía electromagnética. Esta energía, en forma de ondas, puede viajar a través del vacío, el aire y algunos materiales como el vidrio. Una propiedad importante de toda onda de energía es la longitud de onda. Figura 3.12.

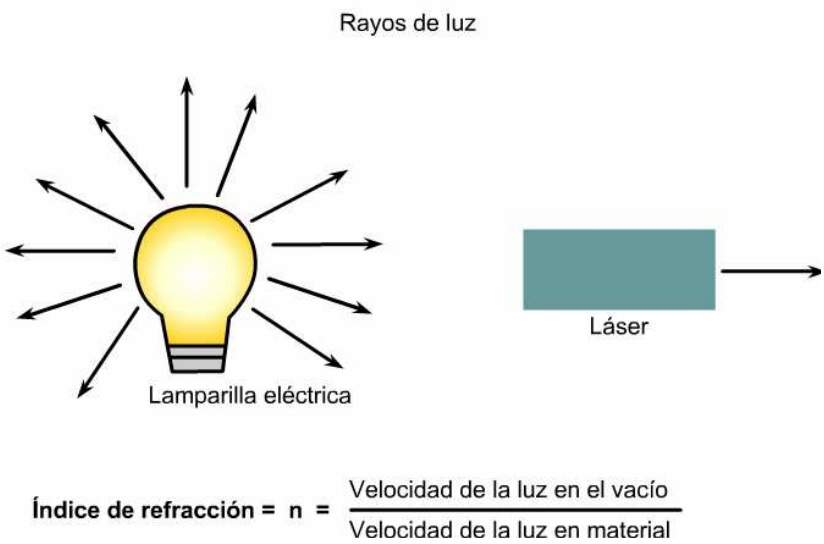


Figura 3.13 Modelo de Rayo de Luz

3.2.3 Reflexión

Cuando un rayo de luz (el rayo incidente) llega a la superficie brillante de una pieza plana de vidrio, se refleja parte de la energía de la luz del rayo. El ángulo que se forma entre el rayo incidente y una línea perpendicular a la superficie del vidrio, en el punto donde el rayo incidente toca la superficie del vidrio, recibe el nombre de ángulo de incidencia. Esta línea perpendicular recibe el nombre de normal. No es un rayo de luz sino una herramienta que permite la medición de los ángulos.

El ángulo que se forma entre el rayo reflejado y la normal recibe el nombre de ángulo de reflexión. La Ley de la Reflexión establece que el ángulo de reflexión de un rayo de luz es equivalente al ángulo de incidencia. En otras palabras, el ángulo en el que el rayo de luz toca una superficie reflectora determina el ángulo en el que se reflejará el rayo en la superficie.

3.2.4 Refracción

Cuando la luz toca el límite entre dos materiales transparentes, se divide en dos partes. Parte del rayo de luz se refleja a la primera sustancia, con un ángulo de reflexión equivalente al ángulo de incidencia. La energía restante del rayo de luz cruza el límite penetrando a la segunda sustancia.

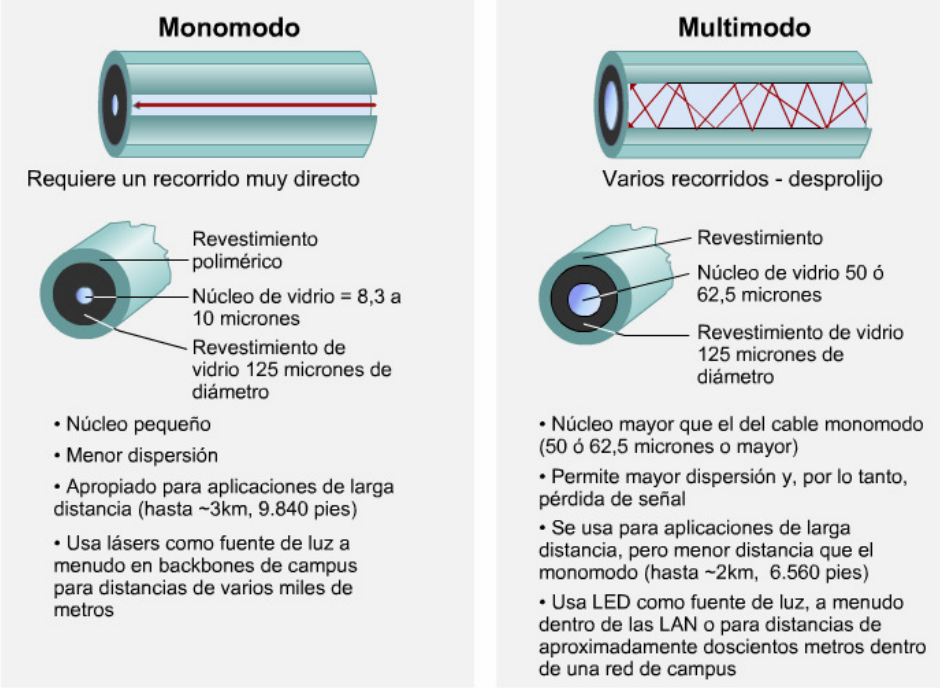


Figura 3.14 Fibra monomodo y multimodo

En general, un cable de fibra óptica se compone de cinco partes. Estas partes son: el núcleo, el revestimiento, un amortiguador, un material resistente y un revestimiento exterior. Figura 3.15

f

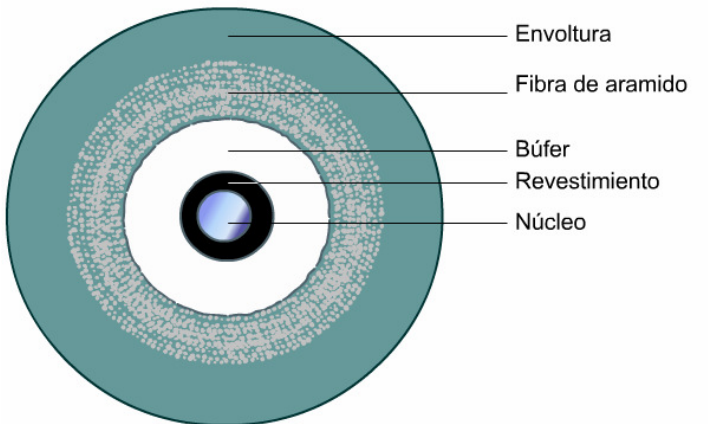


Figura 3.15 Partes de la fibra optica

El núcleo es el elemento que transmite la luz y se encuentra en el centro de la fibra óptica. Todas las señales luminosas viajan a través del núcleo. El núcleo es, en general, vidrio fabricado de una combinación de dióxido de silicio (sílice) y otros elementos.

3.3 Medios inalámbricos

3.3.1 Estándares y organizaciones de las LAN inalámbricas

Una comprensión de las reglamentaciones y los estándares que se aplican a la tecnología inalámbrica permitirá la interoperabilidad y cumplimiento de todas las redes existentes. Como en el caso de las redes cableadas, la IEEE es la principal generadora de estándares para las redes inalámbricas. Los estándares han sido creados en el marco de las reglamentaciones creadas por el Comité Federal de Comunicaciones (Federal Communications Commission - FCC).

La tecnología clave que contiene el estándar 802.11 es el Espectro de Dispersión de Secuencia Directa (DSSS). El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma. El siguiente estándar aprobado fue el 802.11b, que aumentó las capacidades de transmisión a 11 Mbps. Aunque las WLAN de DSSS podían interoperar con las WLAN de Espectro de Dispersión por Salto de Frecuencia (FHSS), se presentaron problemas que motivaron a los fabricantes a realizar cambios en el diseño.

En este caso, la tarea del IEEE fue simplemente crear un estándar que coincidiera con la solución del fabricante.

802.11b también recibe el nombre de Wi-Fi™ o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso.

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

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

Sólo la trama de datos es parecida las tramas 802.3. Las tramas inalámbricas y la 802.3 cargan 1500 bytes; sin embargo una trama de Ethernet no puede superar los 1518 bytes mientras que una trama inalámbrica puede alcanzar los 2346 bytes.

En general, el tamaño de la trama de WLAN se limita a 1518 bytes ya que se conecta, con mayor frecuencia, a una red cableada de Ethernet.

Debido a que la radiofrecuencia (RF) es un medio compartido, se pueden producir colisiones de la misma manera que se producen en un medio compartido cableado. La principal diferencia es que no existe un método por el que un nodo origen pueda detectar que ha ocurrido una colisión. Por eso, las WLAN utilizan Acceso Múltiple con Detección de Portadora/Carrier y Prevención de Colisiones (CSMA/CA). Es parecido al CSMA/CD de Ethernet.

Cuando un nodo fuente envía una trama, el nodo receptor devuelve un acuse de recibo positivo (ACK). Esto puede consumir un 50% del ancho de banda disponible. Este gasto, al combinarse con el del protocolo de prevención de colisiones reduce la tasa de transferencia real de datos a un máximo de 5,0 a 5,5 Mbps en una LAN inalámbrica 802.11b con una velocidad de 11 Mbps.

El rendimiento de la red también estará afectado por la potencia de la señal y por la degradación de la calidad de la señal debido a la distancia o interferencia. A medida que la señal se debilita, se puede invocar la Selección de Velocidad Adaptable (ARS). La unidad transmisora disminuirá la velocidad de transmisión de datos de 11 Mbps a 5,5 Mbps, de 5,5 Mbps a 2 Mbps o de 2 Mbps a 1 Mbps.

3.3.4 Autenticación y asociación

La autenticación de la WLAN se produce en la Capa 2. Es el proceso de autenticar el dispositivo no al usuario. Este es un punto fundamental a tener en cuenta con respecto a la seguridad, detección de fallas y administración general de una WLAN.

La autenticación puede ser un proceso nulo, como en el caso de un nuevo AP y NIC con las configuraciones por defecto en funcionamiento. El cliente envía una trama de petición de autenticación al AP y éste acepta o rechaza la trama. El cliente recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el AP para derivar la tarea de autenticación a un servidor de autenticación, que realizaría un proceso de credencial más exhaustivo.

La asociación que se realiza después de la autenticación, es el estado que permite que un cliente use los servicios del AP para transferir datos.

por otros. Al pasar de un material, como el aire, a otro material, como una pared de yeso, las ondas de radio se refractan. Las gotas de agua que se encuentran en el aire también dispersan y absorben las ondas de radio.

Es importante recordar estas cualidades de las ondas de radio cuando se está planificando una WLAN para un edificio o en un complejo de edificios. El proceso de evaluar la ubicación donde se instala una WLAN se conoce como inspección del sitio.

Como las señales de radio se debilitan a medida que se alejan del transmisor, el receptor también debe estar equipado con una antena. Cuando las ondas de radio llegan a la antena del receptor, se generan débiles corrientes eléctricas en ella. Estas corrientes eléctricas, producidas por las ondas de radio recibidas, son equivalentes a las corrientes que originalmente generaron las ondas de radio en la antena del transmisor. El receptor amplifica la fuerza de estas señales eléctricas débiles.

En un transmisor, las señales eléctricas (datos) que provienen de un computadora o de una LAN no son enviadas directamente a la antena del transmisor. En cambio, estas señales de datos son usadas para alterar una segunda señal potente llamada señal portadora.

3.3.6 Señales y ruido en una WLAN

En una red Ethernet cableada, a menudo, resulta simple diagnosticar la causa de una interferencia. Cuando se utiliza una tecnología de RF es necesario tener en cuenta varios tipos de interferencia.

La banda estrecha es lo opuesto a la tecnología de espectro de dispersión. Como su nombre lo indica, la banda estrecha no afecta al espectro de frecuencia de la señal inalámbrica. Una solución para el problema de interferencia en la banda estrecha consiste en simplemente cambiar el canal que utiliza el AP.

La interferencia en la banda completa afecta toda la gama del espectro. Las tecnologías Bluetooth™ saltan a través de los 2.4 GHz completo, varias veces por segundo y pueden producir una interferencia significativa en una red 802.11b. Es común ver carteles en instalaciones que usan redes inalámbricas solicitando que se desconecten todos los dispositivos Bluetooth™ antes de entrar. En los hogares y las oficinas, un dispositivo que, a menudo, se pasa por alto y que causa interferencia es el horno de microondas estándar. Un microondas que tenga una pérdida de tan sólo un watt que ingrese al espectro de RF puede causar una importante interferencia en la red. Los teléfonos inalámbricos que funcionan en el espectro de 2.4GHZ también pueden producir trastornos en la red.

Las condiciones climáticas, inclusive las más extremas, por lo general no afectan la señal de RF. Sin embargo, la niebla o condiciones de humedad elevada pueden afectar y afectan las redes inalámbricas. Los rayos también pueden cargar la atmósfera y alterar el trayecto de una señal transmitida.

Resumen

Se debe haber obtenido una comprensión adecuada de los siguientes puntos clave:

• Toda la materia está compuesta por átomos y los tres componentes de un átomo son: protones, neutrones y electrones. Los protones y los neutrones se encuentran en la parte central del átomo (núcleo).
• La descarga electrostática (ESD) puede causar graves problemas en equipos electrónicos sensibles.
• La atenuación se relaciona a la resistencia al flujo de electrones y la razón por la que una señal se degrada a medida que viaja.
• Las corrientes fluyen por bucles cerrados llamados circuitos, que deben estar compuestos por materiales conductores y deben contar con fuentes de voltaje.
• El multímetro se usa para medir voltaje, corriente, resistencia y otras mediciones eléctricas expresadas en forma numérica.
• Son tres los tipos de cable de cobre que se utilizan en networking. directo, de conexión cruzada y transpuesto.
• El cable coaxial consta de un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno único.
• El cable UTP es un medio de cuatro pares de hilos que se utiliza en varios tipos de redes.
• El cable STP combina las técnicas de blindaje, cancelación y trenzado de los hilos.
• La fibra óptica es un excelente medio de transmisión cuando es instalada, probada y mantenida correctamente.
• La energía de la luz, un tipo de onda de energía electromagnética, se utiliza para transmitir grandes cantidades de datos de forma segura a distancias relativamente grandes.
• La señal luminosa que transporta una fibra es producida por un transmisor que convierte una señal eléctrica en señal luminosa.
• El receptor convierte la luz que llega al otro extremo del cable nuevamente en la señal eléctrica original.
• Las fibras son utilizadas en pares para proporcionar comunicaciones full duplex.
• Los rayos de luz obedecen a las leyes de reflexión y refracción a medida que recorren la fibra de vidrio, lo que permite la fabricación de fibras con propiedad de reflexión interna total.
• La reflexión total interna hace que las señales luminosas permanezcan en el interior de la fibra, aunque la fibra no sea recta.
• La atenuación de la señal luminosa es un problema en el caso de cables largos, especialmente si secciones del cable están conectados a paneles de conexión o están empalmados.
• El cable y los conectores deben estar correctamente instalados y deben ser cuidadosamente probados con equipo óptico de prueba de alta calidad antes de ser utilizados.
• Los enlaces de cable deben ser verificados periódicamente con instrumentos ópticos de prueba de alta calidad para controlar si, de alguna manera, se ha deteriorado el enlace.
• Siempre se debe tener cuidado y proteger los ojos de las fuentes de luz intensa, como los láser.

CAPITULO 4: Prueba del cable

Las ondas sinoidales son representaciones gráficas de muchas ocurrencias naturales que varían regularmente a lo largo del tiempo. Algunos ejemplos de estas ocurrencias son la distancia de la tierra al sol, la distancia al suelo en un paseo en la Rueda de la Fortuna, y la hora a la que sale el sol. Debido a que las ondas sinoidales varían continuamente, son ejemplos de ondas analógicas. Las ondas rectangulares, al igual que las ondas sinoidales, son periódicas. Sin embargo, los gráficos de las ondas rectangulares no varían continuamente en el tiempo. La onda conserva un valor durante un tiempo, y luego cambia repentinamente a otro valor.

Este valor se conserva durante cierto tiempo, y luego cambia rápidamente de vuelta a su valor original. Las ondas rectangulares representan señales digitales, o pulsos. Como ocurre con todas las ondas, las ondas rectangulares se pueden describir en función de su amplitud, período y frecuencia. (Figura 4.2)

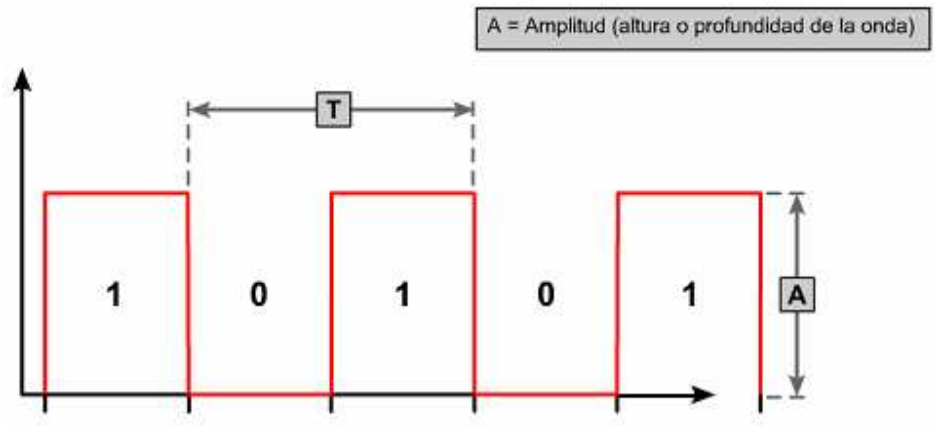


Figura 4.2 Ondas rectangulares

4.1.3 Exponentes y logaritmos

En de redes, existen tres sistemas numéricos importantes:

- **Base 2:** binario
- **Base 10:** decimal
- **Base 16:** hexadecimal

Recuerde que la base de un sistema numérico se refiere a la cantidad de diferentes símbolos que pueden ocupar una posición. Por ejemplo, en el sistema binario sólo existen dos valores posibles, 0 y 1. En el sistema decimal, existen diez valores posibles, los números del 0 al 9. En el sistema hexadecimal existen 16 valores posibles, los números del 0 al 9 y las letras de la A a la F.

Las variables representan los siguientes valores:

dB mide la pérdida o ganancia de la potencia de una onda. Los decibelios pueden ser valores negativos lo cual representaría una pérdida de potencia a medida que la onda viaja o un valor positivo para representar una ganancia en potencia si la señal es amplificada.

$\log_{10}$ implica que el número entre paréntesis se transformará usando la regla del logaritmo en base 10

P_{final} es la potencia suministrada, medida en vatios

P_{ref} es la potencia original, medida en vatios

V_{final} es el voltaje suministrado, medido en voltios

$V_{referencia}$ es el voltaje original, medido en voltios

La primera fórmula describe los decibelios en función de la potencia (P), y la segunda en función del voltaje (V). Normalmente, las ondas de luz en las fibras ópticas y las ondas de radio en el aire se miden usando la fórmula de potencia. Las ondas electromagnéticas en los cables de cobre se miden usando la fórmula del voltaje. Estas fórmulas poseen muchas cosas en común.

En la formula $dB = 10 \log_{10} (Pfinal / P_{ref})$, ingrese valores para dB y P_{ref} para encontrar la potencia entregada. Esta fórmula se puede utilizar para saber cuánta potencia queda en una onda de radio después de recorrer cierta distancia a través de diferentes materiales, y a través de varias etapas de sistemas electrónicos, como un radio. Para mayor exploración de los decibelios, intente con los siguientes ejemplos en las actividades flash:

Si la potencia de la fuente del laser original, o P_{ref} es siete microwatts (1×10^{-6} Watts), y la pérdida total de un enlace de fibra es 13 dB, cuanto potencia es entregada?

Si la pérdida total de un enlace de fibra óptica es 84 dB y la potencia fuente del láser original (P_{ref}) es un miliVatio (1×10^{-3} Vatios), ¿cuánta potencia se está suministrando?

Si se miden dos microVoltios (2×10^{-6} Voltios) en el extremo de un cable y el voltaje fuente es de un voltio, ¿cuál es la pérdida o ganancia en decibelios? ¿Este valor es positivo o negativo? ¿Este valor representa una ganancia o un pérdida de voltaje?

4.1.5 Visualización de señales en tiempo y frecuencia

Uno de los hechos más importantes de la era informática es que los datos que simbolizan caracteres, palabras, fotografías, videos o música se pueden representar electrónicamente mediante configuraciones de voltaje en cables y dispositivos electrónicos.

Los datos representados por estos patrones de voltaje se pueden convertir en ondas de luz o de radio, y luego de vuelta en ondas de voltaje. Piense en el ejemplo de un teléfono analógico.

Todos los sistemas de comunicación tienen cierta cantidad de ruido. Aunque es imposible eliminar el ruido, se pueden minimizar sus efectos si se comprenden los orígenes del ruido. Son muchas las posibles fuentes de ruido:

- Cables cercanos que transportan señales de datos
- Interferencia de radiofrecuencia (RFI), que es el ruido de otras señales que se están transmitiendo en las proximidades
- Interferencia electromagnética (EMI), que es el ruido que proviene de fuentes cercanas como motores y luces
- Ruido de láser en la transmisión o recepción de una señal óptica

El ruido que afecta por igual a todas las frecuencias de transmisión se denomina ruido blanco. El ruido que afecta únicamente a pequeños intervalos de frecuencia se denomina interferencia de banda estrecha. Al detectarse en un receptor de radio, el ruido blanco interfiere con todas las estaciones de radio. La interferencia de banda estrecha afectaría sólo a algunas estaciones cuyas frecuencias estuvieran próximas entre sí. Al detectarse en una LAN, el ruido blanco podría afectar a todas las transmisiones de datos, pero la interferencia de banda estrecha puede interferir quizás sólo en algunas señales.

4.1.8 Ancho de banda

El ancho de banda es un concepto sumamente importante para los sistemas de comunicación. Dos formas de considerar el ancho de banda, que resultan importantes en el estudio de las LAN, son el ancho de banda analógico y el ancho de banda digital. El ancho de banda analógico normalmente se refiere a la gama de frecuencias de un sistema electrónico analógico. El ancho de banda analógico se podría utilizar para describir la gama de frecuencias transmitidas por una estación de radio o un amplificador electrónico. La unidad de medida para el ancho de banda analógico es el hercio, al igual que la unidad de frecuencia. El ancho de banda digital mide la cantidad de información que puede fluir desde un punto hacia otro en un período de tiempo determinado. La unidad de medida fundamental para el ancho de banda digital es bits por segundo (bps). Como las LAN son capaces de velocidades de miles o millones de bits por segundo, la medida se expresa en kbps o Mbps. Los medios físicos, las tecnologías actuales y las leyes de la física limitan el ancho de banda.

4.2 Señales y ruido

4.2.1 Señales en cable de cobre y fibra óptica

En los cables de cobre, las señales de datos se representan por niveles de voltaje que representan unos y ceros binarios. Los niveles de voltaje se miden respecto de un nivel de referencia de cero voltios tanto en el transmisor como en el receptor. Este nivel de referencia se denomina tierra de señal.

El cable de fibra óptica se usa para transmitir señales de datos mediante una tecnología que aumenta y disminuye la intensidad de la luz para representar unos y ceros binarios. (Figura 4.6) La intensidad de una señal luminosa no disminuye tanto como la intensidad de una señal eléctrica sobre una tramo de igual longitud. Las señales ópticas no se ven afectadas por el ruido eléctrico, y no es necesario conectar la fibra óptica a tierra a menos que la chaqueta contenga un miembro de tensión metálico.

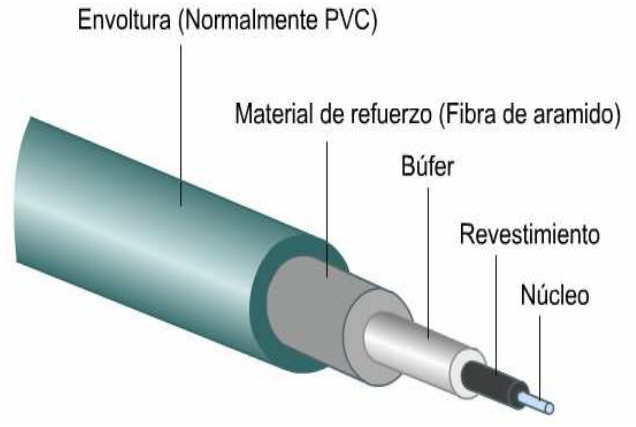


Figura 4.6 Cable de fibra óptica

4.2.2 Atenuación y pérdida de inserción en medios de cobre

La atenuación (Figura 4.7) es la disminución de la amplitud de una señal sobre la extensión de un enlace. Los cables muy largos y las frecuencias de señal muy elevadas contribuyen a una mayor atenuación de la señal. Por esta razón, la atenuación en un cable se mide con un analizador de cable, usando las frecuencias más elevadas que dicho cable admite. La atenuación se expresa en decibelios (dB) usando números negativos. Los valores negativos de dB más bajos indican un mejor rendimiento del enlace.

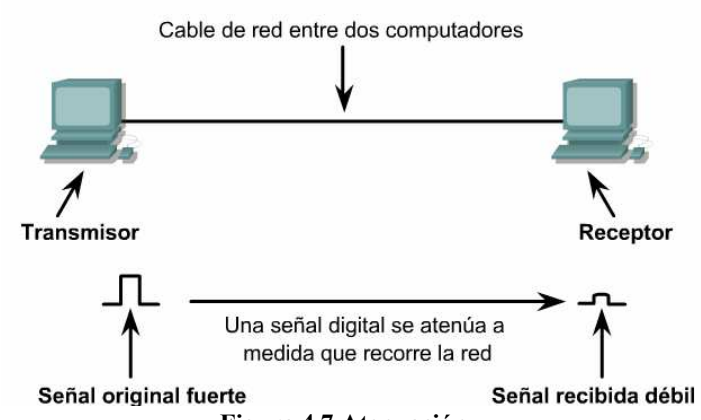


Figura 4.7 Atenuación

Trenzar un par de hilos en un cable, contribuye además a reducir la diafonía en las señales de datos o de ruido provenientes de un par de hilos adyacentes. En las categorías de UTP más altas, hacen falta más trenzas en cada par de hilos del cable para minimizar la diafonía a frecuencias de transmisión elevadas. Al colocar conectores en los extremos de los cables UTP, se debe minimizar el destrenzado de los pares de hilos para asegurar una comunicación confiable en la LAN.

4.2.4 Tipos de diafonía

Existen tres tipos distintos de diafonía: Figura 4.8

- Paradiafonía (NEXT)
- Telediafonía (FEXT)
- Paradiafonía de suma de potencia (PSNEXT)

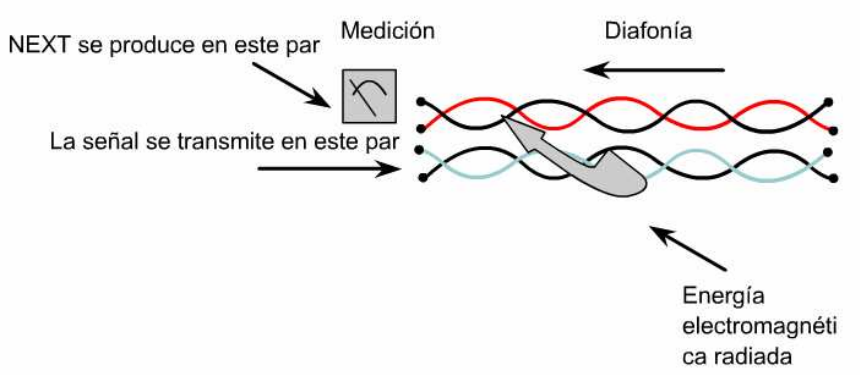


Figura 4.8 Diafonía

La paradiafonía (NEXT) se computa como la relación entre la amplitud de voltaje de la señal de prueba y la señal diafónica, medida en el mismo extremo del enlace. Esta diferencia se expresa como un valor negativo en decibelios (dB).

Los números negativos bajos indican más ruido, de la misma forma en que las temperaturas negativas bajas indican más calor. Tradicionalmente, los analizadores de cables no muestran el signo de menos que indica los valores NEXT negativos. Una lectura NEXT de 30 dB (que en realidad indica –30 dB) indica menos ruido NEXT y una señal más limpia que una lectura NEXT de 10 dB.

El NEXT se debe medir de par en par en un enlace UTP, y desde ambos extremos del enlace. Para acortar los tiempos de prueba, algunos instrumentos de prueba de cables permiten que el usuario pruebe el desempeño NEXT de un enlace utilizando un intervalo de frecuencia mayor que la especificada por el estándar TIA/EIA.

Algunos estándares de Ethernet, como 10BASE-T y 100 BASE-TX, reciben datos de un solo par de hilos en cada dirección. No obstante, para las tecnologías más recientes como 1000 BASE-T, que reciben datos simultáneamente desde múltiples pares en la misma dirección, las mediciones de suma de potencias son pruebas muy importantes.

4.2.5 Estándares de prueba de cables

El estándar TIA/EIA-568-B especifica diez pruebas que un cable de cobre debe pasar si ha de ser usado en una LAN Ethernet moderna de alta velocidad. Se deben probar todos los enlaces de cables a su calificación más alta aplicable a la categoría de cable que se está instalando.

Los diez parámetros de prueba principales que se deben verificar para que un enlace de cable cumpla con los estándares TIA/EIA son:

- Mapa de cableado
- Pérdida de inserción
- Paradiafonía (NEXT)
- Paradiafonía de suma de potencia (PSNEXT)
- Telediafonía del mismo nivel (ELFEXT)
- Telediafonía del mismo nivel de suma de potencia (PSELFEXT)
- Pérdida de retorno
- Retardo de propagación
- Longitud del cable
- Sesgo de retardo

El estándar de Ethernet especifica que cada pin de un conector RJ-45 debe tener una función particular. Figura 4.11. Una NIC (tarjeta de interfaz de red) transmite señales en los pins 1 y 2, y recibe señales en los pins 3 y 6. Los hilos de los cables UTP deben estar conectados a los correspondientes pins en cada extremo del cable.

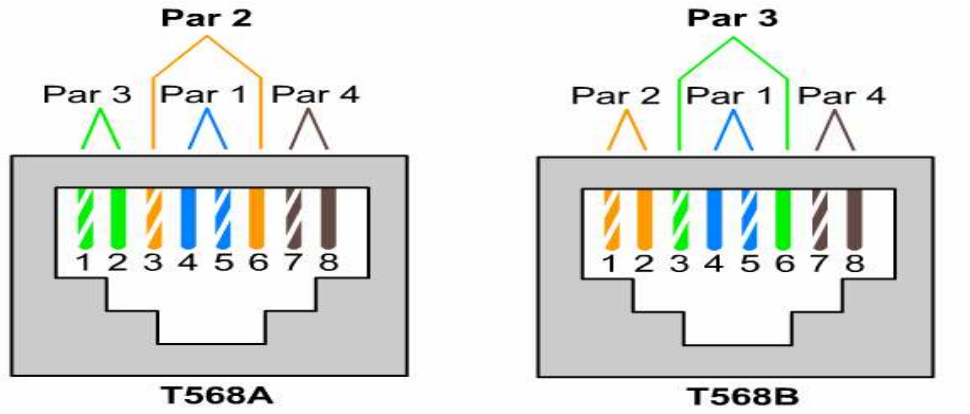


Figura 4.11 Estándar Ethernet T568A, T568B

Una falla de cableado de par dividido ocurre cuando un hilo de un par se cruza con un hilo de un par diferente. Esta mezcla entorpece el proceso de cancelación cruzada y hace el cable más susceptible a la diafonía y la interferencia. Observe con atención los números de pin en el gráfico para detectar la falla de cableado. Un par dividido da lugar a dos pares transmisores o receptores, cada uno con dos hilos no trenzados entre sí.

Las fallas de cableado de pares transpuestos se producen cuando un par de hilos se conecta a pins completamente diferentes en ambos extremos. Compare esto con un par invertido, en donde el mismo par de pins se usa en ambos extremos.

4.2.6 Otros parámetros de prueba

La combinación de los efectos de una señal atenuada con las discontinuidades en la impedancia en un enlace de comunicación se conoce como pérdida de inserción. La pérdida de inserción se mide en decibelios en el extremo más lejano del cable. El estándar TIA/EIA exige que un cable y sus conectores pasen una prueba de pérdida de inserción antes de que se pueda usar dicho cable en una LAN, como enlace para comunicaciones.

La diafonía se mide en cuatro pruebas distintas. Un analizador de cable mide la NEXT aplicando una señal de prueba a un par de cables y midiendo la amplitud de las señales de diafonía recibidas por los otros pares de cables. El valor NEXT, expresado en decibelios, se computa como la diferencia de amplitudes entre la señal de prueba y la señal diafónica medidas en el mismo extremo del cable.

Recuerde, como el número de decibelios que muestra el analizador de cables es un número negativo, cuanto mayor sea ese número, menor será la NEXT en ese par de hilos. Tal como se había mencionado previamente, la prueba PSNEXT es en realidad un cálculo basado en los efectos NEXT combinados.

La prueba de telediafonía de igual nivel (ELFEXT) mide FEXT. La ELFEXT de par a par se expresa en dB como la diferencia entre la pérdida FEXT medida y la pérdida de inserción del par de hilos cuya señal está perturbada por la FEXT. La ELFEXT es una medición importante en redes Ethernet que usan tecnología 1000BASE-T. La telediafonía de igual nivel de suma de potencia (PSELFEXT) es el efecto combinado de ELFEXT de todos los pares de hilos

La pérdida de retorno es una medida en decibelios de los reflejos causados por discontinuidades en la impedancia en todos los puntos del enlace. Recuerde que el mayor impacto de la pérdida de retorno no es la pérdida de la potencia de señal.

El problema significativo es que los ecos de señal producidos por los reflejos originados en discontinuidades en la impedancia, afectarán al receptor a diferentes intervalos, causando la fluctuación de las señales.

Se debe usar un instrumento de certificación para asegurar que se pasan todas las pruebas para ser considerado dentro de los estándares. Estas pruebas garantizan que los enlaces de cable funcionarán de manera confiable a velocidades y frecuencias altas.

4.2.8 Prueba de fibra óptica

Un enlace de fibra óptica consta de dos fibras de vidrio separadas que funcionan como recorridos de datos independientes. Una fibra transporta las señales transmitidas en una dirección, en tanto que la otra transporta señales en dirección contraria. Cada fibra de vidrio está cubierta por un revestimiento que no permite el paso de la luz, por lo tanto los cables de fibra óptica no presentan problemas de diafonía. La interferencia eléctrica desde el exterior, o ruido, no afecta los cableados de fibra óptica. Se produce atenuación en los enlaces de fibra óptica, pero en menor medida que en los cables de cobre.

Los enlaces de fibra óptica están sujetos al equivalente óptico de la discontinuidad en la impedancia de UTP. Cuando la luz encuentra una discontinuidad óptica, tal como una impureza en el vidrio o una microfractura, parte de la señal de luz se refleja en la dirección opuesta. Esto significa que sólo una fracción de la señal de luz original continuará su recorrido por la fibra en su camino hacia el receptor.

Como consecuencia, el receptor recibe una energía luminosa menor, lo que dificulta el reconocimiento de la señal. Al igual que con el cable UTP, los conectores mal instalados son la principal causa del reflejo de luz y de la pérdida de potencia de la señal en las fibras ópticas.

Como el ruido ya no es un problema en las transmisiones por fibra óptica, el problema principal en un enlace de fibra óptica es la potencia con la que una señal luminosa llega hasta el receptor. Si la atenuación debilita la señal luminosa en el receptor, se producirán errores en los datos. Las pruebas de cables de fibra óptica implican principalmente recorrer la fibra con una luz y medir si la cantidad de luz que llega al receptor es suficiente.

4.2.9 Un nuevo estándar

El 20 de junio de 2002, se publicó el suplemento para la Categoría 6 (o Cat 6) en el estándar TIA-568. El título oficial del estándar es ANSI/TIA/EIA-568-B.2-1. Este nuevo estándar especifica el conjunto original de parámetros de rendimiento que deben ser probados para los cableados Ethernet, así como también los puntajes de aprobación para cada una de estas pruebas. Los cables certificados como Cat 6 deben aprobar las diez pruebas.

Aunque las pruebas de Cat 6 son esencialmente las mismas que las especificadas por el estándar Cat 5, el cable Cat 6 debe aprobar las pruebas con puntajes mayores para lograr la certificación. Un cable Cat 6 debe tener la capacidad de transportar frecuencias de hasta 250 MHz y debe presentar niveles inferiores de diafonía y pérdida de retorno.

Resumen

Se debe haber obtenido una comprensión adecuada de los siguientes puntos clave:

• Las ondas son energía que se desplaza de un lugar a otro, y son generadas por disturbios. Todas las ondas poseen atributos similares, como amplitud, período y frecuencia.
• Las ondas sinoidales son funciones periódicas de variación continua. Las señales analógicas son parecidas a las ondas sinoidales.
• Las ondas rectangulares son funciones periódicas cuyos valores permanecen constantes durante un período de tiempo y luego cambian en forma abrupta. Las señales digitales son parecidas a las ondas rectangulares.
• Los exponentes se utilizan para representar cifras muy grandes o muy pequeñas. La base de un número elevado a un exponente positivo equivale a la base multiplicada por sí misma tantas veces como lo indica el exponente. Por ejemplo, 103 = 10x10x10 = 1000.
• Los logaritmos son similares a los exponentes. Un logaritmo en base 10 de un número equivale al exponente al que habría que elevar 10 para que equivaliera a dicho número. Por ejemplo, log10 1000 = 3 porque 103= 1000.
• Los decibelios son las mediciones de una ganancia o una pérdida de potencia de una señal. Los valores negativos representan pérdidas, y los valores positivos representan ganancias.
• El análisis de dominio temporal es la graficación del voltaje o corriente respecto del tiempo, usando un osciloscopio. El análisis de dominio de frecuencia es la graficación del voltaje o potencia respecto de la frecuencia, usando un analizador de espectro.
• Las señales indeseables en un sistema de comunicaciones se denominan ruido. El ruido se genera desde otros cables, RFI y EMI. El ruido blanco afecta a todas las frecuencias, en tanto que la interferencia de banda estrecha afecta únicamente a un cierto subconjunto de frecuencias.
• El ancho de banda analógico es el intervalo de frecuencias asociado con ciertas transmisiones analógicas, como las de televisión o radio FM.
• La mayoría de los problemas de las LAN ocurren en la capa física. La única forma de evitar o diagnosticar muchos de estos problemas es mediante el uso de analizadores de cables.
• Las instalaciones de cable adecuadas, que observan los estándares, aumentan la confiabilidad y el rendimiento de las LAN.
• Los medios de cobre vienen en forma blindada y no blindada. El cable no blindado es más susceptible al ruido.
• La degradación de una señal depende de varios factores, tales como ruido, atenuación, desacoplamiento en la impedancia y diferentes tipos de diafonía. Estos factores reducen el rendimiento de la red.
• El estándar TIA/EIA-568-B especifica diez pruebas que un cable de cobre debe pasar si ha de ser usado en una LAN Ethernet moderna de alta velocidad.
• La fibra óptica también se debe probar conforme a los estándares de redes.
• Un cable de Categoría 6 debe cumplir con estándares de frecuencia más rigurosos que un cable de Categoría 5.

5.1 Cableado LAN

5.1.1 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. Figura 5.1

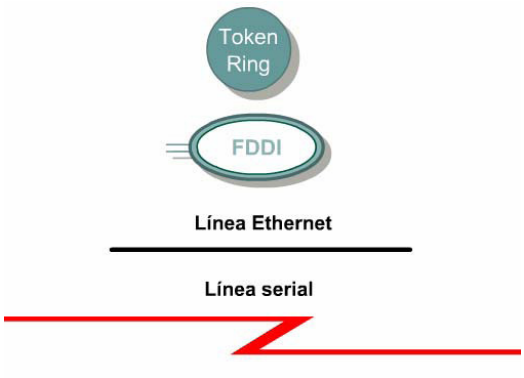


Figura 5.1 Representación de símbolos

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 Cat 5e.

Muchas topologías son compatibles con las LAN así como muchos diferentes medios físicos. La Figura 5.2, muestra un subconjunto de implementaciones de la capa física que se pueden implantar para su uso con Ethernet.

Por lo general, las tecnologías Ethernet se pueden utilizar en redes de campus 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.
- 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 campus y evitar los cuellos de botella, se puede utilizar Fast Ethernet para conectar servidores empresariales.
- A medida que se tornen económicos, se debe implementar Fast Ethernet o Gigabit Ethernet entre dispositivos backbone.

5.1.3 Medios de Ethernet y requisitos de conector

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 la Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (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).

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. Como se ve en la 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.

Identifique la categoría de cableado EIA/TIA (Figura 5.4) 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 de conexión directa (straight-through) o de conexión cruzada (crossover).

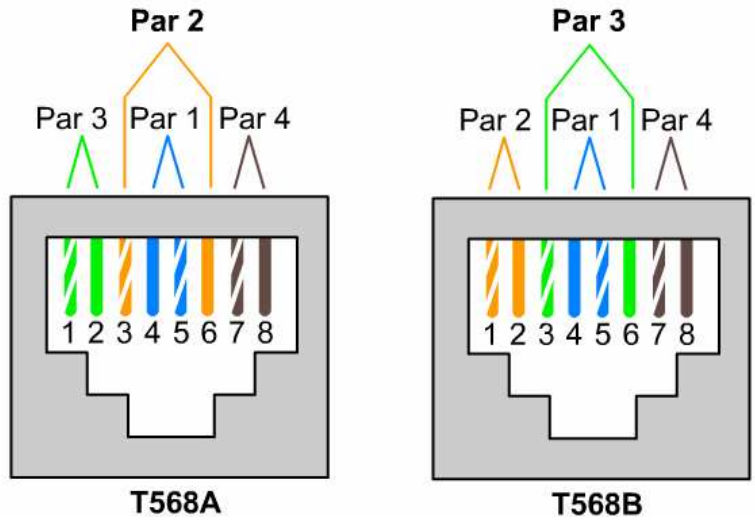


Figura 5.4 código de colores T568A, o T568B

La Figura 5.7, da las pautas de qué tipo de cable se debe utilizar cuando se interconecten dispositivos de Cisco.

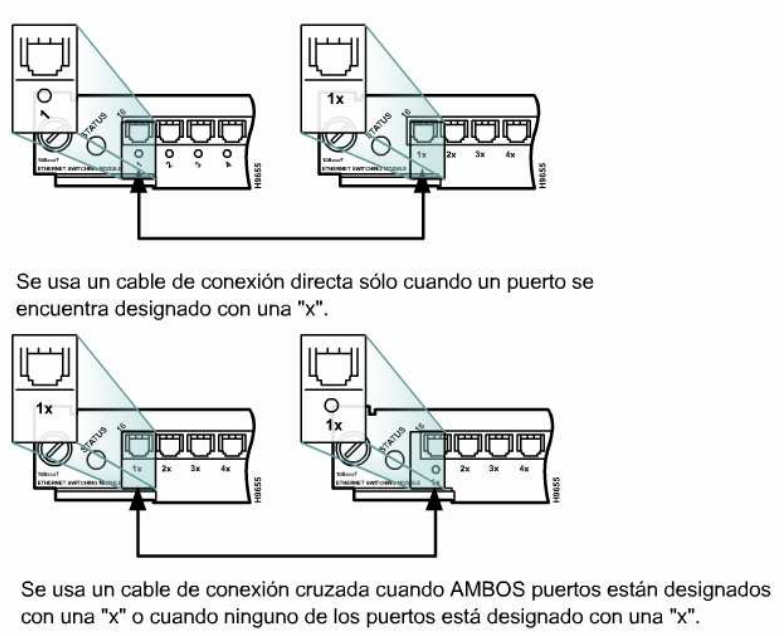


Figura 5.7 Interconexión dispositivos Cisco

Utilice cables de conexión directa para el siguiente cableado:

- Switch a router
- Switch a PC o servidor
- Hub a PC o servidor

Utilice cables de conexión cruzada para el siguiente cableado:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a router
- PC a PC
- Router a PC

5.1.7 Hubs

Los hubs 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 hub por lo general tiene de cuatro a veinticuatro puertos. Los hubs por lo general se utilizan en las redes Ethernet 10BASE-T o 100BASE-T, aunque hay otras arquitecturas de red que también los utilizan. El uso de un hub 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 hub, los datos que llegan a un puerto del hub 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 hubs vienen en tres tipos básicos:

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

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

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

Los dispositivos conectados al hub reciben todo el tráfico que se transporta a través del hub. Cuántos más dispositivos están conectados al hub, mayores son las probabilidades de que haya colisiones. Las colisiones ocurren cuando dos o más estaciones de trabajo envían al mismo tiempo datos a través del cable de la red. Cuando esto ocurre, todos los datos se corrompen. Cada dispositivo conectado al mismo segmento de red se considera un miembro de un dominio de colisión.

Algunas veces los hubs se llaman concentradores, porque los hubs sirven como punto de conexión central para una LAN de Ethernet.

5.1.8 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 computadora a otro sin una conexión de cable permanente.

Los switches y los puentes operan en la capa de enlace de datos del modelo de referencia OSI. La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

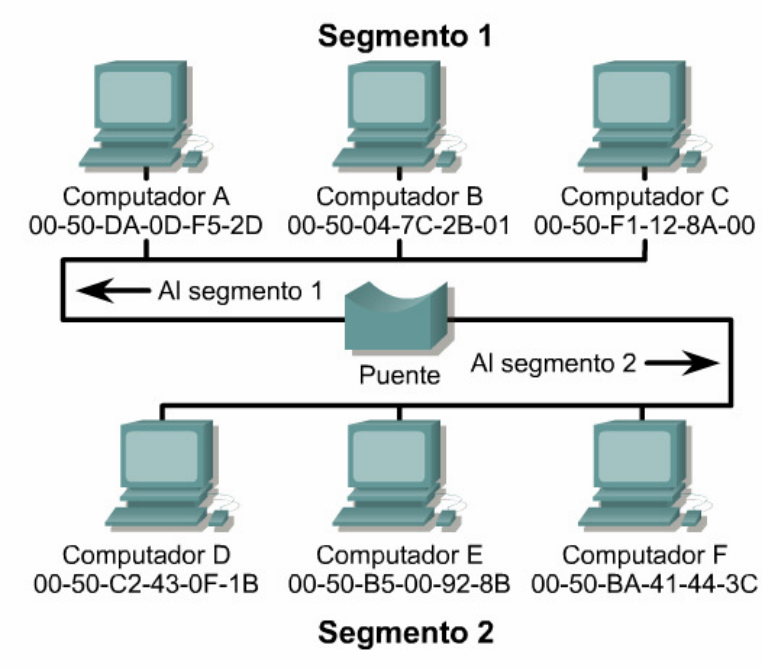


Figura 5.9 LAN dividida en segmentos

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.

5.1.10 Switches

Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar.

Las NIC no se representan con ningún símbolo estandarizado. Se entiende que siempre que haya dispositivos de networking conectados a un medio de red, existe alguna clase de NIC o un dispositivo similar a la NIC. Siempre que se ve un punto en un mapa topológico, éste representa una interfaz NIC o puerto que actúa como una NIC.

5.1.12 Comunicación de par a par

Al usar tecnologías LAN y WAN, muchas computadoras se interconectan para brindar servicios a sus usuarios. Para lograrlo, los computadoras en red toman diferentes roles o funciones entre si. Figura 14. Algunos tipos de aplicaciones requieren que las computadoras funcionen como socios en partes iguales. Otro tipo de aplicaciones distribuyen sus tareas de modo que las funciones de una computadora sirvan a una cantidad de otros de manera desigual. En cualquiera de los casos, dos computadoras por lo general se comunican entre si usando protocolos petición/respuesta. Una computadora realiza una petición de servicio, y el segundo computadora lo recibe y responde. El que realiza la petición asume el papel de cliente, y el que responde el de servidor.

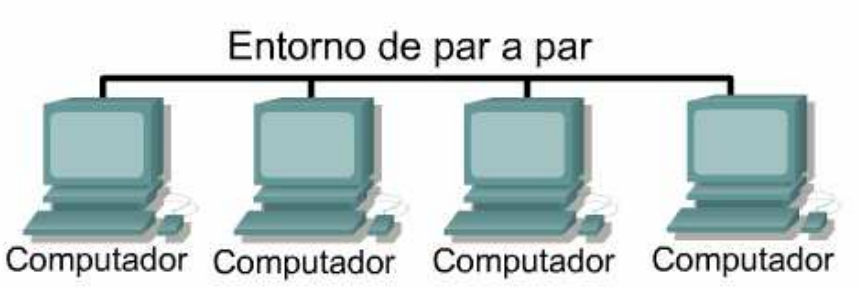


Figura 5.10 Comunicación de par a par.

En una red de par a par, (Figura 5.10) las computadoras en red actúan como socios en partes iguales, o pares. Como pares, cada computadora puede tomar la función de cliente o de servidor. En algún momento, la computadora A pedirá un archivo al computadora B, el cual responderá entregándole el archivo al computadora A. La computadora A funciona como cliente, mientras que el B funciona como servidor. Más tarde, las computadoras 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. Es posible que los usuarios requieran una contraseña antes de permitir que otros tengan accesos a sus recursos. 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.

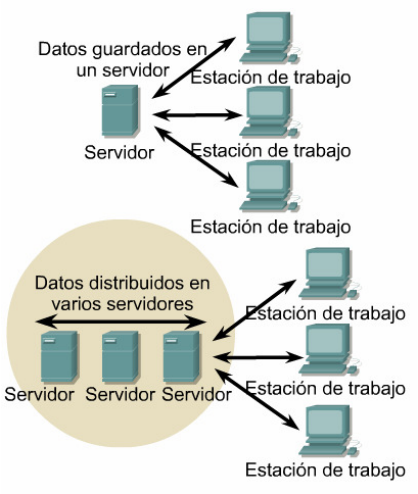


Figura 5.12 Servidores

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. El servicio de autenticación actúa como guardián para proteger el acceso a la red. 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.

La concentración de recursos de red como archivos, impresoras y aplicaciones en servidores hace que sea más fácil hacer una copia de seguridad de los datos generados y de mantenerlos. En vez de estar repartidos en equipos individuales, los recursos pueden encontrarse en servidores dedicados y especializados para facilitar el acceso. La mayoría de los sistemas cliente/servidor también incluyen recursos para mejorar la red al agregar servicios que extienden la utilidad de la misma.

La distribución de las funciones en las redes cliente/servidor ofrece grandes ventajas, pero también lleva aparejado algunos costos. Aunque la agregación de recursos en los sistemas de servidor trae mayor seguridad, acceso más sencillo y control coordinado, el servidor introduce un punto único de falla a la red.

Sin el servidor operacional, la red no puede funcionar en absoluto. Los servidores requieren de personal entrenado y capacitado para su administración y mantenimiento. Esto aumenta los costos de hacer funcionar la red. Los sistemas de servidor también necesitan hardware adicional y especializado que hace que el costo aumente.

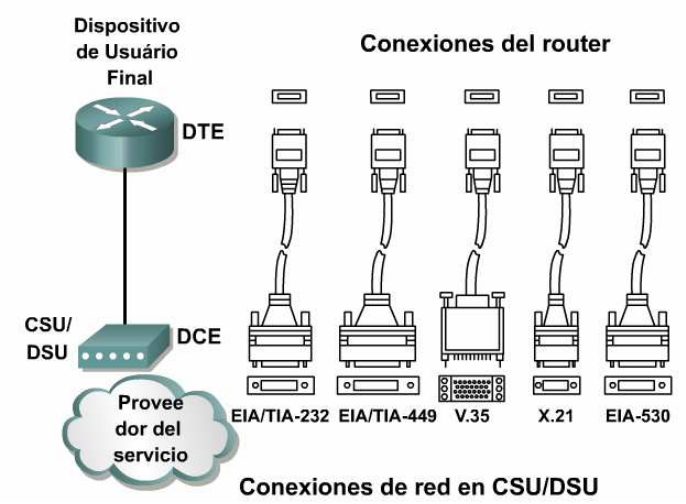


Figura 5.13 Conexiones seriales en un router

Para un router Cisco, 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. Figura 18

5.2.3 Conexiones seriales y router

Los routers son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Dentro de un entorno de LAN, el router contiene broadcasts, brinda servicios locales de resolución de direcciones, tal como ARP, y puede segmentar la red utilizando una estructura de subred. Para brindar estos servicios, el router debe conectarse a la LAN y a la WAN.

Además de determinar el tipo de cable, es necesario determinar si se requieren conectores DTE o DCE. El DTE es el punto final del dispositivo del usuario en un enlace WAN. El DCE en general es el punto donde la responsabilidad de enviar los datos se transfiere al proveedor de servicios. 12.01

Al conectarse en forma directa a un proveedor de servicios, o a un dispositivo como CSU/DSU que suministrará la señal de temporización, el router actúa como DTE y necesita un cable serial DTE. Figura 19. En general, esta es la forma de conectar los routers.

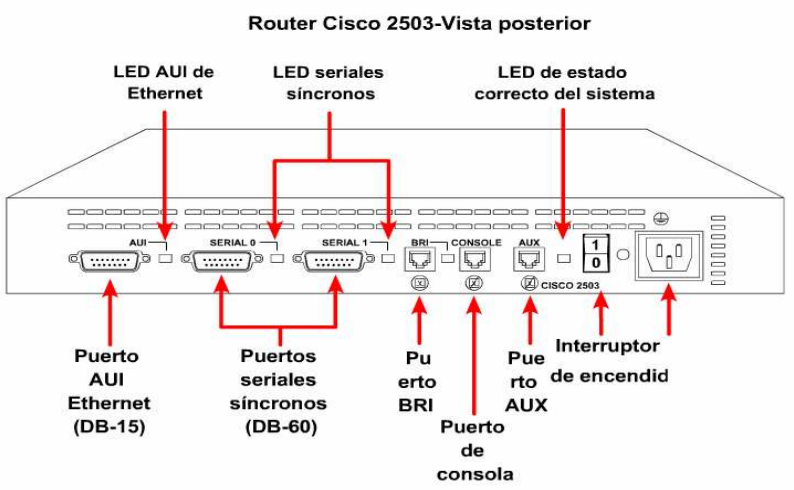


Figura 5.16 Interfaces del Router

Las interfaces de los routers que tienen puertos seriales modulares se rotulan según el tipo de puerto, ranura y número de puerto. Figura 5.17. La ranura indica la ubicación del módulo. Para configurar un puerto de una tarjeta modular, es necesario especificar la interfaz usando la sintaxis "tipo de puerto/número de ranura/número de puerto."

Use el rótulo "serial 1/0," cuando la interfaz sea serial, el número de ranura donde se instala el módulo es el 1, y el puerto al que se hace referencia es el puerto 0.

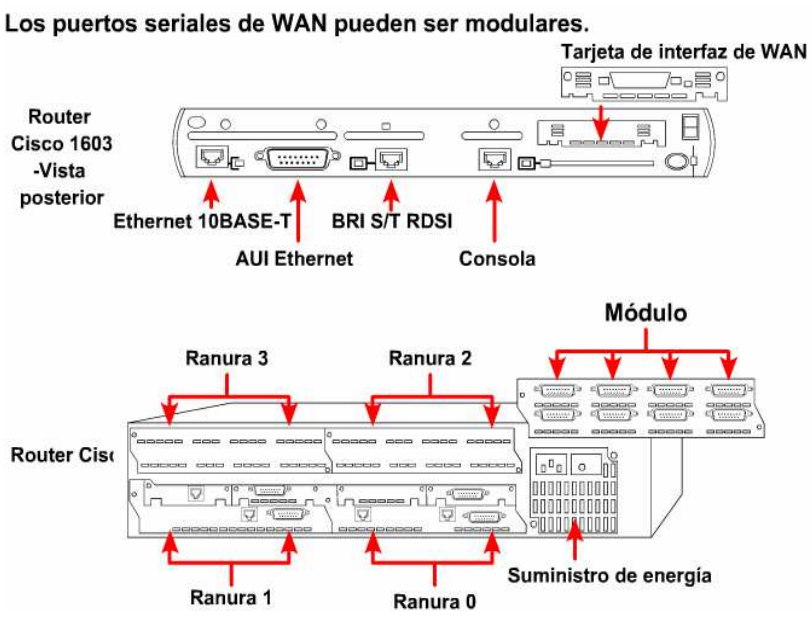


Figura 5.17 Puertos seriales WAN

5.2.4 Conexiones BRI RDSI y routers

Se pueden utilizar dos tipos de interfaces para BRI RDSI: BRI S/T y BRI U. Establezca quién está suministrando el dispositivo de terminación de la red 1 (NT1) para determinar qué interfaz se necesita.

5.2.5 Conexiones DSL y routers

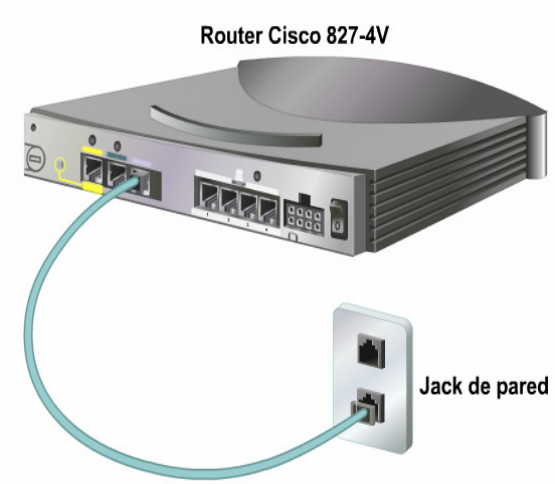


Figura 5.19 Router ADSL Cisco 827

El router ADSL Cisco 827 (figura 5.19), posee una interfaz de línea de suscripción digital asimétrica (ADSL). Figura 24. Para conectar una línea ADSL al puerto ADSL de un router, haga lo siguiente:

- Conecte el cable del teléfono al puerto ADSL en el router.
- 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.

5.2.6 Conexiones de cable-modem y routers

El router de acceso al cable uBR905 (Figura 5.20) de Cisco 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 router 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 router y el sistema de cable.

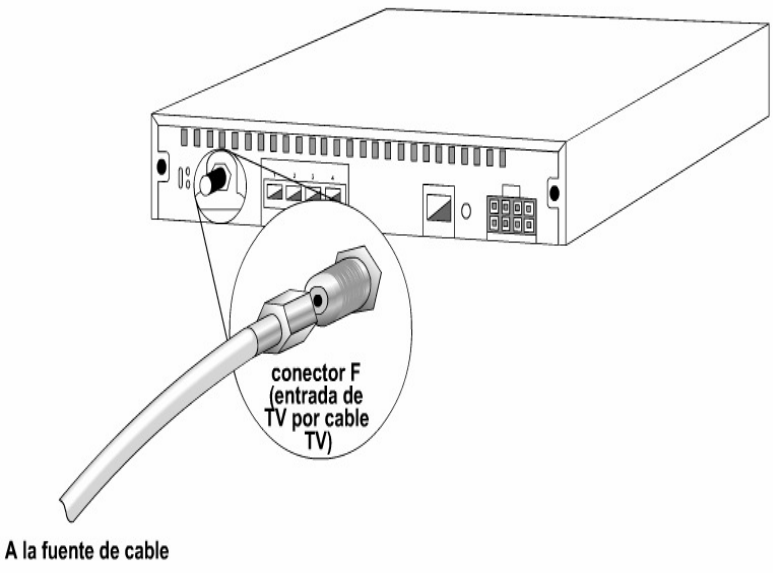


Figura 5.20 Conexión cable uBR905

El cable que se utiliza entre la terminal y el puerto de consola es el cable transpuesto, con conectores RJ-45. Figura 1. El cable transpuesto, 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

Para establecer una conexión entre la terminal y el puerto de consola de Cisco, hay que realizar dos pasos. Primero conecte los dispositivos utilizando un cable transpuesto desde el puerto de consola del router hasta el puerto serial de la estación de trabajo. Es posible que se necesite un adaptador RJ-45-a-DB-9 o un RJ-45-a-DB-25 para la terminal o el PC. Luego, configure la aplicación de emulación de terminal con los siguientes parámetros de puerto (COM) usuales para equipos. 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo.

El puerto AUX se utiliza para ofrecer administración fuera de banda a través de un módem. El puerto AUX debe ser configurado a través del puerto de consola antes de ser utilizado. El puerto AUX también utiliza los parámetros de 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo.

CAPÌTULO 6: Principios básicos de Ethernet

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

Por este motivo, se considera que Ethernet es muy escalable. El ancho de banda de la red podría aumentarse muchas veces sin cambiar la tecnología base de Ethernet.

6.1.2 Reglas de 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 (F = cable de fibra óptica, T = par trenzado de cobre no blindado).

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 es el estándar IEEE para una red Ethernet 802.3 que usa cable coaxial grueso a 10 Mbps como medio de transmisión de banda ancha. 10BROAD36 se considera ahora obsoleto. Una señal analógica, o señal portadora, es modulada por la data, y la señal portadora modulada es transmitida.

En la radio difusión y en la TV por cable se usa la señalización de banda ancha. Una señal analógica (señal portadora) es modulada por la data y se transmite la señal portadora modulada. Las estaciones de radio y la TV por cable utilizan la señalización banda ancha.

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. Las estaciones separadas por repetidores se encuentran dentro del mismo domino de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes. 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.

Algunas limitaciones que podemos encontrar entre capa y capa son:

- La capa 1 no se puede comunicar con las capas de niveles superiores
- La capa 2 hace esto con el Control de Enlace Lògico (LLC)
- La capa 1 no puede identificar computadoras
- La capa 2 usa un proceso de direccionamiento
- La capa 1 solo puede describir corrientes de bits
- La capa 2 usa el entramado para organizar o agrupar los bits
- La capa 1 no puede descifrar cual de los computadores transmitira los datos binarios desde un grupo en el que todos estan tratando de realizar la transmisión al mismo tiempo
- La capa 2 usa un sistema denominado Control de Aceso al Medio (MAC)

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

6.1.4 Denominación

Para permitir el envío local de las tramas en Ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar los computadoras y las interfaces de manera exclusiva. Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales.

6.1.5 Entramado de la Capa 2

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

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

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. Como se muestra en la figura 6.4

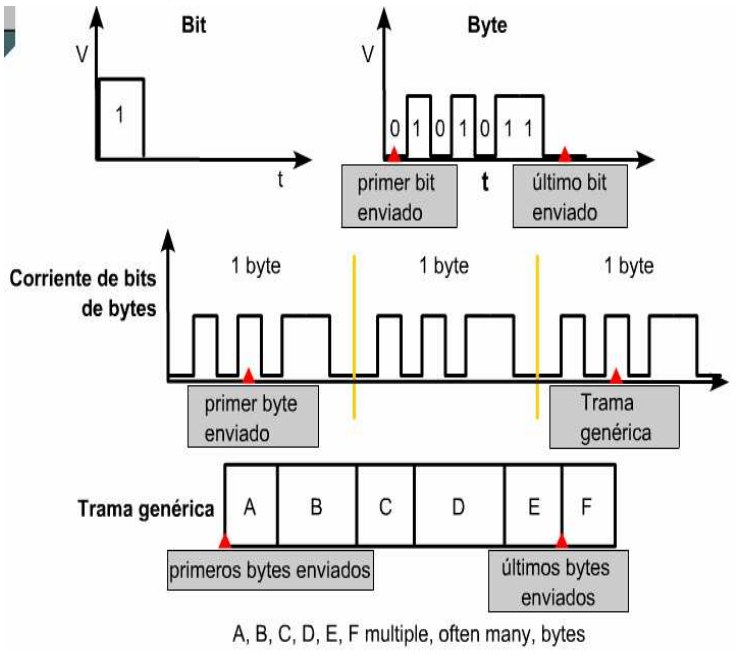


Figura 6.4 Diagrama de formato de trama

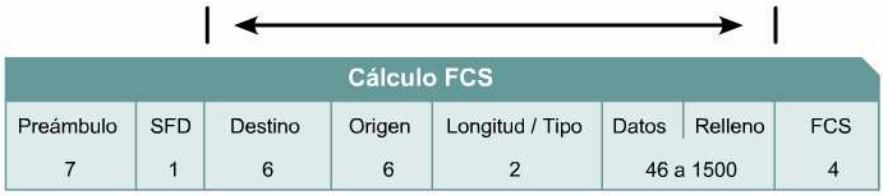
Hay tres formas principales para calcular el número de Secuencia de verificación de trama:

- **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.

6.1.6 Estructura e 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. Figura 6.5. 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.



Campos de tramas Ethernet EEE 802.3

Octetos	Descripción
• 7	Preámbulo
• 1	Delimitador de inicio de trama (SFD)
• 6	Dirección MAC de destino
• 6	Dirección MAC de origen
• 2	Campo de longitud/Tipo (longitud si es menos que 0600 hexadecimal, de lo contrario tipo de protocolo)
• 46 a 1500	Datos* (si es menos de 46 octetos, se debe agregar un relleno al final)
• 4	Secuencia de verificación de trama (suma de comprobación CRC)

Figura 6.5 Estructura de una trama

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. Ya que la corrupción de un solo bit en cualquier punto desde el inicio de la dirección destino hasta el extremo del campo de FCS hará que la checksum (suma de verificación) sea diferente, la cobertura de la FCS se auto-incluye. No es posible distinguir la corrupción de la FCS en sí y la corrupción de cualquier campo previo que se utilizó en el cálculo.

6.2 Operación de Ethernet

6.2.1 Control de acceso al medio (MAC)

MAC se refiere a los protocolos que determinan cuál de los computadoras de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la Capa 2 del modelo OSI. Tanto MAC como LLC son subcapas de la Capa 2. 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". CSMA/CD es un sistema sencillo. La NIC espera la ausencia de señal en el medio y comienza a transmitir. Si dos nodos transmiten al mismo tiempo, se produce una colisión y ningún nodo podrá transmitir.

Las 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) Figura 6.6

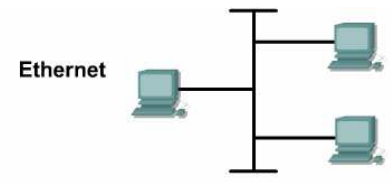


Figura 6.6 Representación de Ethernet

6.2.2 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: Figura 6.9.

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

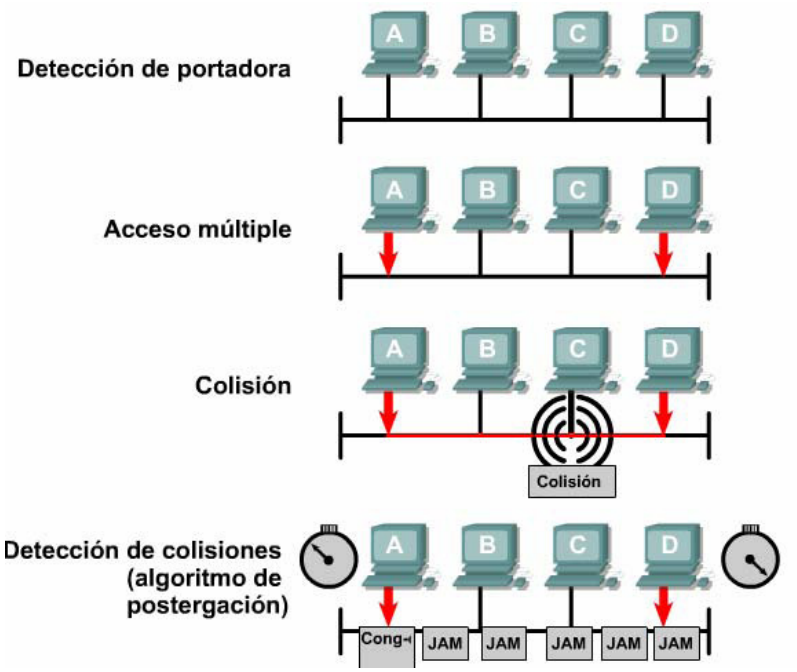


Figura 6.9 Funciones de Ethernet

En el método de acceso CSMA/CD, los dispositivos de networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo determinado al azar antes de reintentar. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar.

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

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión.

La ranura temporal de la Ethernet de 10 y 100 Mbps es de 512 tiempos de bit o 64 octetos. La ranura temporal de la Ethernet de 1000 Mbps es de 4096 tiempos de bit o 512 octetos. La ranura temporal se calcula en base de las longitudes máximas de cable para la arquitectura de red legal de mayor tamaño. Todos los tiempos de retardo de propagación del hardware se encuentran al máximo permisible y se utiliza una señal de congestión de 32 bits cuando se detectan colisiones.

La ranura temporal real calculada es apenas mayor que la cantidad de tiempo teórica necesaria para realizar una transmisión entre los puntos de máxima separación de un dominio de colisión, colisionar con otra transmisión en el último instante posible y luego permitir que los fragmentos de la colisión regresen a la estación transmisora y sean detectados. Para que el sistema funcione, la primera estación debe enterarse de la colisión antes de terminar de enviar la trama legal de menor tamaño. Para que una Ethernet de 1000 Mbps pueda operar en half duplex, se agregó un campo de extensión al enviar tramas pequeñas con el sólo fin de mantener ocupado al transmisor el tiempo suficiente para que vuelva el fragmento de colisión. Este campo sólo se incluye en los enlaces en half-duplex de 1000 Mbps y permite que las tramas de menor tamaño duren el tiempo suficiente para satisfacer los requisitos de la ranura temporal. La estación receptora descarta los bits de extensión.

En Ethernet de 10 Mbps, un bit en la capa MAC requiere de 100 nanosegundos (ns) para ser transmitido. A 100 Mbps el mismo bit requiere de 10 ns para ser transmitido y a 1000 Mbps sólo requiere 1 ns. A menudo, se utiliza una estimación aproximada de 20,3 cm (8 in) por nanosegundo para calcular el retardo de propagación a lo largo de un cable UTP. En 100 metros de UTP, esto significa que tarda menos de 5 tiempos de bit para que una señal de 10BASE-T se transporte a lo largo del cable.

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

6.2.4 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.

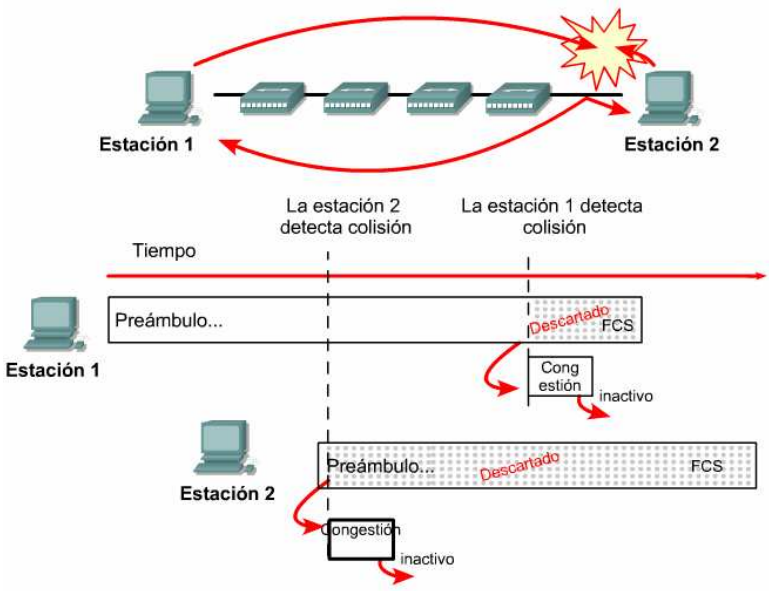


Figura 6.10 Ethernet y las Colisiones

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.

En la Figura 8, dos estaciones escuchan para asegurarse de que el cable esté inactivo, luego transmiten. La Estación 1 pudo transmitir un porcentaje significativo de la trama antes de que la señal alcanzara el último segmento del cable. La Estación 2 no había recibido el primer bit de la transmisión antes de iniciar su propia transmisión y sólo pudo enviar algunos bits antes de que la NIC detectara la colisión. De inmediato, la Estación 2 interrumpió la transmisión actual, la sustituyó con la señal de congestión de 32 bits y cesó todas sus transmisiones. Durante la colisión y el evento de congestión que la Estación 2 experimentaba, los fragmentos de la colisión iban en ruta por el dominio de colisiones repetido hacia la Estación 1. La Estación 2 completó la transmisión de la señal de congestión de 32 bits y quedó en silencio antes de que la colisión se propagara hacia la Estación 1, que todavía no sabía de la misma y continuaba transmitiendo.

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.

El inicio de la forma de onda en la Figura 2contiene datos normales codificados en Manchester. Unos pocos ciclos dentro de la muestra, la amplitud de onda se duplica. Este es el inicio de la colisión, donde las dos formas de onda se superponen. Justo antes de la finalización de la muestra, la amplitud se vuelve normal.

Esto sucede cuando la primera estación que detecta la colisión deja de transmitir y cuando todavía se observa la señal de congestión proveniente de la segunda estación que ha sufrido la colisión. Figura 6.12.

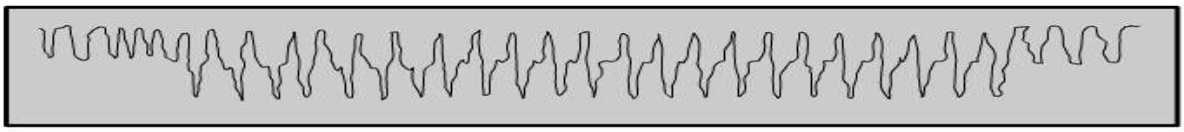


Figura 6.12 Señal con colisión

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. Por otra parte, una falla en el cable, como por ejemplo una diafonía excesiva, puede hacer que una estación perciba su propia transmisión como si fuera una colisión local.

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

Los jabbers y las tramas largas superan ambas el tamaño máximo permitido de trama. La jabber es bastante más grande. Figura 6.13

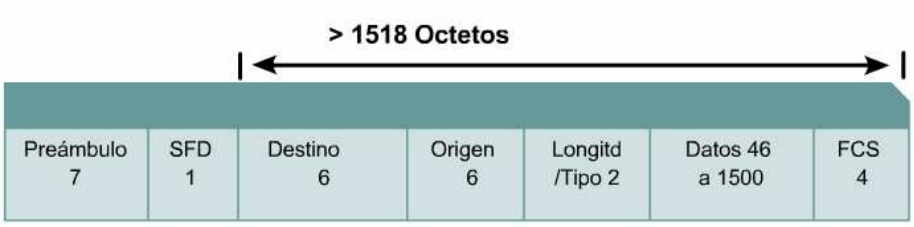


Figura 6.13 Los Jabber y las tramas

Una trama larga es una trama de longitud mayor al tamaño máximo legal y que tiene en cuenta si la trama está rotulada o no. No toma en cuenta si la trama tiene una checksum de FCS válida o no. En general, este error significa que se detectó jabber en la red.

Una trama corta es una trama de longitud menor al tamaño mínimo legal de 64 octetos, con una secuencia de verificación de trama correcta. Algunos analizadores de protocolos y monitores de red llaman a estas tramas "runts". Por lo general, la presencia de tramas cortas no significa que la red esté fallando. Las tramas cortas están formadas correctamente en todos los aspectos salvo uno y tienen sumas de comprobación FCS validas, pero tienen un tamaño de trama menor que el mínimo (64 octetos). Figura 6.14

Figura 6.14 Tramas cortas

El término runt es generalmente un término coloquial (en Inglés) impreciso que significa algo menor al tamaño legal de la trama. Puede referirse a las tramas cortas con una checksum de FCS válida aunque, en general, se refiere a los fragmentos de colisión.

6.2.8 FCS y màs allà

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.

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

6.2.10 Establecimiento del enlace y full dúplex y half duplex

Los extremos del enlace pueden saltar el ofrecimiento de las configuraciones a las que pueden operar. Esto permite que el administrador de la red fuerce que los puertos operen a una velocidad seleccionada y a una configuración duplex, sin deshabilitar la Auto-Negociación.

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

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

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

Resumen

Se debe haber obtenido una comprensión adecuada de los siguientes puntos clave:

• Principios básicos de la tecnología de Ethernet.
• Reglas de denominación para la tecnología de Ethernet.
• Cómo interactúan Ethernet y el modelo OSI.
• Proceso de entramado de Ethernet y estructura de la trama.
• Denominaciones de los campos de Ethernet y su propósito.
• Características y función del CSMA/CD
• Temporización de Ethernet
• Espacio entre las tramas.
• Algoritmo de postergación y tiempo posterior a una colisión.
• Errores de Ethernet y colisiones.
• Auto-negociación en relación a la velocidad y duplex

7.1 Ethernet de 10-Mbps y 100-Mbps

7.1.1 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.

Ethernet de 10 Mbps y versiones mas lentas son asíncronas. Cada estación receptora usa ocho octetos de información de temporización para sincronizar sus circuitos receptores a la data que entra. Las 10BASE5, 10BASE2 y 10BASE-T todas comparten los mismos parámetros de temporización.Por ejemplo, 1 tiempo de bit a 10 Mbps = 100 nanosegundos = 0,1 µicrosegundos = 1 diez millonésima parte de un segundo.Esto significa que en una red Ethernet de 10 Mbps, 1 bit en la subcapa MAC requiere de 100 nseg para ser transmitido.

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

Todas las formas de Ethernet de 10 Mbps toman octetos recibidos de la subcapa MAC y realizan un proceso denominado codificación de la línea. La codificación de la línea describe de qué manera los bits se transforman en señal en el cable. Las codificaciones más sencillas tienen una temporización y características eléctricas no recomendables. Por lo tanto, los códigos de línea se han diseñado para tener propiedades de transmisión recomendables. Esta forma de codificación utilizada en los sistemas de 10 Mbps se denomina codificación Manchester.

La codificación Manchester (Figura 7.1), 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. La forma de la onda superior tiene un borde que cae, así se interpreta como 0. La segunda forma de onda muestra un borde ascendente que se interpreta como 1. En la tercera forma de onda, se da una secuencia binaria alternada. C

Con los datos binarios alternados, no hay necesidad de volver al nivel de voltaje previo. Como se puede observar en la tercera y cuarta forma de onda del gráfico, los valores binarios de bits están indicados por la dirección del cambio durante un período de bits dado. Los niveles de voltaje de la forma de la onda al comienzo o fin de cualquier período de bits no son factores al determinar valores binarios.

7.1.2 10 BASE 5

El producto original para Ethernet del año 1980, 10BASE5 transmitía 10 Mbps a través de un solo cable bus coaxial grueso. 10BASE5 es importante porque fue el primer medio que se utilizó para Ethernet. 10BASE5 formaba parte del estándar original 802.3. El principal beneficio de 10BASE5 era su longitud. En la actualidad, puede hallarse en las instalaciones antiguas, pero no se recomienda para las instalaciones nuevas. 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. Los sistemas 10BASE5 también representan un único punto de falla.

10BASE5 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.

La Figura 7.2, ilustra una posible configuración para un máximo dominio de colisión de punta a punta. Entre dos estaciones lejanas cualesquiera, sólo se permite que tres segmentos repetidos tengan estaciones conectadas, usando los otros dos segmentos repetidos solamente como segmentos de enlace para extender la red.

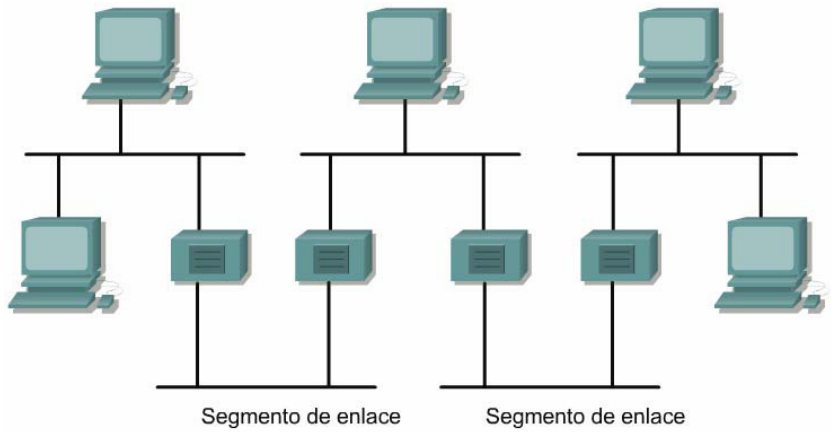


Figura 7.2 Máximo dominio de colisión de punta a punta.

7.1.4 10 BASE-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. Este cable se conectaba a un dispositivo de conexión central que contenía el bus compartido. Este dispositivo era un hub. Se encontraba en el centro de un conjunto de cables que partían hacia los PC, como los radios que parten desde el centro de una rueda. Esto se conoce como topología en estrella. Las distancias que los cables podían cubrir desde el hub y la ruta que se seguía al instalar los UTP comenzaron a utilizar, cada vez más, estrellas compuestas por estrellas: estructura que recibió el nombre de topología en estrella extendida. Al principio, 10BASE-T era un protocolo half-duplex pero más tarde se agregaron características de full-duplex. 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. La Figura 7.4 muestra la disposición de la salida de los pins para una conexión 10BASE-T. El par transmisor del lado receptor se conecta al par receptor del dispositivo conectado.

Numero e Pin	Señal
1	TD + (Transmitir datos, señal diferencial positiva)
2	TD – (Transmitir datos, señal diferencial negativa)
3	RD + (Recibir datos, señal diferencial positiva)
4	Unused
5	No se utiliza
6	RD- (Recibir datos, señal diferencial negtiva)
7	No se utiliza
8	No se utiliza

Figura 7.4 Salida de pins conexión 10BASE-T

Consideraciones a tomar en un Enlace de 10BASE –T:

1. La longitud del cable de un segmento de enlace UTP es normalmene de 1 a 100 m entre la estacion de trabajo y un hub, y entre los hubs.
2. Cada hub es un repetidor multipuesto, de manera que los enlaces entre hubs cuentan en el limite para los repetidores.
3. Estos dos hubs “apilables” con backlanes inerconectados se cuentan como un solo hub (repetidor).

7.1.6 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.

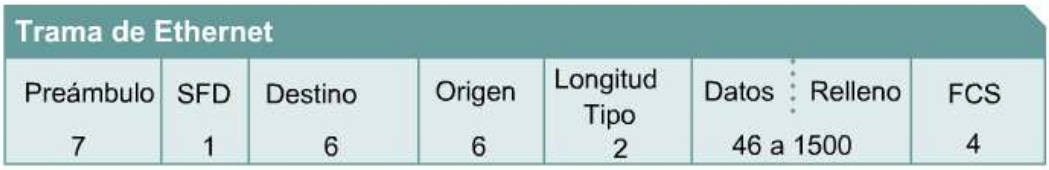


Figura 7.6 Trama de Ethernet 100-Mbps

El formato de trama de 100-Mbps es el mismo que el de la trama de 10-Mbps. Figura 5

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. La primera parte de la codificación utiliza una técnica denominada 4B/5B, la segunda parte es la codificación real de la línea específica para el cobre o la fibra.

7.1.8 100 BASE-FX

En el momento en que se introdujo Fast Ethernet con base de cobre, también se deseaba una versión en fibra. Una versión en fibra podría ser utilizada para aplicaciones con backbones, conexiones entre distintos pisos y edificios donde el cobre es menos aconsejable y también en entornos de gran ruido. Se introdujo 100BASE-FX para satisfacer esa necesidad.

Sin embargo, nunca se adoptó con éxito la 100BASE-FX. Esto se debió a la oportuna introducción de los estándares de fibra y de cobre para Gigabit Ethernet. Los estándares para Gigabit Ethernet son, en estos momentos, la tecnología dominante en instalaciones de backbone, conexiones cruzadas de alta velocidad y necesidades generales de infraestructura.

La temporización, el formato de trama y la transmisión son todos comunes a ambas versiones de Fast Ethernet de 100 Mbps . 100BASE-FX también utiliza la codificación 4B/5B. En la Figura 7.8, note la forma de onda resaltada en el ejemplo. La forma de onda superior no presenta transición, lo que indica la presencia de un binario 0.

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.

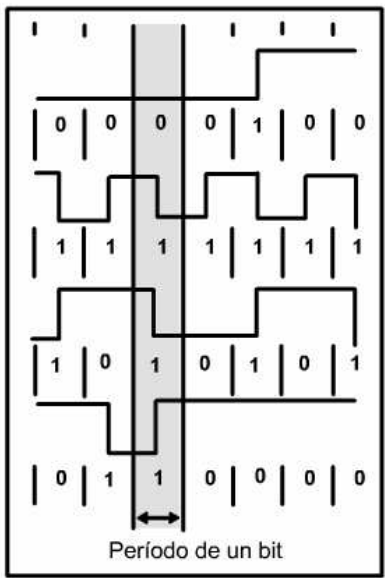


Figura 7.8 100BASE-FX

7.2 Ethernet Gigabit 10-Gigabit

7.2.1 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. Figura 7.10, 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 mejor.

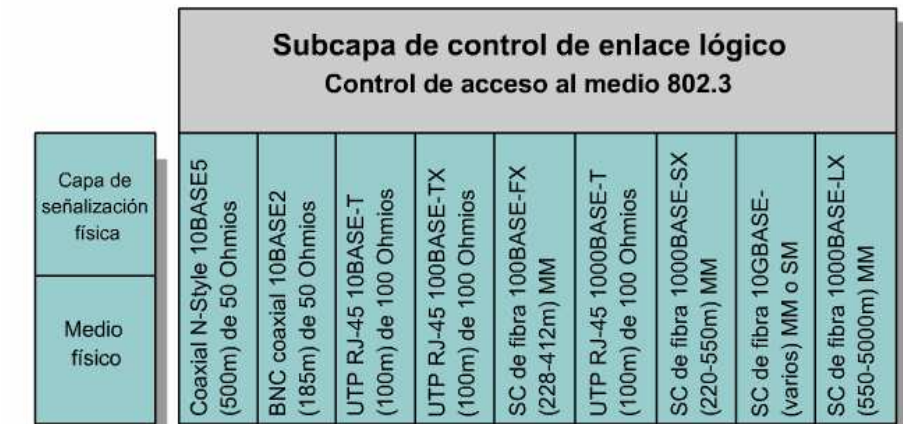


Figura 7.10 Estándar Ethernet de 1000-Mbps

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización, como muestra la Figura 7.11. Utilizan un tiempo de bit de 1 nanosegundo (0,000000001 segundos) o 1 mil millonésima parte de un segundo.

Parámetro	Valor
Tipos de Ethernet	1 nsec
Ranura temporal	4096 períodos de bit
Espacio entre las tramas	96 bits *
Límite de intento de colisión	16
Límite de postergación de colisión	10
Tamaño de atascamiento de colisiones	32 bits
Tamaño de trama máximo sin rotular	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Límite de ráfaga	65,536 bits

Figura 7.11 Parámetros de temporizacion.

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 1Gigabit. 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. Como se muestra en la Figura 7.12, 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.

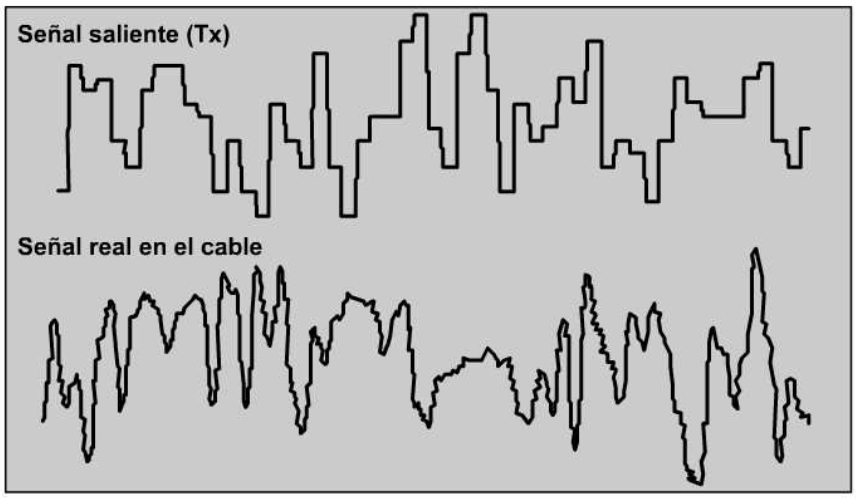


Figura 7.12 Señal de transmisión durante una colisión

7.2.3 1000 BASE-SX Y LX

El estándar IEEE 802.3 recomienda Gigabit Ethernet en fibra como la tecnología de backbone de preferencia. Ventajas de Gigabit Ethernet con fibra óptica.

- Inmunidad al ruido
- Sin problemas potenciales de conexión a tierra
- Excelentes características de distancia
- Muchas opciones de dispositivos 1000BASE-X
- Se puede usar para conectar segmentos Fast Ethernet ampliamente dispersos

La temporización, el formato de trama y la transmisión son comunes a todas las versiones de 1000 Mbps. En la capa física, se definan dos esquemas de codificación de la señal. Figura 7.14, El esquema 8B/ 10B se utiliza para los medios de fibra óptica y de cobre blindado y la modulación de amplitud de pulso 5 (PAM5) se utiliza para los UTP.

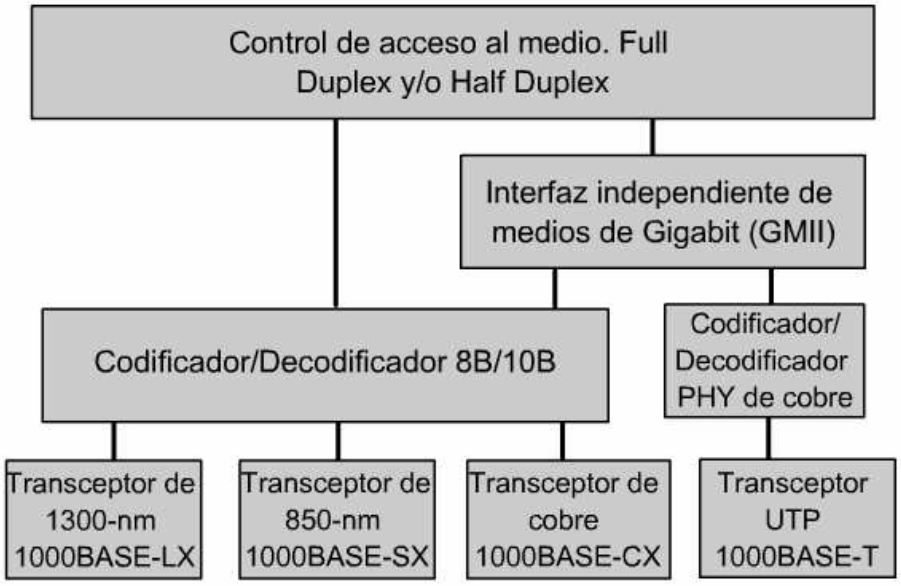


Figura 7.14 Esquemas de Codificación en la capa física

7.2.4 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, los valores de las siguientes tablas (tabla 7.1), son los límites prácticos entre los dispositivos. Las topologías de cadena de margaritas, de estrella y de estrella extendida están todas permitidas. El problema entonces yace en la topología lógica y el flujo de datos y no en las limitaciones de temporización o distancia.

MEDIO	ANCHO DE BANDA MODAL	DISTANCIA MAXIMA
Fibra multimodo 62.5 nm	160	220 m
Fibra multimodo 62.5 nm	200	275 m
Fibra multimodo 50 nm	400	500 m
Fibra multimodo 10 nm	500	500 m

MEDIO	ANCHO DE BANDA MODAL	DISTANCIA MAXIMA
Fibra multimodo 62.5 nm	500	220 m
Fibra multimodo 50 nm	400	275 m
Fibra multimodo 50 nm	500	500 m
Fibra multimodo 10 nm	N/A	5000 m

Tabla 7.2 Limitaciones de distancia enlaces full-duplex

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.

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.

La Fuerza de Tarea IEEE 802.3ae y la Alianza de Ethernet de 10 Gigabit (10 GEA) están trabajando para estandarizar estas tecnologías emergentes.

10-Gbps Ethernet (IEEE 802.3ae) se estandarizó en junio de 2002. Es un protocolo full-duplex que utiliza sólo fibra óptica como medio de transmisión. Las distancias máximas de transmisión dependen del tipo de fibra que se utiliza. Cuando se utiliza fibra monomodo como medio de transmisión, la distancia máxima de transmisión es de 40 kilómetros (25 millas). De algunas conversaciones recientes entre los miembros del IEEE, surge la posibilidad de estándares para una Ethernet de 40, 80 e inclusive 100 Gbps.

7.2.6 Arquitecturas de 10-Gigabit Ethernet

Tal como sucedió en el desarrollo de Gigabit Ethernet, el aumento en la velocidad llega con mayores requisitos. Una menor duración del tiempo de bit que resulta de una mayor velocidad requiere consideraciones especiales. En las transmisiones en 10 GbE, 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. Debido a la corta duración del bit de datos de 10 GbE, a menudo resulta difícil separar un bit de datos del ruido.

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.

En respuesta a estos problemas de la sincronización, el ancho de banda y la Relación entre Señal y Ruido, Ethernet de 10 Gigabits utiliza dos distintos pasos de codificación. Al utilizar códigos para representar los datos del usuario, la transmisión de datos se produce de manera más eficiente. Los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores características de la Relación entre Señal y Ruido.

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.

7.2.7 El futuro 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.

Se han presentando propuestas para esquemas de arbitraje de Ethernet que no sean CSMA/CD. El problema de las colisiones con las topologías físicas en bus de 10BASE5 y 10BASE2 y de los hubs de 10BASE-T y 100BASE-TX ya no es tan frecuente. El uso de UTP y de la fibra óptica con distintas rutas de Tx y Rx y los costos reducidos de los switches hacen que las conexiones a los medios en half-duplex y los medios únicos compartidos sean mucho menos importantes.

El futuro de los medios para networking tiene tres ramas:

1. Cobre (hasta 1000 Mbps, tal vez más)
2. Inalámbrico (se aproxima a los 100 Mbps, tal vez más)
3. 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.

CAPITULO 8: Conmutación de Ethernet

- El puente se acaba de encender, por lo tanto la tabla de puenteo se encuentra vacía. El puente sólo espera el tráfico en ese segmento. Cuando detecta el tráfico, el puente lo procesa.
- 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 repuesta 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 repuesta 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.

Además de la aparición de microprocesadores y memoria más rápidos, otros dos avances tecnológicos hicieron posible la aparición de los switch. La memoria de contenido direccionable (Content Addressable Memory, CAM) es una memoria que esencialmente funciona al revés en comparación con la memoria convencional. Ingresar datos a la memoria devolverá la dirección asociada. El uso de memoria CAM permite que un switch encuentre directamente el puerto que está asociado con la dirección MAC sin usar un algoritmo de búsqueda. Un circuito integrado de aplicación específica (Application Specific Integrated Circuit, 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 switch pueda mantenerse al ritmo de la demanda de los datos de muchos microsegmentos y velocidades de bits altas.

8.1.4 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.

8.1.5 Modo de conmutación

Cómo se conmuta una trama a su puerto de destino es una compensación entre la latencia y la confiabilidad. Un switch 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 switch. Sin embargo, no se puede verificar la existencia de errores. En el otro extremo, el switch puede recibir toda la trama antes de enviarla al puerto destino.

Esto le da al software del switch la posibilidad de controlar la secuencia de verificación de trama (Frame Check Sequence, FCS) para asegurar que la trama se haya recibido de modo confiable antes de enviarla al destino.

Si bien se recomienda el uso de rutas redundantes, ellas pueden tener efectos colaterales indeseables. Los bucles de conmutación son uno de esos efectos. Los bucles de conmutación pueden ocurrir ya sea por diseño o por accidente, y pueden llevar tormentas de broadcast que rápidamente abrumen la red. Para contrarrestar la posibilidad de bucles, se proporcionan switches con un protocolo basado en los estándares llamado protocolo de spanning tree (Spanning Tree Protocol, STP).

Cada switch en una LAN que usa STP envía un mensaje especial llamado unidades de datos del protocolo puente (Bridge Protocol Data Unit, BPDU) desde todos sus puertos para que los otros switches sepan de su existencia y elijan un puente raíz para la red. Los switches entonces usan un algoritmo spanning-tree (Spanning Tree Algorithm, STA) para resolver y desconectar las rutas redundantes.

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

- Bloquear. Recibe solo las BPDU
- Escuchar. Creación de una topología “activa”
- Aprender Envío y recepción de datos del usuario
- Enviar Creación de una tabla de puenteo
- Desactivar Administrativamente abajo

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

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

El resultado de la resolución y eliminación de bucles usando STP es la creación de un árbol jerárquico lógico sin bucles. Sin embargo, si se necesitan, las rutas alternativas están disponibles.

8.2 Dominios de colisión y de broadcast

8.2.1 Entorno de medios compartidos

Comprender los dominios de colisión requiere de la comprensión de lo que son las colisiones y cómo se originan. Para ayudar a explicar las colisiones, aquí se revisan los medios y topologías de Capa 1.

Algunas redes se conectan directamente y todos los hosts comparten la Capa 1. Aquí hay algunos ejemplos:

Figura 8.4 Segmentos del medio OSI en colisiones

Los tipos de dispositivos que interconectan los segmentos de medios definen los dominios de colisión. Figura 8.4. 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 hubs, 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 computadoras 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 hubs repetidores entre dos computadoras en la red. Para asegurar que una red 10BASE-T con repetidores funcionará de forma adecuada, el cálculo del retardo del recorrido de ida y vuelta debe estar dentro de ciertos límites, 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.

Los dispositivos de Capa 2 dividen o segmentan los dominios de colisión. Figura 8.6. 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 switches, hacen un seguimiento de las direcciones MAC y el segmento en el que se encuentran. Al hacer esto, estos dispositivos pueden controlar el flujo de tráfico en el nivel de Capa 2. Esta función hace que las redes sean más eficientes, al permitir que los datos se transmitan por diferentes segmentos de la LAN al mismo tiempo sin que las tramas colisionen. Al usar puentes y switches, el dominio de colisión se divide efectivamente en partes más pequeñas, que se transforman cada una a su vez en un dominio de colisión.

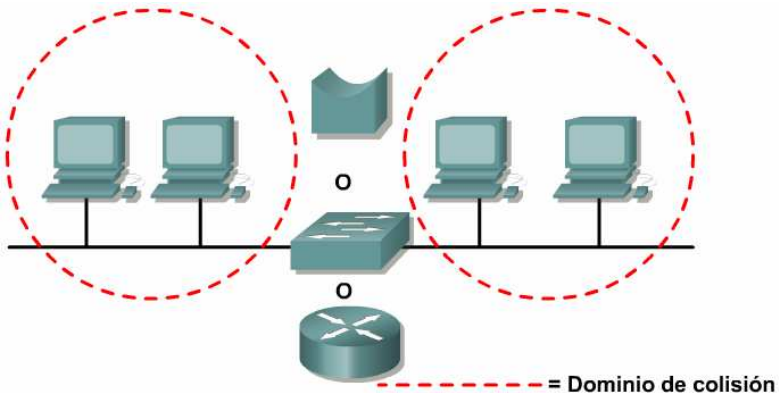


Figura 8.6 Segmentación de dominios de colisión

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.

La mayoría de las veces, el host no se beneficia al procesar el broadcast, ya que no es el destino buscado. Al host no le interesa el servicio que se publicita, o ya lo conoce. Los niveles elevados de radiación de broadcast pueden 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 routers y las aplicaciones multicast.

Las estaciones de trabajo envían en broadcast una petición de protocolo de resolución de direcciones (Address Resolution Protocol, ARP) cada vez que necesitan ubicar una dirección MAC que no se encuentra en la tabla ARP. Las tormentas de broadcast pueden originarse en un dispositivo que requiere información de una red que ha crecido demasiado. La petición original recibe tantas respuestas que el dispositivo no las puede procesar, o la primera petición desencadena peticiones similares de otros dispositivos que efectivamente bloquean el flujo de tráfico en la red.

Como ejemplo, el comando **telnet mumble.com** se traduce a una dirección IP a través de una búsqueda en el sistema de denominación de dominios (Domain Naming System, DNS). Para ubicar la dirección MAC correspondiente, se envía una petición ARP.

Por lo general, las estaciones de trabajo IP guardan entre 10 y 100 direcciones en sus tablas ARP durante dos horas aproximadamente. La velocidad de un ARP en una estación de trabajo típica puede ser cercana a 50 direcciones cada dos horas o 0,007 ARP por segundo. 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. Algunos administradores configuran todas las estaciones de trabajo para que ejecuten el protocolo de información de enrutamiento (Routing Information Protocol, RIP) como una política de redundancia y alcance. Cada 30 segundos, el RIPv1 utiliza broadcasts para retransmitir toda la tabla de enrutamiento a otros routers RIP.

Si 2000 estaciones de trabajo se configuraran para ejecutar RIP y, en promedio, se requieren 50 paquetes para transmitir la tabla de enrutamiento, las estaciones de trabajo generarían 3333 broadcasts por segundo. La mayoría de los administradores de red sólo configuran un número pequeño de routers, por lo general de cinco a diez, para ejecutar un RIP. En el caso de una tabla de enrutamiento que tiene un tamaño de 50 paquetes, 10 routers RIP generarán cerca de 16 broadcasts por segundo.

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

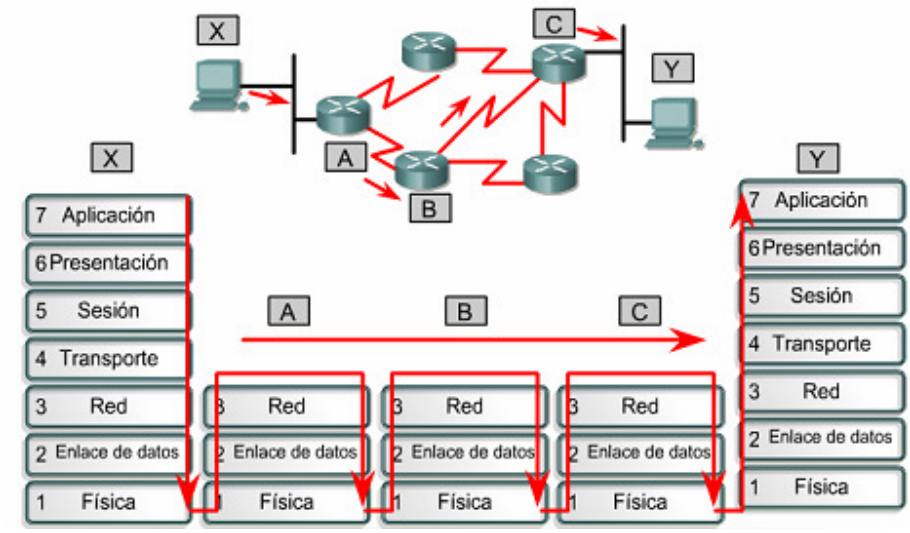


Figura 8.8 flujos de datos en un contexto de dominios de colisión y de broadcast

Una buena regla a seguir es que un dispositivo de Capa 1 siempre envíe la trama, mientras que un dispositivo de Capa 2 desee enviar la trama. En otras palabras, un dispositivo de Capa 2 siempre enviará la trama al menos que algo se lo impida. Un dispositivo de Capa 3 no enviará la trama a menos que se vea obligado a hacerlo. Usar esta regla ayudará a identificar la forma en que los datos fluyen a través de la red.

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

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

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

Resumen

Se debe haber obtenido una comprensión adecuada de los siguientes puntos clave:

• Evolución del puenteo y la conmutación
• Memoria de contenido direccionable (Content Addressable Memory, CAM)
• Latencia de puenteo
• Modos de conmutación de almacenamiento y envío y por el método de corte.
• Protocolo de spanning tree (Spanning Tree Protocol, STP).
• Colisiones, broadcasts, dominios de colisión y de broadcast.
• Dispositivos de Capa 1, 2, y 3 utilizados para crear dominios de colisión y de broadcast.
• Flujo de datos y los problemas de broadcast.
• Segmentación de la red y los dispositivos utilizados en la creación de segmentos

9.1 Introducción a TCP/IP

9.1.1 Historia y futuro e TCP/IP

El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia. Para tener una mejor idea, imagine un mundo, cruzado por numerosos tendidos de cables, alambres, microondas, fibras ópticas y enlaces satelitales. Entonces, imagine la necesidad de transmitir datos independientemente del estado de un nodo o red en particular. El DoD requería una transmisión de datos confiable hacia cualquier destino de la red, en cualquier circunstancia. La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño. Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa la Internet. Figura 9.1

Figura 9.1 Modelo TCP/IP

Al leer sobre las capas del modelo TCP/IP, tenga en cuenta el propósito original de la Internet. Recordar su propósito ayudará a reducir las confusiones. El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. Resulta fundamental no confundir las funciones de las capas de los dos modelos ya que estas desempeñan diferentes funciones en cada modelo.

9.1.2 La capa de aplicación

La capa de aplicación del modelo TCP/IP, figura 9.2, maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. Figura 9.2

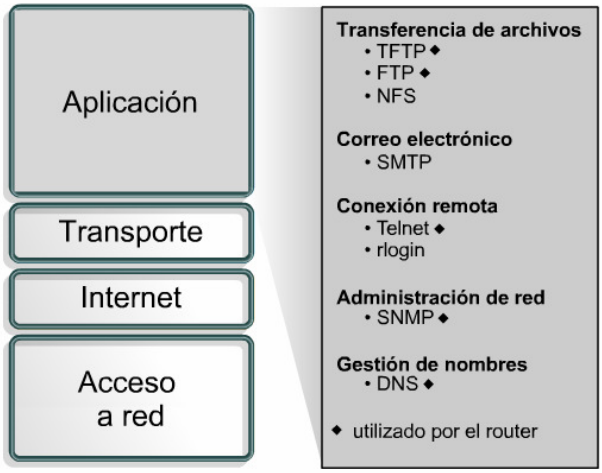


Figura 9.2 Capa de aplicación modelo TCP/IP

La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

Generalmente, se compara la Internet con una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. El control de punta a punta, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP. La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts. Los servicios de transporte incluyen los siguientes servicios:

TCP y UDP

- Segmentación de los datos de capa superior
- Envío de los segmentos desde un dispositivo en un extremo a otro dispositivo en otro extremo.

TCP solamente

- Establecimiento de operaciones de punta a punta.
- Control de flujo proporcionado por ventanas deslizantes.
- Confiabilidad proporcionada por los números de secuencia y los acuses de recibo

Generalmente, se representa la Internet con una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. Figura 1 La nube maneja los aspectos tales como la determinación de la mejor ruta. Figura 9.4

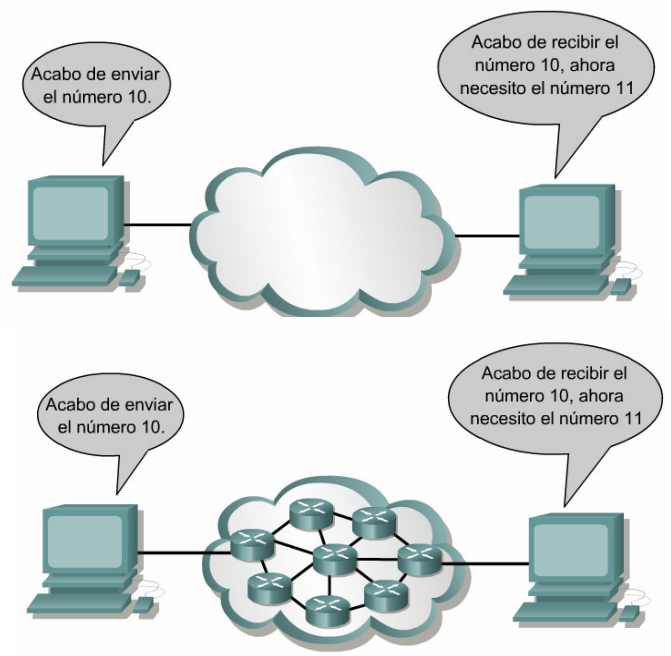


Figura 9.4 Representación de Internet en envío de paquetes

9.1.5 La capa de acceso de red

La capa de acceso de red también se denomina capa de host a red. Figura 9.5. La capa de acceso de red es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

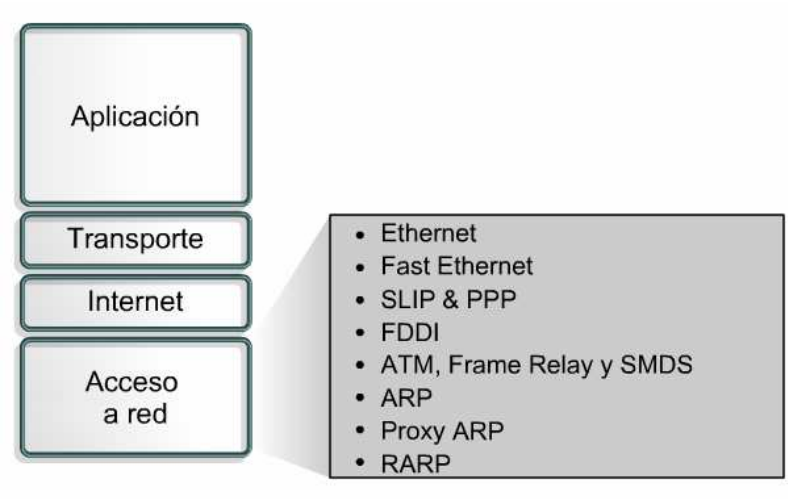


Figura 9.5 Capa de acceso de red

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión.

Los estándares del protocolo de los módem tales como el Protocolo Internet de enlace serial (SLIP) y el Protocolo de punta a punta (PPP) brindan acceso a la red a través de una conexión por módem. Debido a un intrincado juego entre las especificaciones del hardware, el software y los medios de transmisión, existen muchos protocolos que operan en esta capa.

Las funciones de la capa de acceso de red incluyen la asignación de direcciones IP a las direcciones físicas y el encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

9.1.7 Arquitectura de Internet

Aunque Internet es compleja, existen algunas ideas básicas que rigen su operación. Esta sección examinará la arquitectura básica de la Internet. La Internet es una idea que parece muy sencilla a primera vista, y cuando se repite a gran escala, permite la comunicación casi instantánea de datos por todo el mundo entre cualesquiera personas, en cualquier lugar, en cualquier momento.

Las LAN son redes de menor tamaño que se limitan a un área geográfica. Muchas LAN conectadas entre sí permiten que funcione La Internet. Pero las LAN tienen sus limitaciones de tamaño. Aunque se han producido avances tecnológicos que mejoran la velocidad de las comunicaciones, tales como la Ethernet de 10 Gigabits, de 1 Gigabit y Metro Optical, la distancia sigue siendo un problema.

Concentrarse en la comunicación entre la computadora origen y destino y los computadoras intermedios al nivel de la capa de aplicación es una forma de ver el panorama de la arquitectura de Internet. Colocar copias idénticas de una aplicación en todos los computadoras de la red podría facilitar el envío de mensajes a través de la gran red. Sin embargo, esto no funciona bien a mayor escala. Para que un nuevo software funcione correctamente, se requiere de la instalación de nuevas aplicaciones en cada computadora de la red. Para que un hardware nuevo funcione correctamente, se requiere de la modificación del software. Cualquier falla en un computadora intermedio o en la aplicación del mismo causaría una ruptura en la cadena de mensajes enviados.

Internet utiliza el principio de la interconexión en la capa de red. Con el modelo OSI a modo de ejemplo, el objetivo consiste en construir la funcionalidad de la red en módulos independientes. Esto permite que una variedad de tecnologías LAN existan en las Capas 1 y 2 y una variedad de aplicaciones funcionen en las Capas 5; 6 y 7. El modelo OSI proporciona un mecanismo en el cual se separan los detalles de las capas inferior y superior. Esto permite que los dispositivos intermedios de networking "retransmitan" el tráfico sin tener que molestarse con los detalles de la LAN.

Esto nos lleva al concepto de internetworking o la construcción de redes de redes. Una red de redes recibe el nombre de internet, que se escribe con "i" minúscula. Cuando se hace referencia a las redes desarrolladas por el DoD en las que corre la Worldwide Web (www) (Red mundial), se utiliza la letra "I" mayúscula y recibe el nombre de Internet. Internetworking debe ser escalable respecto del número de redes y computadoras conectados. Internetworking debe ser capaz de manejar el transporte de datos a lo largo de grandes distancias. Tiene que ser flexible para admitir las constantes innovaciones tecnológicas. Además, debe ser capaz de ajustarse a las condiciones dinámicas de la red. Y, sobre todo, las internetworks deben ser económicas. Las internetworks deben estar diseñadas para permitir que en cualquier momento, en cualquier lugar, cualquier persona reciba la comunicación de datos.

Dos computadoras, en cualquier lugar del mundo, si se conforman con determinadas especificaciones de hardware, software y protocolos, pueden comunicarse de forma confiable. La estandarización de las prácticas y los procedimientos de transportación de datos por las redes ha hecho que Internet sea posible.

9.2 Dirección de Internet

9.2.1 Direccionamiento IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura 9.9, no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones. Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.

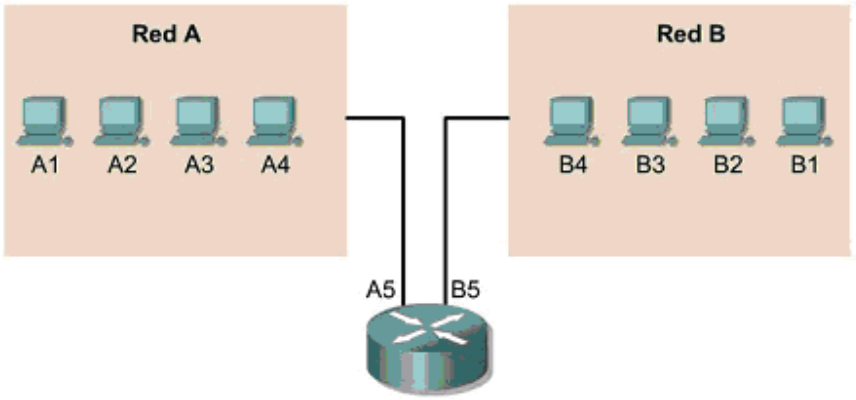


Figura 9.9 Direccionamiento IP

Una computadora puede estar conectada a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión dla computadora a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadoras localicen el dispositivo en una determinada red. La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computadora conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP.

Esta dirección, que opera en la Capa 3, permite que una computadora localice otro computadora en la red. Todas las computadoras también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

9.2.2 Conversión decimal y binaria

Son muchas las formas de resolver un problema. Además, existen varias formas de convertir números decimales en números binarios. Uno de los métodos se presenta a continuación, sin embargo no es el único.

Al convertir un número decimal a binario, se debe determinar la mayor potencia de dos que pueda caber en el número decimal. Figura 11, Si se ha diseñado este proceso para trabajar con computadoras, el punto de inicio más lógico son los valores más altos que puedan caber en uno o dos bytes.

Como se mencionó anteriormente, el agrupamiento más común de bits es de ocho, que componen un byte. Sin embargo, a veces el valor más alto que un byte puede contener no es lo suficientemente alto para los valores requeridos.

Para adaptarse a esta circunstancia, se combinan los bytes. En lugar de tener dos números de ocho dígitos, se crea un solo número de 16 bits. En lugar de tener tres números de ocho dígitos, se crea un número de 24 bits.

Las mismas reglas se aplican de la misma forma a los números de ocho bits. Multiplique el valor de la posición previa por dos para obtener el presente valor de columna.

Ya que el trabajo con computadoras, a menudo, se encuentra referenciado por los bytes, resulta más sencillo comenzar con los límites del byte y comenzar a calcular desde allí. Primero hay que calcular un par de ejemplos, el primero de 6 783.

Como este número es mayor a 255, el valor más alto posible en un solo byte, se utilizarán dos bytes. Comience a calcular desde 2^{15}. El equivalente binario de 6 783 es 00011010 01111111.

El segundo ejemplo es 104. Como este número es menor a 255, puede representarse con un byte. El equivalente binario de 104 es 01101000. Figura 12

Este método funciona con cualquier número decimal. Considere el número decimal un millón. Como un millón es mayor que el valor más alto que puede caber en dos bytes, 65535, se necesitarán por lo menos tres bytes. Multiplicando por dos hasta llegar a 24 bits, se llega a los tres bytes, el valor será de 8 388 608.

Esto significa que el valor más alto que puede caber en 24 bits es de 16 777 215. De modo que comenzando en los 24 bits, siga el proceso hasta llegar al cero. Si se continúa con el procedimiento descripto, se llega a determinar que el número decimal un millón es equivalente al número binario 00001111 01000010 01000000.

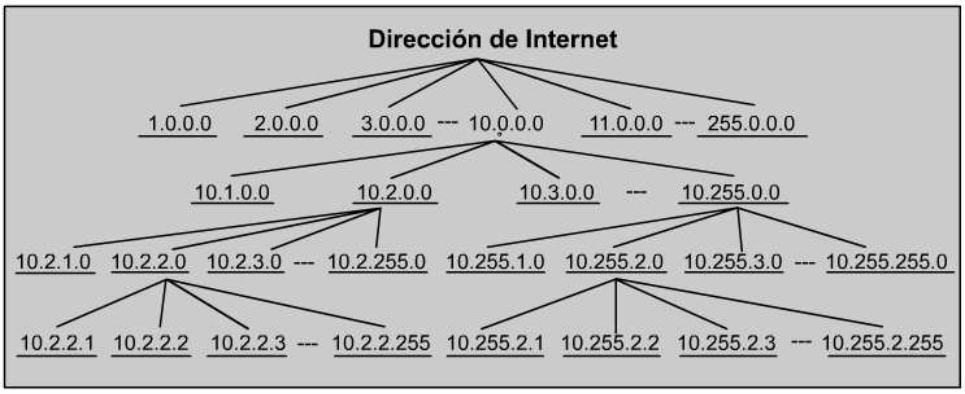


Figura 9.12 Dirección jerárquica

Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser un número exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la parte del host, identifica qué máquina en particular de la red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Figura 9.13. El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Clase de dirección	Cantidad de redes	Cantidad de hosts por red
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	No es aplicable	No es aplicable

Clase de dirección IP:	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0 - 127 *	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

Figura 9.13 Asignación de clases en direcciones IP

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal. El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Figura 9.17. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.

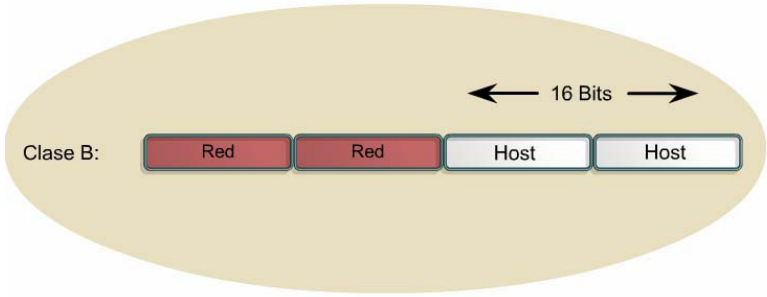


Figura 9.17 Dirección Clase B

Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Figura 9.18. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.

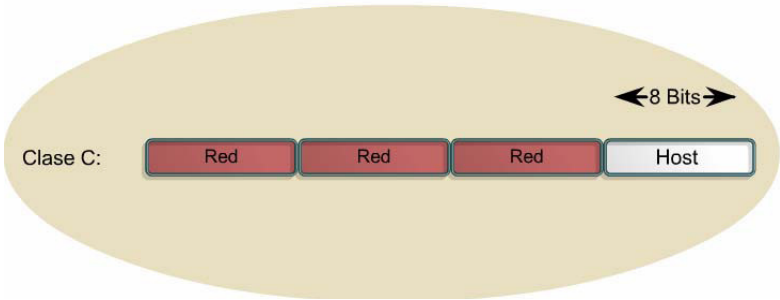


Figura 9.18 Dirección clase C

Rango de las direcciones IP, Figura 9.21, del primer octeto tanto en decimales como en binarios para cada clase de dirección IP.

Clase de dirección IP	Intervalo de dirección IP (Valor decimal d
Clase A	1-126 (00000001-01111110) *
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Figura 9.21 Rango de Direcciones IP

9.2.5 Direcciones IP reservadas

Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:

- **Dirección de red:** Utilizada para identificar la red en sí.

En la Figura 9.21, la sección que está identificada en el casillero superior representa la red 198.150.11.0.

Los datos enviados a cualquier Host de dicha red:

(198.150.11.1- 198.150.11.254)

Se verá desde afuera de la red del área local con la dirección: 198.159.11.0.

Los números del host sólo tienen importancia cuando los datos se encuentran en una red de área local. La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que el número de la red es 198.150.12.0.

- **Dirección de broadcast:** Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.

En la Figura 9.21, la sección que se identifica en el casillero superior representa la dirección de broadcast 198.150.11.255. Todos los hosts de la red leerán los datos enviados a la dirección de broadcast (198.150.11.1- 198.150.11.254).

En una dirección de red Clase B, los primeros dos octetos se designan como porción de red. Los últimos dos octetos contienen ceros, dado que esos 16 bits corresponden a los números de host y se utilizan para identificar los dispositivos que están conectados a la red. La dirección IP, 176.10.0.0, es un ejemplo de una dirección de red. Esta dirección nunca se asigna como dirección de host. Una dirección de host para un dispositivo conectado a la red 176.10.0.0 podría ser 176.10.16.1. En este ejemplo, "176.10" es la parte de RED y "16.1" es la parte de host.

Para enviar información a todos los dispositivos de l red, se necesita una dirección de broadcast. Figura 9.23 Un broadcast se produce cuando una fuente envía datos a todos los dispositivos de una red. Para asegurar que todos los demás dispositivos de una red procesen el broadcast, el transmisor debe utilizar una dirección IP destino que ellos puedan reconocer y procesar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host.

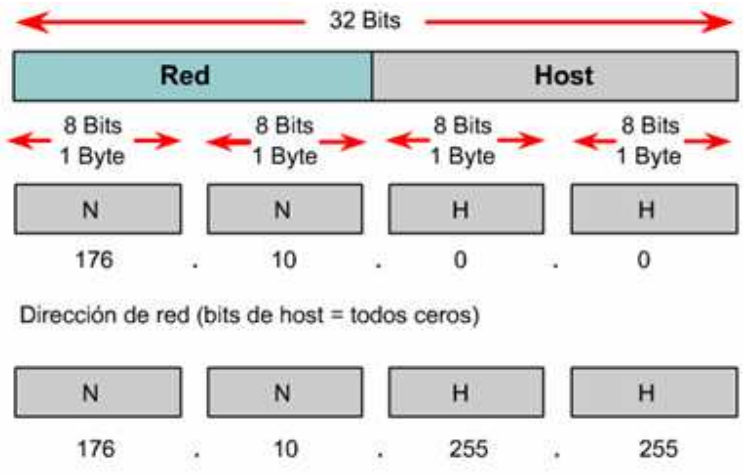


Figura 9.23 Dirección de broadcast

En el ejemplo de la red, 176.10.0.0, los últimos 16 bits componen el campo del host o la parte de la dirección del host. El broadcast que se envía a todos los dispositivos de la red incluye una dirección destino de 176.10.255.255. Esto se produce porque 255 es el valor decimal de un octeto que contiene 11111111.

9.2. 6 Direcciones IP públicas y privadas

La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente. En la Figura 9.24, se muestran ciertos aspectos del esquema del direccionamiento de red. Al observar las redes, ambas tienen la dirección 198.150.11.0.

Las direcciones IP privadas son otra solución al problema del inminente agotamiento de las direcciones IP públicas. Como ya se ha mencionado, las redes públicas requieren que los hosts tengan direcciones IP únicas. Sin embargo, las redes privadas que no están conectadas a la Internet pueden utilizar cualquier dirección de host, siempre que cada host dentro de la red privada sea exclusivo. Existen muchas redes privadas junto con las redes públicas. Sin embargo, no es recomendable que una red privada utilice una dirección cualquiera debido a que, con el tiempo, dicha red podría conectarse a Internet. El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado, como se muestra en la tabla, Estos tres bloques consisten en una dirección de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C. Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los Routers de Internet descartan inmediatamente las direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, un laboratorio de prueba o una red doméstica, es posible utilizar las direcciones privadas en lugar de direcciones exclusivas a nivel global. Figura 9.25 Las direcciones IP privadas pueden entremezclarse, como muestra el gráfico, con las direcciones IP públicas. Así, se conservará el número de direcciones utilizadas para conexiones internas.

Direcciones IP

Clase	Intervalo de direcciones internas RFC 1918
A	10.0.0.0 A 10.255.255.255
B	172.16.0.0 A 172.31.255.255
C	192.168.0.0 A 192.168.255.255

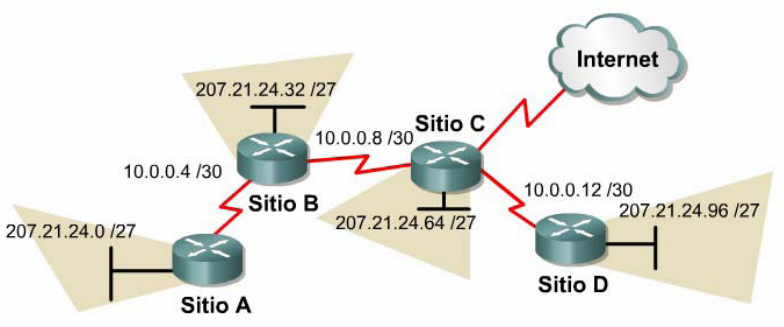


Figura 9.25 Direcciones IP públicas

La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un Router es el dispositivo que realiza la NAT. NAT, junto con CIDR e IPv6 se describen con mayor detalle más adelante en el currículo.

9.2.8 IPv4 en comparación con IPv6

Cuando se adoptó TCP/IP en los años 80, dependía de un esquema de direccionamiento de dos niveles. En ese entonces, esto ofrecía una escalabilidad adecuada. Desafortunadamente, los diseñadores de TCP/IP no pudieron predecir que, con el tiempo, su protocolo sostendría una red global de información, comercio y entretenimiento. Hace más de viente años, la Versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones.

Las direcciones Clase A y B forman un 75 por ciento del espacio de direccionamiento IPv4, sin embargo, se pueden asignar menos de 17 000 organizaciones a un número de red Clase A o B. Las direcciones de red Clase C son mucho más numerosas que las direcciones Clase A y B aunque ellas representan sólo el 12,5 por ciento de los cuatro mil millones de direcciones IP posibles.

Lamentablemente, las direcciones Clase C están limitadas a 254 hosts utilizables. Esto no satisface las necesidades de organizaciones más importantes que no pueden adquirir una dirección Clase A o B. Aún si hubiera más direcciones Clase A, B y C, muchas direcciones de red harían que los Routers se detengan debido a la carga del enorme tamaño de las tablas de enrutamiento, necesarias para guardar las rutas de acceso a cada una de las redes.

Ya en 1992, la Fuerza de tareas de ingeniería de Internet (IETF) identificó las dos dificultades siguientes:

- Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.

- Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits. Dos de las más importantes son las máscaras de subred y el enrutamiento entre dominios sin clase (CIDR), que se tratan con mayor detalle en lecciones posteriores.

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). Figura 2. IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones.

Este protocolo es un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien en forma conjunta y sean tratadas como grupos. Estos grupos de direcciones posibilitan una eficiente transferencia de datos a través de la Internet.

Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente. Como muestra la Figura 9.26, los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.

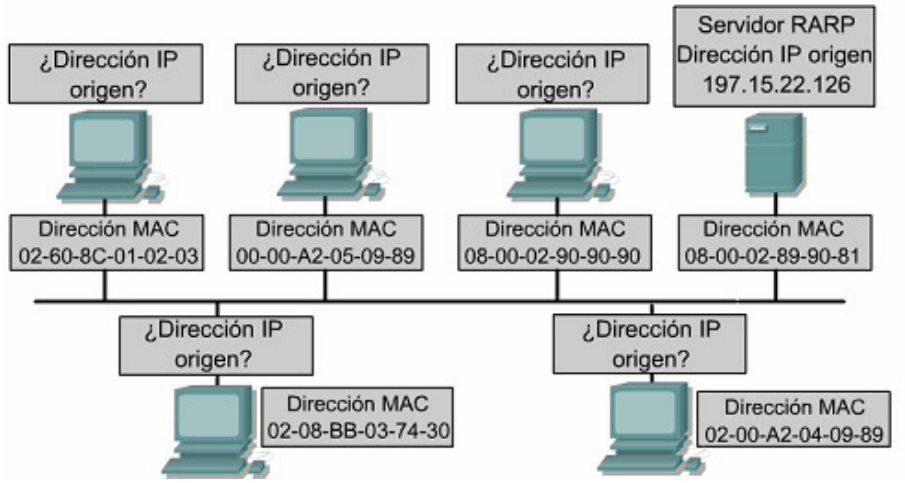


Figura 9.26 Direccionamiento estático y dinámico

9.3.2 Asignación estática de una dirección IP

La asignación estática funciona mejor en las redes pequeñas con poca frecuencia de cambios. De forma manual, el administrador del sistema asigna y rastrea las direcciones IP para cada computadora, impresora o servidor de una red interna. Es fundamental llevar un buen registro para evitar que se produzcan problemas con las direcciones IP repetidas. Esto es posible sólo cuando hay una pequeña cantidad de dispositivos que rastrear.

Los servidores deben recibir una dirección IP estática de modo que las estaciones de trabajo y otros dispositivos siempre sepan cómo acceder a los servicios requeridos. Considere lo difícil que sería realizar un llamado telefónico a un lugar que cambiara de número todos los días.

Otros dispositivos que deben recibir direcciones IP estáticas son las impresoras en red, servidores de aplicaciones y Routers.

9.3.5 Administración de direcciones DHCPIP

El Protocolo de configuración dinámica del host (DHCP) es el sucesor del BOOTP. A diferencia del BOOTP, el DHCP permite que el host obtenga la dirección IP de forma dinámica sin que el administrador de red tenga que configurar un perfil individual para cada dispositivo. Lo único que se requiere para utilizar el DHCP es un rango definido de direcciones IP en un servidor DHCP. A medida que los hosts entran en línea, se comunican con el servidor DHCP y solicitan una dirección. El servidor DHCP elige una dirección y se la arrienda a dicho host. Con DHCP, la configuración completa de las red se puede obtener en un mensaje. Esto incluye todos los datos que proporciona el mensaje BOOTP más una dirección IP arrendada y una máscara de subred.

La principal ventaja que el DHCP tiene sobre el BOOTP es que permite que los usuarios sean móviles. Esta mobilidad permite que los usuarios cambien libremente las conexiones de red de un lugar a otro. Ya no es necesario mantener un perfil fijo de cada dispositivo conectado a la red como en el caso del sistema BOOTP. La importancia de este avance del DHCP es su capacidad de arrendar una dirección IP a un dispositivo y luego reclamar dicha dirección IP para otro usuario una vez que el primero la libera. Esto siginifica que DHCP puede asignar una dirección IP disponible a cualquiera que se conecte a la red.

9.3.6 Problemas en la resolución de direcciones

Uno de los principales problemas del networking es cómo comunicarse con los otros dispositivos de la red. En la comunicación TCP/IP, el datagrama de una red de área local debe contener tanto una dirección MAC destino como una dirección IP destino.

Estas direcciones deben ser correctas y concordar con las direcciones IP y MAC destino del dispositivo host. Si no concuerdan, el host destino descartará el datagrama. La comunicación dentro de un segmento de LAN requiere de dos direcciones.

Debe haber una forma de mapear las direcciones IP a MAC de forma automática. Se necesitaría demasiado tiempo si el usuario creara los mapas de forma manual. El conjunto TCP/IP cuenta con un protocolo, llamado Protocolo de resolución de direcciones (ARP), que puede obtener las direcciones MAC, de forma automática, para la transmisión local. Pueden surgir diferentes problemas cuando se manda información fuera de la LAN.

Las comunicaciones entre dos segmentos de LAN tienen una tarea extra. Tanto las direcciones IP como las MAC son necesarias para el dispositivo de enrutamiento intermedio y el host destino. TCP/IP tiene una variante en ARP llamada ARP proxy que proporciona la dirección MAC de un dispositivo intermedio para realizar la transmisión a otro segmento de la red fuera de la LAN.

El Router responde con direcciones MAC para aquellas peticiones en las que la dirección IP no se encuentra en el rango de direcciones de la subred local.

Otro método para enviar datos a la dirección de un dispositivo que se encuentra en otro segmento de red consiste en configurar un gateway por defecto. El Gateway por defecto es una opción de host en la que la dirección IP de la interfaz del Router se guarda en la configuración de red del host. El host origen compara la dirección IP destino y su propia dirección IP para determinar si las dos direcciones están ubicadas en el mismo segmento. Si el host receptor no está en el mismo segmento, el host origen envía los datos utilizando la dirección IP real del destino y la dirección MAC del Router. La dirección MAC para el Router se obtuvo de la tabla ARP utilizando la dirección IP de dicho Router.

Si el gateway por defecto del host o la característica ARP proxy del Router no están configurados, el tráfico no podrá salir de la red del área local. Es necesario el uno o el otro para tener una conexión fuera de la red del área local.

CAPITULO 10: Principios básicos de enrutamiento y subredes

A medida que la información fluye hacia abajo por las capas del modelo OSI, los datos se procesan en cada capa. En la capa de red, los datos se encapsulan en paquetes, también denominados datagramas. IP determina los contenidos de cada encabezado de paquete IP, lo cual incluye el direccionamiento y otra información de control, pero no se preocupa por la información en sí. IP acepta todos los datos que recibe de las capas superiores.

10.1.3 Propagación y conmutación de los paquetes dentro del Router

A medida que un paquete pasa por la internetwork a su destino final, los encabezados y la información final de la trama de Capa 2 se eliminan y se remplazan en cada dispositivo de Capa 3. Figura 10.1. Esto sucede porque las unidades de datos de Capa 2, es decir, las tramas, son para direccionamiento local. Las unidades de datos de Capa 3 (los paquetes) son para direccionamiento de extremo a extremo.

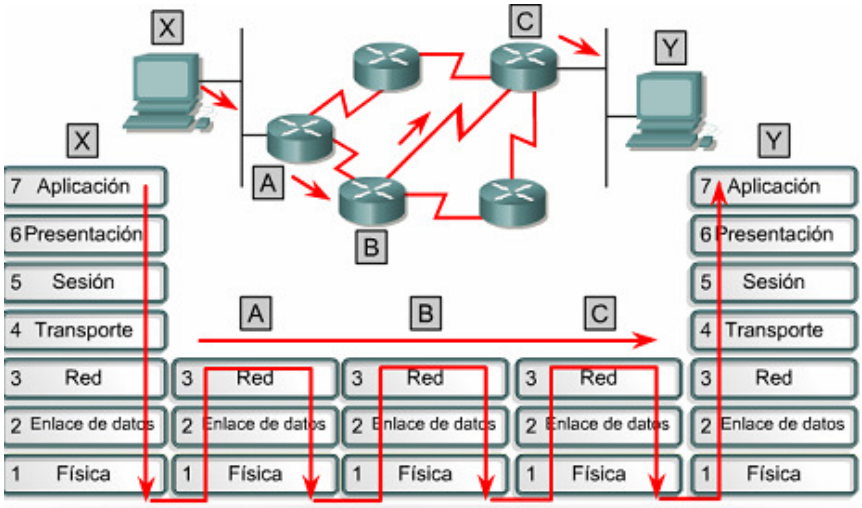


Figura 10.1 Propagación y conmutación de los paquetes

Las tramas de Ethernet de Capa 2 están diseñadas para operar dentro de un dominio de broadcast utilizando la dirección MAC que está grabada en del dispositivo físico. Otros tipos de tramas de Capa 2 incluyen los enlaces seriales del protocolo punto a punto (PPP) y las conexiones de Frame Relay, que utilizan esquemas de direccionamiento de Capa 2 diferentes. No obstante el tipo de direccionamiento de Capa 2 utilizado, las tramas están diseñadas para operar dentro del dominio de broadcast de Capa 2, y cuando los datos atraviesan un dispositivo de Capa 3, la información de Capa 2 cambia.

En el momento en que se recibe una trama en la interfaz del Router, se extrae la dirección MAC destino. Se revisa la dirección para ver si la trama se dirige directamente a la interfaz del Router, o si es un broadcast. En cualquiera de los dos casos se acepta la trama. De lo contrario, se descarta la trama ya que está destinada a otro dispositivo en el dominio de colisión.

IP es el principal protocolo ruteado, pero no el único. TCP agrega a IP servicios de Capa 4 confiables orientados a conexión.

10.1.5 Anatomía de un paquete IP

Los paquetes IP constan de los datos de las capas superiores más el encabezado IP. El encabezado IP está formado por lo siguiente:

- **Versión:** Especifica el formato del encabezado de IP. Este campo de cuatro bits contiene el número 4 si el encabezado es IPv4 o el número 6 si el encabezado es IPV6. Sin embargo este campo no se usa para distinguir entre ambas versiones, para esto se usa el campo de tipo que se encuentra en el encabezado de la trama de capa 2.
- **Longitud del encabezado IP (HLEN):** Indica la longitud del encabezado del datagrama en palabras de 32 bits. Este número representa la longitud total de toda la información del encabezado, e incluye los dos campos de encabezados de longitud variable.
- **Tipo de servicio (TOS):** Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular, 8 bits.
- **Longitud total:** Especifica la longitud total de todo el paquete en bytes, incluyendo los datos y el encabezado, 16 bits. Para calcular la longitud de la carga de datos reste HLEN a la longitud total.
- **Identificación:** Contiene un número entero que identifica el datagrama actual, 16 bits. Este es el número de secuencia.
- **Señaladores:** Un campo de tres bits en el que los dos bits de menor peso controlan la fragmentación. Un bit especifica si el paquete puede fragmentarse, y el otro especifica si el paquete es el último fragmento en una serie de paquetes fragmentados.
- **Desplazamiento de fragmentos:** usado para ensamblar los fragmentos de datagramas, 13 bits. Este campo permite que el campo anterior termine en un límite de 16 bits.
- **Tiempo de existencia (TTL):** campo que especifica el número de saltos que un paquete puede recorrer. Este número disminuye por uno cuando el paquete pasa por un Router. Cuando el contador llega a cero el paquete se elimina. Esto evita que los paquetes entren en un loop (bucle) interminable.
- **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.
- **Checksum del encabezado:** ayuda a garantizar la integridad del encabezado IP, 16 bits.
- **Dirección de origen:** especifica la dirección IP del nodo emisor, 32 bits.
- **Dirección de destino:** especifica la dirección IP del nodo receptor, 32 bits.
- **Opciones:** permite que IP admita varias opciones, como seguridad, longitud variable.
- **Relleno:** se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits
- **Datos:** contiene información de capa superior, longitud variable hasta un de máximo 64 Kb.

Los Routers interconectan segmentos de red o redes enteras. Pasan tramas de datos entre redes basándose en la información de Capa 3. Los Routers toman decisiones lógicas con respecto a cuál es la mejor ruta para la entrega de datos. Luego dirigen los paquetes al puerto de salida adecuado para que sean encapsulados para la transmisión.

Los pasos del proceso de encapsulamiento y desencapsulamiento ocurren cada vez que un paquete atraviesa un router. El router debe desencapsular la trama de capa 2 y examinar la dirección de capa 3. Como se muestra en la figura 10.3, el proceso completo del envío de datos de un dispositivo a otro comprende encapsulamiento y desencapsulamiento de las siete capas OSI.

Este proceso divide el flujo de datos en segmentos, agrega los encabezados apropiados e información final y luego transmite los datos. El proceso de desencapsulamiento es el proceso inverso: quita los encabezados e información final, y luego combina los datos en un flujo continuo.

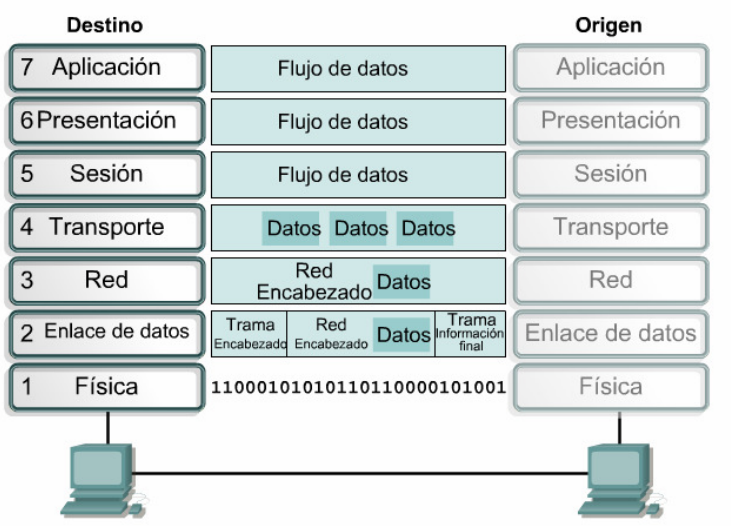


Figura 10.3 Encapsulamiento y desencapsulamiento

Otros ejemplos de protocolos enrutables incluyen IPX/SPX y AppleTalk. Estos protocolos admiten la Capa 3. Los protocolos no enrutables no admiten la Capa 3. El protocolo no enrutable más común es el NetBEUI. NetBeui es un protocolo pequeño, veloz y eficiente que está limitado a la entrega de tramas de un segmento.

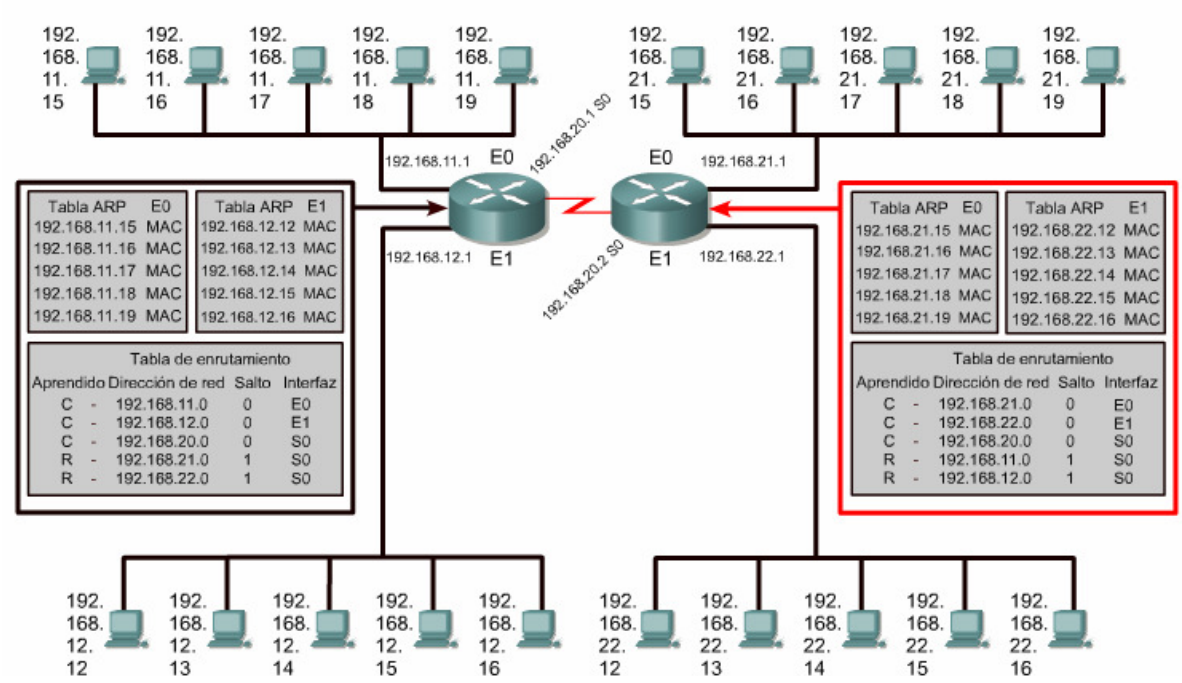


Figura 10.5 Tablas ARP de las direcciones MAC de Capa 2 y las tablas de enrutamiento de las direcciones IP de Capa 3

Los switches Capa 2 construyen su tabla usando direcciones MAC. Cuando un host va a mandar información a una dirección IP que no es local, entonces manda la trama al router más cercano., también conocida como su Gateway por defecto. El Host utiliza las direcciones MAC del Router como la dirección MAC destino.

Un switch interconecta segmentos que pertenecen a la misma red o subred lógicas. Para los host que no son locales, el switch reenvía la trama a un router en base a la dirección MAC destino. El router examina la dirección destino de Capa 3 para llevar a cabo la decisión de la mejor ruta. El host X sabe la dirección IP del router puesto que en la configuración del host se incluye la dirección del Gateway por defecto.

Únicamente un switch mantiene una tabla de direcciones MAC conocidas, el router mantiene una tabla de direcciones IP. Las direcciones MAC no están organizadas de forma lógica. Las IP están organizadas de manera jerárquica.

Un switch soporta un número limitado de direcciones MAC desorganizadas debido a que sólo tiene que buscar direcciones MAC que están dentro de su segmento. Los Routers necesitan administrar un mayor volumen de direcciones. Entonces, los Routers necesitan un sistema de direccionamiento organizado que pueda agrupar direcciones similares y tratarlas como una sola unidad de red hasta que los datos alcancen el segmento destino.

10.2.4 Determinación de la ruta

La determinación de la ruta ocurre a nivel de la capa de red. La determinación de la ruta permite que un Router compare la dirección destino con las rutas disponibles en la tabla de enrutamiento, y seleccione la mejor ruta. Los Routers conocen las rutas disponibles por medio del enrutamiento estático o dinámico. Las rutas configuradas de forma manual por el administrador de la red son las rutas estáticas. Las rutas aprendidas por medio de otros Routers usando un protocolo de enrutamiento son las rutas dinámicas.

El Router utiliza la determinación de la ruta para decidir por cuál puerto debe enviar un paquete en su trayecto al destino. Este proceso se conoce como enrutamiento del paquete. Cada Router que un paquete encuentra a lo largo del trayecto se conoce como salto. El número de saltos es la distancia cubierta. La determinación de la ruta puede compararse a una persona que conduce un automóvil desde un lugar de la ciudad a otro. El conductor tiene un mapa que muestra las calles que puede tomar para llegar a su destino, así como el Router posee una tabla de enrutamiento. El conductor viaja desde una intersección a otra al igual que un paquete va de un Router a otro en cada salto. En cualquier intersección el conductor determinar su ruta al ir hacia la izquierda, la derecha, o avanzar derecho. Del mismo modo, un Router decide por cuál puerto de salida debe enviarse un paquete.

Las decisiones del conductor se ven influenciadas por múltiples factores como el tráfico en la calle, el límite de velocidad, el número de carriles, si hay peaje o no, y si esa ruta se encuentra cerrada o no con frecuencia. A veces es más rápido tomar un recorrido más largo por una calle más angosta y menos transitada que ir por una autopista con mucho tránsito. De la misma forma, los Routers pueden tomar decisiones basándose en la carga, el ancho de banda, el retardo, el costo y la confiabilidad en los enlaces de red.

Se utiliza el siguiente proceso durante la determinación de la ruta para cada paquete que se enruta:

- El router compara la dirección IP del paquete recibido contra las tablas que tiene.
- Se obtiene la dirección destino del paquete .
- Se aplica la máscara de la primera entrada en la tabla de enrutamiento a la dirección destino.
- Se compara el destino enmascarado y la entrada de la tabla de enrutamiento.
- Si hay concordancia, el paquete se envía al puerto que está asociado con la entrada de la tabla.
- Si no hay concordancia, se compara con la siguiente entrada de la tabla.
- Si el paquete no concuerda con ninguno de las entradas de la tabla, el Router verifica si se envió una ruta por defecto.
- Si se envió una ruta por defecto, el paquete se envía al puerto asociado. Una ruta por defecto es aquella que está configurada por el administrador de la red como la ruta que debe usarse si no existe concordancia con las entradas de la tabla de enrutamiento.
- El paquete se elimina si no hay una ruta por defecto. Por lo general se envía un mensaje al dispositivo emisor que indica que no se alcanzó el destino.

- **Métrica de enrutamiento:** los distintos protocolos de enrutamiento utilizan métricas de enrutamiento distintas. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta. Por ejemplo, el números de saltos es la única métrica de enrutamiento que utiliza el protocolo de información de enrutamiento (RIP). El Protocolo de enrutamiento Gateway interior (IGRP) utiliza una combinación de ancho de banda, carga, retardo y confiabilidad como métricas para crear un valor métrico compuesto.
- **Interfaces de salida:** la interfaz por la que se envían los datos para llegar a su destino final.

Los Routers se comunican entre sí para mantener sus tablas de enrutamiento por medio de la transmisión de mensajes de actualización del enrutamiento. Algunos protocolos de enrutamiento transmiten estos mensajes de forma periódica, mientras que otros lo hacen cuando hay cambios en la topología de la red. Algunos protocolos transmiten toda la tabla de enrutamiento en cada mensaje de actualización, y otros transmiten sólo las rutas que se han modificado. Un Router crea y guarda su tabla de enrutamiento, analizando las actualizaciones de enrutamiento de los Routers vecinos.

10.2.6 Algoritmos de enrutamiento y métricas

Un algoritmo es una solución detallada a un problema. En el caso de paquetes de enrutamiento, diferentes protocolos utilizan distintos algoritmos para decidir por cuál puerto debe enviarse un paquete entrante. Los algoritmos de enrutamiento dependen de las métricas para tomar estas decisiones. Los protocolos de enrutamiento con frecuencia tienen uno o más de los siguientes objetivos de diseño:

- **Optimización:** la optimización describe la capacidad del algoritmo de enrutamiento de seleccionar la mejor ruta. La mejor ruta depende de las métricas y el peso de las métricas que se usan para hacer el cálculo. Por ejemplo, un algoritmo puede utilizar tanto las métricas del número de saltos como la del retardo, pero puede considerar las métricas de retardo como de mayor peso en el cálculo.
- **Simplicidad y bajo gasto:** cuanto más simple sea el algoritmo, más eficientemente será procesado por la CPU y la memoria del Router. Esto es importante ya que la red puede aumentar en grandes proporciones, como la Internet.
- **Solidez y estabilidad:** un algoritmo debe funcionar de manera correcta cuando se enfrenta con una situación inusual o desconocida; por ejemplo, fallas en el hardware, condiciones de carga elevada y errores en la implementación.
- **Flexibilidad:** un algoritmo de enrutamiento debe adaptarse rápidamente a una gran variedad de cambios en la red. Estos cambios incluyen la disponibilidad y memoria del Router, cambios en el ancho de banda y retardo en la red.
- **Convergencia rápida:** la convergencia es el proceso en el cual todos los Routers llegan a un acuerdo con respecto a las rutas disponibles. Cuando un evento en la red provoca cambios en la disponibilidad de los Routers, se necesitan actualizaciones para restablecer la conectividad en la red. Los algoritmos de enrutamiento que convergen lentamente pueden hacer que los datos no puedan enviarse.

Los IGP enrutan datos dentro de un sistema autónomo.

- Protocolo de información de enrutamiento (RIP) y (RIPv2).
- Protocolo de enrutamiento de Gateway interior (IGRP)
- Protocolo de enrutamiento de Gateway interior mejorado (EIGRP)
- Primero la ruta libre más corta (OSPF)
- Protocolo de sistema intermedio-sistema intermedio (IS-IS).
-

Los EGP enrutan datos entre sistemas autónomos. Un ejemplo de EGP es el protocolo de Gateway fronterizo (BGP).

10.2.8 Estado de Enlace y Vector de Distancia

Los protocolos de enrutamiento pueden clasificarse en IGP o EGP, lo que describe si un grupo de Routers se encuentra bajo una sola administración o no. Los IGP pueden a su vez clasificarse en protocolos de vector-distancia o de estado de enlace.

El enrutamiento por vector-distancia determina la dirección y la distancia (vector) hacia cualquier enlace en la internetwork. La distancia puede ser el número de saltos hasta el enlace. Los Routers que utilizan los algoritmos de vector-distancia envían todos o parte de las entradas de su tabla de enrutamiento a los Routers adyacentes de forma periódica. Esto sucede aún si no ha habido modificaciones en la red.

Un Router puede verificar todas las rutas conocidas y realizar las modificaciones a su tabla de enrutamiento al recibir las actualizaciones de enrutamiento. Este proceso también se llama "enrutamiento por rumor". La comprensión que el Router tiene de la red se basa en la perspectiva que tiene el Router adyacente de la topología de la red.

Los ejemplos de los protocolos por vector-distancia incluyen los siguientes:

- **Protocolo de información de enrutamiento(RIP):** es el IGP más común de la red. RIP utiliza números de saltos como su única métrica de enrutamiento.
- **Protocolo de enrutamiento de Gateway interior (IGRP):** es un IGP desarrollado por Cisco para resolver problemas relacionados con el enrutamiento en redes extensas y heterogéneas.

- **IGRP mejorada (EIGRP):** esta IGP propiedad de Cisco incluye varias de las características de un protocolo de enrutamiento de estado de enlace. Es por esto que se ha conocido como protocolo híbrido balanceado, pero en realidad es un protocolo de enrutamiento vector-distancia avanzado.

Los protocolos de enrutamiento de estado de enlace se diseñaron para superar las limitaciones de los protocolos de enrutamiento vector distancia. Los protocolos de enrutamiento de estado de enlace responden rápidamente a las modificaciones en la red, enviando actualizaciones sólo cuando se producen las modificaciones.

El sistema intermedio-sistema intermedio (IS-IS) es un protocolo de enrutamiento de estado de enlace utilizado para protocolos enrutados distintos a IP. El IS-IS integrado es un sistema de implementación expandido de IS-IS que admite varios protocolos de enrutamiento, inclusive IP.

Cisco es propietario de EIGRP y también IGRP. EIGRP es una versión mejorada de IGRP. En especial, EIGRP suministra una eficiencia de operación superior tal como una convergencia rápida y un bajo gasto del ancho de banda. EIGRP es un protocolo mejorado de vector-distancia que también utiliza algunas de las funciones del protocolo de estado de enlace. Por ello, el EIGRP veces aparece incluido en la categoría de protocolo de enrutamiento híbrido.

El protocolo de Gateway fronterizo (BGP) es un ejemplo de protocolo de Gateway exterior (EGP). BGP intercambia información de enrutamiento entre sistemas autónomos a la vez que garantiza una elección de ruta libre de loops.

BGP es el protocolo principal de publicación de rutas utilizado por las compañías más importantes e ISP en la Internet. BGP4 es la primera versión de BGP que admite enrutamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de Gateway internos (IGP), como RIP, OSPF y EIGRP, BGP no usa métricas como número de saltos, ancho de banda, o retardo. En cambio, BGP toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

10.3 Mecanismos de la división en subredes

10.3.1 Clases de direcciones IP de red

Las clases de direcciones IP ofrecen de 256 a 16,8 millones de Hosts. Para administrar de forma eficiente un número limitado de direcciones IP, todas las clases pueden subdividirse en subredes más pequeñas. La Figura 10.7 ofrece una descripción de la división entre redes y Hosts.

Clase A	Red	Host		
Octeto	1	2	3	4

Clase B	Red		Host	
Octeto	1	2	3	4

Clase C	Red			Host
Octeto	1	2	3	4

Clase D	Host			
Octeto	1	2	3	4

Figura 10.7 División entre redes y Hosts

La máscara de subred da al Router la información necesaria para determinar en qué red y subred se encuentra un Host determinado. Figura 2 La máscara de subred se crea mediante el uso de 1s binarios en los bits de red. Los bits de subred se determinan mediante la suma de los valores de las posiciones donde se colocaron estos bits.

Si se pidieron prestados tres bits, la máscara para direcciones de Clase C sería 255.255.255.224. Como se muestra en a Figura 10.8. Esta máscara se puede representar con una barra inclinada seguida por un número, por ejemplo /27. El número representa el número total de bits que fueron utilizados por la red y la porción de subred.

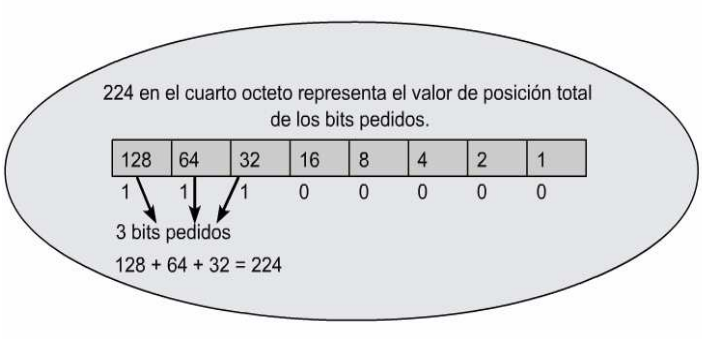


Figura 10.8 Mascara de direcciones clase C

Para determinar el número de bits que se deberán utilizar, el diseñador de redes calcula cuántos Hosts necesita la subred más grande y el número de subredes necesarias. Como ejemplo, la red necesita 30 Hosts y cinco subredes.

Una manera más fácil de calcular cuántos bits reasignar es utilizar la tabla de subrees como se muestra en la Figura 10.9.

Formato de barra diagonal	/25	/26	/27	/28	/29	/30	No es aplicable	No es aplicable
Máscara	128	192	224	240	248	252	254	255
Bits pedidos	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1
Subredes totales		4	8	16	32	64		
Subredes que se pueden utilizar		2	6	14	30	62		
Hosts totales		64	32	16	8	4		
Hosts que se pueden utilizar		62	30	14	6	2		

Figura 10.9 Tabla de subredes

Subred N	ID de subred	Rango de hos	ID de broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Figura 10.10 Esquema de Subred

Al llenar la tabla de subred, tres de los campos son automáticos, otros requieren de cálculos. El ID de subred de la subred 0 equivale al número principal de la red, en este caso 192.168.10.0. El ID de broadcast de toda la red es el máximo número posible, en este caso 192.168.10.255. El tercer número representa el ID de subred para la subred número siete. Este número consiste en los tres octetos de red con el número de máscara de subred insertado en la posición del cuarto octeto. Se asignaron tres bits al campo de subred con un valor acumulativo de 224. El ID de la subred siete es 192.168.10.224. Al insertar estos números, se establecen puntos de referencia que verificarán la exactitud cuando se complete la tabla.

10.3.5 Como dividir las redes de Clase A y B en subredes

El procedimiento de dividir las redes de Clase A y B en subredes es idéntico al proceso utilizado para la Clase C, excepto que puede haber muchos más bits involucrados. Hay 22 bits disponibles para asignación a los campos de subred en una dirección de Clase A, y 14 bits en la de B. Figura 10.11 y Figura 10.12.

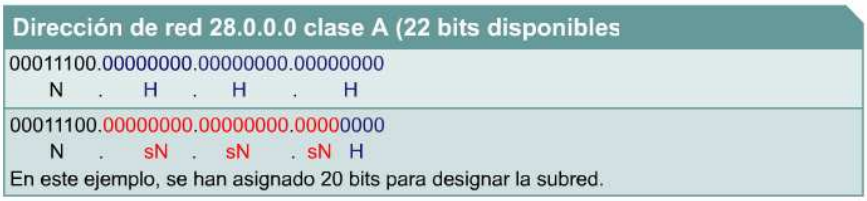


Figura 10.11 División de redes clase A

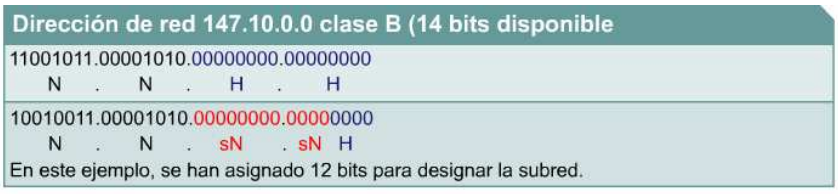


Figura 10.12 Division de redes clase B

Este proceso se administra a un nivel binario. Por lo tanto, es necesario ver la dirección IP y la máscara de forma binaria. Figura 10.14 se realiza la operación "AND"con la dirección IP y la dirección de subred y el resultado es el ID de subred. El Router entonces utiliza esa información para enviar el paquete por la interfaz correcta.

La división en subredes es algo que debe aprenderse. Habrá que dedicar mucho tiempo a la realización de ejercicios prácticos para desarrollar esquemas flexibles y que funcionen. Existe una gran variedad de calculadoras de subredes disponibles en la Web. Sin embargo, un administrador de red debe saber cómo calcular las subredes de forma manual para diseñar esquemas de red efectivos y asegurar la validez de los resultados obtenidos con una calculadora de subred. La calculadora de subred no proporcionará el esquema inicial, sólo el direccionamiento final. Tampoco se permite el uso de calculadoras, de ningúna clase, durante el examen de certificación.

CAPITULO 11: Capa de aplicación y transporte de TCP/IP

11.1.2 Control de flujo

A medida que la capa de transporte envía segmentos de datos, trata de garantizar que los datos no se pierdan. Un host receptor que no puede procesar los datos tan rápidamente como llegan puede provocar una pérdida de datos. El host receptor se ve obligado a descartar los datos. El control de flujo evita el problema que se produce cuando un host que realiza la transmisión inunda los buffers del host destinatario. TCP suministra el mecanismo de control de flujo al permitir que el host emisor y el receptor se comuniquen. Luego los dos hosts establecen velocidades de transferencia de datos que sean aceptables para ambos. Figura 1

11.1.3 Descripción general del establecimiento, mantenimiento y terminación de sesión.

Múltiples aplicaciones pueden compartir la misma conexión de transporte en el modelo de referencia OSI. La funcionalidad de transporte se logra segmento por segmento. En otras palabras, esto significa que las distintas aplicaciones pueden enviar segmentos de datos con un sistema basado en el principio "el primero que llega es el primero que se sale". Los segmentos que llegan primero son los primeros que serán resueltos. Estos segmentos se pueden encaminar hacia el mismo destino o hacia distintos destinos. Varias aplicaciones pueden compartir la misma conexión en los modelos de referencia OSI. Esto se denomina multiplexión de conversaciones de capas superiores. Figura 11.1 Varias conversaciones simultáneas de las capas superiores se pueden multiplexar en una sola conexión.

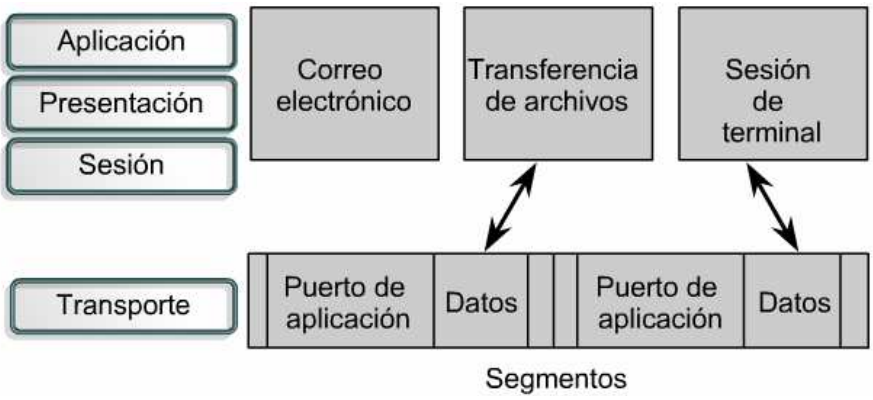


Figura 11.1 multiplexión de conversaciones de capas superiores

Una de las funciones de la capa de transporte es establecer una sesión orientada a conexión entre dispositivos similares en la capa de aplicación. Para que se inicie la transferencia de datos, tanto las aplicaciones emisoras como receptoras informan a sus respectivos sistemas operativos que se iniciará una conexión.

En vez de permitir que se pierda la información, el destino puede enviar un mensaje al origen indicando que no está listo ("not ready"). Este indicador, que funciona como una señal de "pare", indica al emisor que debe dejar de enviar datos. Cuando el receptor está en condiciones de aceptar más datos, envía un indicador de transporte de "listo". Cuando recibe este indicador, el emisor puede reanudar la transmisión de segmentos. Figura 11.3

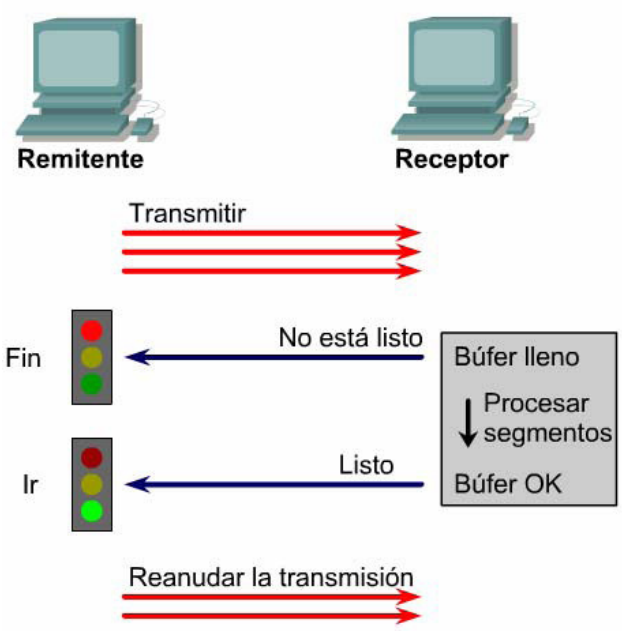


Figura 11.3 Transmisión por segmentos

Al finalizar la transferencia de datos, el host emisor envía una señal que indica que la transmisión ha finalizado. El host receptor ubicado en el extremo de la secuencia de datos acusa recibo del fin de la transmisión y la conexión se termina.

11.1.4 Intercambio de señales de tres vías

TCP es un protocolo orientado a conexión. TCP requiere que se establezca una conexión antes de que comience la transferencia de datos. Para que se establezca o inicialice una conexión, los dos hosts deben sincronizar sus Números de secuencia iniciales (ISN: Initial Sequence Numbers). La sincronización se lleva a cabo a través de un intercambio de segmentos que establecen la conexión al transportar un bit de control denominado SYN (para la sincronización), y los ISN.

Los segmentos que transportan el bit SYN también se denominan "SYN". Esta solución requiere un mecanismo adecuado para elegir un número de secuencia inicial y un proceso levemente complicado para intercambiar los ISN.

La sincronización requiere que ambos lados envíen su propio número de secuencia inicial y que reciban una confirmación del intercambio en un acuse de recibo (ACK) de la otra parte.

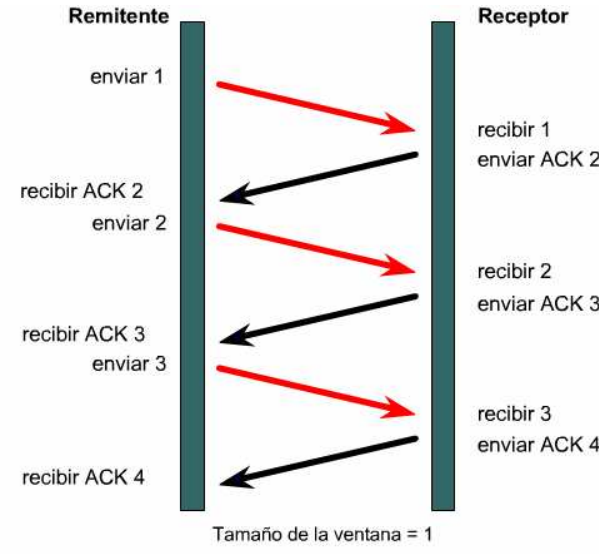


Figura 11.5 Envío de paquete de datos

Si el emisor debe esperar recibir un acuse de recibo luego de enviar cada paquete, el rendimiento es lento. Por lo tanto, la mayoría de los protocolos confiables, orientados a conexión, permiten que haya más de un paquete pendiente en la red a la vez. Como se dispone de tiempo después de que el emisor termina de transmitir el paquete de datos y antes de que el emisor termine de procesar cualquier acuse de recibo, este rango se utiliza para transmitir más datos. El número de paquetes de datos que se permite que un emisor tenga pendientes sin haber recibido un acuse de recibo se denomina "ventana".

TCP usa acuses de recibo expectante. Por "acuses de recibo expectante" se entiende que el número de acuse de recibo se refiere al siguiente paquete esperado. Por "uso de ventanas" se entiende que el tamaño de la ventana se negocia de forma dinámica durante la sesión TCP. El uso de ventanas es un mecanismo de control de flujo. El uso de ventanas requiere que el dispositivo origen reciba un acuse de recibo desde el destino después de transmitir una cantidad determinada de datos. El proceso del TCP receptor indica una "ventana" para el TCP emisor. Esta ventana especifica la cantidad de paquetes, comenzando por el número de acuse de recibo, que el proceso TCP receptor actualmente está preparado para recibir.

Con una ventana de tamaño 3, el origen puede enviar 3 bytes al destino. El origen debe esperar entonces por un acuse de recibo (ACK). Si el destino recibe los 3 bytes, le manda un ACK al origen, el cual ahora ya puede enviar otros 3 bytes. Si el destino NO recibe los tres bytes, por que los buffers tienen un sobreflujo, entonces no manda un ACK. El origen al no recibir el ACK, sabe que tiene que retransmitir los mismos tres bytes que ya había enviado, y la razón de transmisión se decrementa.

La figura 11.7, muestra un emisor que transmite los paquetes de datos 1, 2 y 3. El receptor acusa recibo de los paquetes solicitando el paquete 4. El emisor, al recibir el acuse de recibo, envía los paquetes 4, 5 y 6. Si el paquete 5 no llega a su destino el receptor acusa recibo con una petición para reenviar el paquete 5. El emisor vuelve a enviar el paquete 5 y luego recibe el acuse de recibo antes de transmitir el paquete 7.

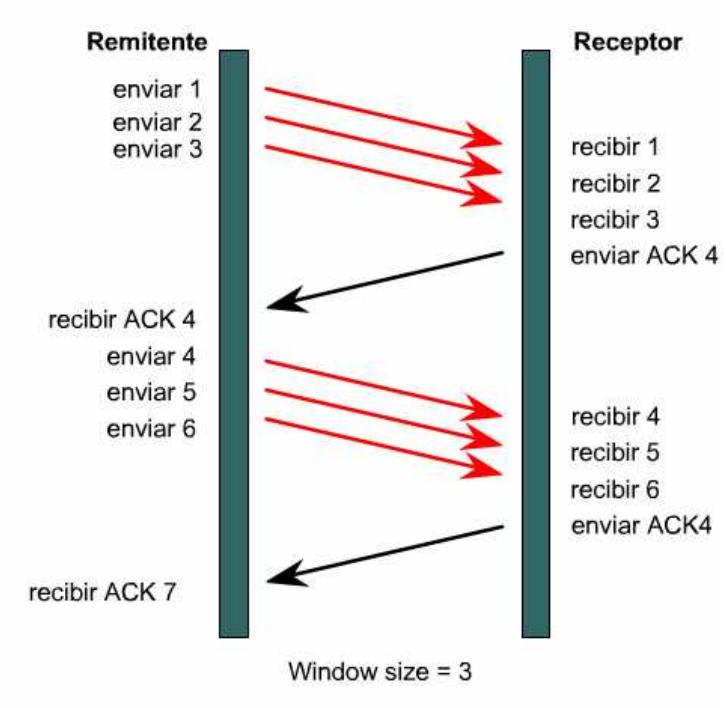


Figura 11.7 Emisor que transmite paquetes de datos

Los protocolos que usan TCP incluyen:

- FTP (Protocolo de transferencia de archivos)
- HTTP (Protocolo de transferencia de hipertexto)
- SMTP (Protocolo simple de transferencia de correo)
- Telnet

Las siguientes son las definiciones de los campos de un segmento TCP: Figura 11.9

- **Puerto origen:** El número del puerto que realiza la llamada.
- **Puerto destino:** El número del puerto al que se realiza la llamada.
- **Número de secuencia:** El número que se usa para asegurar el secuenciamiento correcto de los datos entrantes.
- **Número de acuse de recibo:** Siguiente octeto TCP esperado.
- **HLEN:** La cantidad de palabras de 32 bits del encabezado.
- **Reservado:** Establecido en cero.
- **Bits de código:** Funciones de control, como configuración y terminación de una sesión.
- **Ventana:** La cantidad de octetos que el emisor está dispuesto a aceptar.
- **Checksum (suma de comprobación):** Suma de comprobación calculada a partir de los campos del encabezado y de los datos.
- **Indicador de mensaje urgente:** Indica el final de la transmisión de datos urgentes.
- **Opción:** Una opción definida actualmente, tamaño máximo del segmento TCP.
- **Datos:** Datos de protocolo de capa superior.

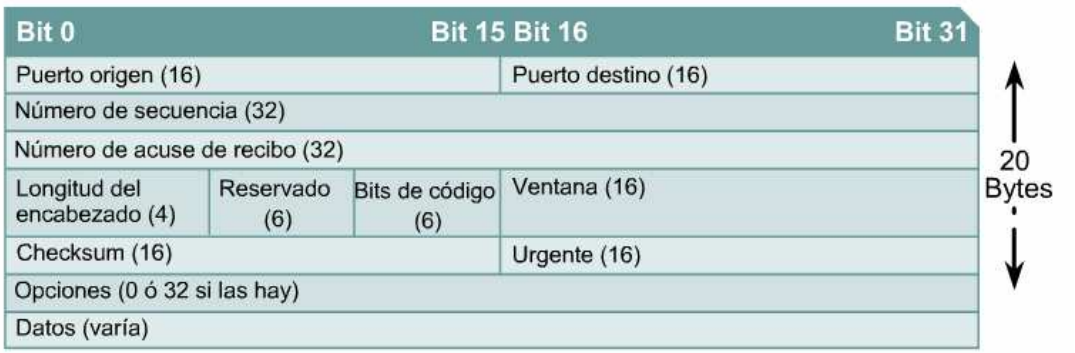


Figura 11.9 campos de un segmento TCP

11.1.9 Numero de puerto TCP y UDP

Tanto TCP como UDP utilizan números de puerto (socket) para enviar información a las capas superiores. Los números de puerto se utilizan para mantener un registro de las distintas conversaciones que atraviesan la red al mismo tiempo.

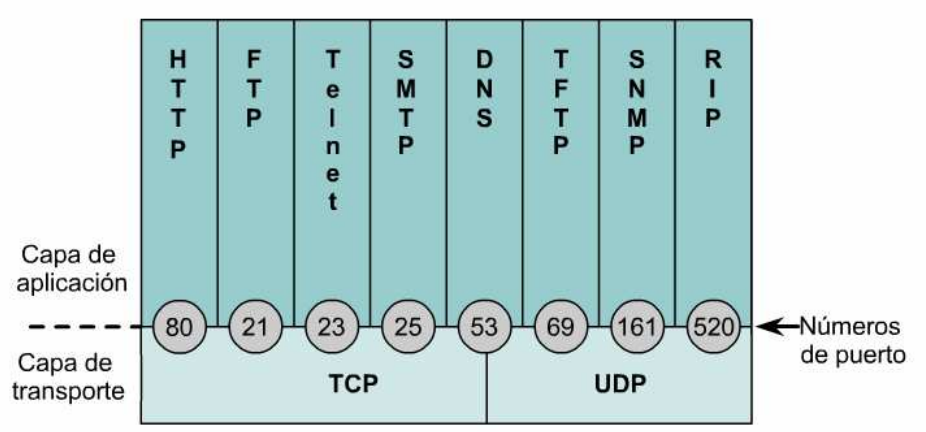


Figura 11.10 Número de asignación de puertos

Los programadores del software de aplicación han aceptado usar los números de puerto conocidos que emite la Agencia de Asignación de Números de Internet (IANA: Internet Assigned Numbers Authority). Figura 11.10. Cualquier conversación dirigida a la aplicación FTP usa los números de puerto estándar 20 y 21. El puerto 20 se usa para la parte de datos y el puerto 21 se usa para control. A las conversaciones que no involucran ninguna aplicación que tenga un número de puerto bien conocido, se les asignan números de puerto que se seleccionan de forma aleatoria dentro de un rango específico por encima de 1023. Algunos puertos son reservados, tanto en TCP como en UDP, aunque es posible que algunas aplicaciones no estén diseñadas para admitirlos. Los números de puerto tienen los siguientes rangos asignados:

- Los números inferiores a 1024 corresponden a números de puerto bien conocidos.
- Los números superiores a 1024 son números de puerto asignados de forma dinámica.
- Los números de puerto registrados son aquellos números que están registrados para aplicaciones específicas de proveedores. La mayoría de estos números son superiores a 1024.

Los sistemas finales utilizan números de puerto para seleccionar la aplicación adecuada. El host origen asigna de forma dinámica los números del puerto de origen. Estos números son siempre superiores a 1023.

11.2.2 DNS

La Internet está basada en un esquema de direccionamiento jerárquico. Este esquema permite que el enrutamiento se base en clases de direcciones en lugar de basarse en direcciones individuales. El problema que esto crea para el usuario es la asociación de la dirección correcta con el sitio de Internet. Es muy fácil olvidarse cuál es la dirección IP de un sitio en particular dado que no hay ningún elemento que permita asociar el contenido del sitio con su dirección. Imaginemos lo difícil que sería recordar direcciones IP de decenas, cientos o incluso miles de sitios de Internet.

Se desarrolló un sistema de denominación de dominio para poder asociar el contenido del sitio con su dirección. El Sistema de denominación de dominios (DNS: Domain Name System) es un sistema utilizado en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP. Un dominio es un grupo de computadoras asociados, ya sea por su ubicación geográfica o por el tipo de actividad comercial que comparten. Un nombre de dominio es una cadena de caracteres, números o ambos. Por lo general, un nombre o una abreviatura que representan la dirección numérica de un sitio de Internet conforma el nombre de dominio.

Existen más de 200 dominios de primer nivel en la Internet, por ejemplo:

.us: Estados Unidos de Norteamérica
.uk: Reino Unido

También existen nombres genéricos, por ejemplo:

.edu: sitios educacionales
.com: sitios comerciales
.gov: sitios gubernamentales
.org: sitios sin fines de lucro
.net: servicio de red

11.2.3 FTP

FTP es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten FTP. El propósito principal de FTP es transferir archivos desde un computadora hacia otro copiando y moviendo archivos desde los servidores hacia los clientes, y desde los clientes hacia los servidores. Cuando los archivos se copian de un servidor, FTP primero establece una conexión de control entre el cliente y el servidor. Luego se establece una segunda conexión, que es un enlace entre los computadoras a través del cual se transfieren los datos. La transferencia de datos se puede realizar en modo ASCII o en modo binario. Estos modos determinan la codificación que se usa para el archivo de datos que, en el modelo OSI, es una tarea de la capa de presentación. Cuando termina la transferencia de archivos, la conexión de datos se termina automáticamente.

El navegador de Web examina el protocolo para determinar si es necesario abrir otro programa y, a continuación, emplea DNS para determinar la dirección IP del servidor de Web. Luego, las capas de transporte, de red, de enlace de datos y física trabajan de forma conjunta para iniciar la sesión con el servidor Web. Los datos transferidos al servidor HTTP contienen el nombre de carpeta de la ubicación de la página Web. Los datos también pueden contener un nombre de archivo específico para una página HTML. Si no se suministra ningún nombre, se usa el nombre que se especifica por defecto en la configuración en el servidor.

El servidor responde a la petición enviando todos los archivos de texto, audio, vídeo y de gráficos, como lo especifican las instrucciones de HTML, al cliente de Web. El navegador del cliente reensambla todos los archivos para crear una vista de la página Web y luego termina la sesión. Si se hace clic en otra página ubicada en el mismo servidor o en un servidor distinto, el proceso vuelve a empezar.

11.2.5 SMTP

Los servidores de correo electrónico se comunican entre sí usando el Protocolo simple de transferencia de correo (SMTP) para enviar y recibir correo. El protocolo SMTP transporta mensajes de correo electrónico en formato ASCII usando TCP.

Cuando un servidor de correo recibe un mensaje destinado a un cliente local, guarda ese mensaje y espera que el cliente recoja el correo. Hay varias maneras en que los clientes de correo pueden recoger su correo.

Pueden usar programas que acceden directamente a los archivos del servidor de correo o pueden recoger el correo usando uno de los diversos protocolos de red. Los protocolos de cliente de correo más populares son POP3 e IMAP4, ambos de los cuales usan TCP para transportar datos.

Aunque los clientes de correo usan estos protocolos especiales para recoger el correo, casi siempre usan SMTP para enviar correo. Dado que se usan dos protocolos distintos y, posiblemente, dos servidores distintos para enviar y recibir correo, es posible que los clientes de correo ejecuten una tarea y no la otra. Por lo tanto, generalmente es una buena idea diagnosticar los problemas de envío de correo electrónico y los problemas de recepción del correo electrónico por separado.

Al controlar la configuración de un cliente de correo, se debe verificar que los parámetros de SMTP y POP o IMAP estén correctamente configurados. Una buena manera de probar si un servidor de correo se puede alcanzar es hacer Telnet al puerto SMTP (25) o al puerto POP3 (110). El siguiente formato de comandos se usa en la línea de comandos de Windows para probar la capacidad de alcanzar el servicio SMTP en el servidor de correo en la dirección IP 192.168.10.5:

C:\>telnet 192.168.10.5 25

El nombre de host es la dirección IP o el nombre DNS dla computadora remoto. El tipo de terminal describe el tipo de emulación de terminal que el cliente Telnet debe ejecutar. La operación Telnet no utiliza la potencia de procesamiento dla computadora que realiza la transmisión. En lugar de ello, transmite las pulsaciones del teclado hacia el host remoto y dirige los resultados hacia el monitor del host local. El procesamiento y almacenamiento se producen en su totalidad en el computador remoto.

Telnet funciona en la capa de aplicación del modelo TCP/IP. Por lo tanto, Telnet funciona en las tres capas superiores del modelo OSI. La capa de aplicación se encarga de los comandos. La capa de presentación administra el formateo, generalmente ASCII. La capa de sesión realiza la transmisión. En el modelo TCP/IP, se considera que todas estas funciones forman parte de la capa de aplicación.

Estudio guiado del cableado estructurado y proyecto de instalación

Las destrezas relacionadas con el cableado estructurado son fundamentales para cualquier profesional de networking. El cableado estructurado crea una topología física en la que el cableado de telecomunicaciones se organiza en estructuras jerárquicas de terminaciones y de interconexiones según los estándares. La palabra telecomunicaciones se usa para expresar la necesidad de manejarse con cables de alimentación eléctrica, cables de teléfono y cable coaxial de televisión por cable, además de los medios de networking de cobre y fibra óptica.

GLOSARIO

Acceso aleatorio: Acceso directo a los registros, sin que tenga importancia su localización física en el medio de almacenamiento.

Acceso de usuario común (CUA; Common User Access): El estándar que deben seguir todas las aplicaciones de software diseñadas para correr en Windows de Microsoft.

Acceso secuencial: El acceso a los registros siguiendo el orden en que están almacenados.

Acumulador: Localidad de almacenamiento de la computadora donde se forma el resultado de una operación aritmética o lógica. (Se relaciona con unidad aritmética y lógica.)

Administración de recursos de información (IRM; Information resource management): Un concepto usado para conseguir que la información sea manejada como un recurso corporativo.

Administrador de bases de datos (DBA, Database administrator): Individuo responsable del mantenimiento físico y lógico de una base de datos.

ADN: (Advanced Digital Network) Usualmente se refiere a línea alquilada de 56Kbps.

Applet: Es un pequeño programa escrito en JAVA y que puede ser insertado en una página HTML. Los applets difieren de las aplicaciones integrales de Java de tal manera que no les permiten accesar ciertos recursos del computador local, tales como archivos y periféricos seriales (modems, impresoras, etc.) y están prohibidos de comunicarse con la mayoría de los otros computadores de la red. La regla común es que un applet solo puede hacer una conexión Internet a la computadora desde donde fué enviado. (Ver: HTML, JAVA)

Arpanet: (Advanced Research Projects Agency Network) – El precursor de la Internet. Desarrollado a fines de los años 60 y principio de los 70, por el Departamento de Defensa de los EE.UU., como un experimento en una gran red, en una gran área, que pudiera sobrevivir una guerra nuclear.

Alfa. Una referencia a las letras del alfabeto. (Compárese con numérico y alfanumérico.)

Alfanumérico: Relacionado con un conjunto de caracteres que contiene letras, dígitos, puntuación y símbolos especiales. (Se relaciona con alfa y numérico.)

Algoritmo: Un procedimiento que se puede usar para resolver un problema particular.

Almacenamiento de información: Una instalación de almacenamiento central basado en la computadora para toda la información de diseño de sistemas (se conoce también como diccionario o enciclopedia).

Arrastrar (Drag): Movimiento del ratón (mouse) por medio del cual se mueve un objeto en la pantalla.

ASCII (American Standard Code for Information Interchange): Un sistema de codificación.

Aseguramiento de la calidad: Un área de especialidad que se encarga de la supervisión de la calidad de todos los aspectos del diseño y la operación de sistemas de información.

Atributo: Un campo en una base de datos relacional.

Automatización de bases de datos: Captura de datos directamente en un sistema de computación desde la fuente sin la necesidad de transcripción vía teclado.

Autopista de información: Una red de conexiones para comunicaciones de datos a alta velocidad que a la larga cubrirá virtualmente todas las facetas de nuestra sociedad.

Banda magnética (Magnetic Band): Un medio de almacenamiento magnético para el almacenamiento de bajo volumen de datos en códigos o tarjetas.

Bandwidth: Ancho de banda. Es cuanta información se puede envíar a través de una conexión. Usualmente se mide en bits por segundo. Una página completa de texto en español tiene aproximadamente un tamaño de 16,000 bits. Un modem rápido puede mover como 15,000 bits por segundo. Una pantalla de video en total movimiento requerirá unos 10,000,000 bits por segundo, dependiendo de la compresión. (Ver: línea de 56k, bps, T-1)

Barra de menú (Menu Bar): Un menú en que las opciones se despliegan a lo ancho de la pantalla.

Base de conocimiento (Knowlegde Base): Base de datos con toda la información referente un tema específico)

Base de datos: 1.El recurso de datos de una organización para todo el procesamiento de información con base en la computación donde los datos están integrados y relacionados para reducir al mínimo la redundancia de datos. 2.Un término alternativo para el software de administración de datos basada en la microcomputación. 3.Lo mismo que un archivo en el contexto del uso de la microcomputadora.

Base de procesadores: Conectores de púas tamaño estándar que permite que los chips se inserten en un tablero de circuito.

BASIC: Un lenguaje de programación popular con propósitos múltiples.

Baudio (Baud): Una medida del número máximo de señales electrónicas que se pueden transmitir a través de un canal de comunicaciones. Binario. Un sistema de numeración de base 2. Bit de paridad. Un bit que se integra a una configuración de Bits (un byte) que se usa para

Campo clave: El campo de un registro que se usa como un identificador del acceso, la salida y la recopilación de registros.

Canal de comunicaciones: La instalación por la que se transmiten datos entre localidades de una red de computación.

Canal: La instalación por la que se transmiten datos entre localidades de una red de computación.

Capacidad de canal: El número de bits que se puede transmitir en un canal de comunicaciones por segundo.

Capacitación basada en computadora (CBT): Uso de las computadoras para la capacitación y la educación.

Captura de datos: La transcripción de datos de fuente en un formato accesible a la máquina.

Capturista de datos: Una persona que utiliza dispositivos de captura por teclado para transcribir datos en un formato accesible a la máquina.

Carga: La transmisión de datos de una PC o una terminal a la computadora mainframe.

Cargar: Transferir programas o datos de un almacenamiento secundario a uno primario.

Carrete de cinta magnética: Medio de almacenamiento de cinta magnética montada en un carrete.

Cartucho de cinta magnética: Medio de almacenamiento de cinta magnética montada en un cartucho.

Cartucho de datos: Almacenamiento de cinta magnética en formato de cassette.

Cartucho de disco: Un módulo de disco intercambiable sellado ambientalmente que contiene uno o m" platos de disco de la unidad de disco duro.

CASE (Computer-Aided Software Engineering; Ingeniería de software asistida por computadora): Una referencia colectiva a una familia de herramientas de productividad de desarrollo de software.

Flujo de procesamiento: Una medida de eficiencia del sistema de computación; la velocidad a la cual se puede realizar un trabajo en un sistema de computación.

Centro de información: Una instalación en que se ponen a la disposición recursos de computación a varios grupos de usuarios.

Ciclo máquina: El ciclo de las operaciones realizadas por el procesador para procesar una instrucción del programa particular: recuperar, decodificar, ejecutar y colocar el resultado en la memoria.

Código de barras: Una técnica de codificación gráfica en que se usan barras verticales de diversa anchura para representar datos.

Código universal de producto (UPC; Universal Product Code): Un código de barras de 10 dígitos que la máquina puede leer, que se coloca en productos de consumo.

Comando: Una instrucción dirigida a una computadora que invoca la ejecución de una secuencia de instrucciones programada previamente.

Comando de ayuda: Una característica del software que ofrece una explicación o instrucción en línea de cómo proceder.

Comodín (carácter): Usualmente un ? o un * que se usa en los comandos del software de la microcomputadora como una referencia genérica a cualquier carácter o cualquier combinación de caracteres, respectivamente.

Compatibilidad: Referente a la capacidad de una computadora para ejecutar programas de otra computadora y accesar a la base de datos de la misma a la vez que se comunica con ésta. 2) Referente a la capacidad de un dispositivo de hardware particular para tener una interfaz con una computadora particular.

Compilador: Sistema de software que realiza el proceso de compilación. (Compárese con interpretadora.)

Compilar: Traducir un lenguaje de programación de alto nivel, como COBOL, en el lenguaje de máquina para preparar la ejecución.

Compufobia: El temor irracional y la aversión a las computadoras.

Computación personal: Un entorno de computación en que los individuos usan microcomputadoras tanto para aplicaciones domésticas como comerciales.

Computadora: Un instrumento electrónico capaz de interpretar y ejecutar comandos programados para entrada, salida, cómputo y operaciones lógicas.

Computadora personal portátil laptop: PC portátil que opera sin una fuente de energía externa.

Computadora personal tipo torre: Una computadora vertical diseñada para instalarse sobre el piso. (Contrástese con computadora personal laptop y computadora personal de escritorio).

Comunicaciones de datos: La recopilación y la distribución de la información desde y hacia instalaciones remotas.

Conectividad en red total: La puesta en red de todo el hardware, software y bases de datos de una organización.

Decodificador: La parte de una unidad de control de procesamiento que interpreta instrucciones.

Densidad de cinta: El número de bits que se pueden almacenar por longitud lineal de una cinta magnética.

Densidad de disco: El número de bits que se puede almacenar por unidad de área en la superficie de la cara del disco.

Densidad: El número de bytes por longitud lineal o área de unidad de un medio de grabación.

Departamento de servicios de información: La entidad organizativa que desarrolla y mantiene sistemas de información con base en la computación.

Depuración: Eliminación de errores de un programa o sistema.

Descarga de memoria: La duplicación del contenido de un dispositivo de almacenamiento en otro dispositivo de almacenamiento o a una impresora.

Descargar: La transmisión de datos de una computadora de estructura principal a una terminal.

Desplazamiento: Uso de las teclas de cursor para ver partes de un documento de procesamiento de texto o una hoja de cálculo que se extiende más allá de la parte inferior, la parte superior o las partes laterales de la pantalla.

Diagrama de flujo de datos: Una técnica de diseño que permite la documentación de un sistema o programa en varios niveles de generalidad.

Diagrama de flujo: Un diagrama que ilustra el flujo de datos, información y trabajo por medio de símbolos especializados que, cuando se conectan por líneas de flujo, reflejan la lógica de un sistema o programa.

Diccionario electrónico: Un diccionario con base en disco que se usa junto con un programa de verificación de ortografía para revisar esta última en un documento de procesamiento de texto.

Diccionario en línea: Software que permite que el usuario solicite sinónimos interactivamente durante una sesión de procesamiento de texto.

Digitalización: Conversión de datos o una imagen en un formato discreto que puede ser interpretado por las computadoras.

Dirección de celda absoluta: Una dirección de celda en una hoja de cálculo que siempre se refiere a la misma celda.

Dirección de celda relativa: Se refiere a la posición de una celda en una hoja de cálculo en relación con la celda que contiene la fórmula en que se usa la dirección.

Domain name: Nombre de dominio. Es un nombre singular y único que identifica a un sitio en el Internet. Los nombres de dominio siempre se componen de dos partes o más separadas por puntos. La parte de la izquierda es la más específica, y la de la derecha es la genérica. Una determinada computadora puede tener más de un nombre de dominio peri un nombre de dominio siempre señala a una solo a computadora.

Doble clic: Pulsación doble del botón de un dispositivo de pulsar y soltar en una sucesión rápida.

Documento fuente: La copia dura original de donde se capturan los datos.

Fabricación asistida por computadora (CAM; Computer aided manufacturing): Término creado para destacar el uso de las computadoras en el proceso de fabricación.

Filtración: Proceso utilizado para la extracción de determinada información de una base de datos.

Firma de usuarios: Procedimiento por el cual se pide a los usuarios que firmen y se comprometan a respetar las especificaciones definidas por el administrador de los sistemas de información.

Flujo de tareas: Secuencia con la que se deben seguir la ejecución de programas.

Fuente de energía ininterrumpible (UPS; uninterrumpible power source): Una fuente de poder que sirve en caso de falla de fuerza eléctrica para darle tiempo a la computadora para apagarla sin falla.

Fuente. Tipo de letra que se describe por su estilo de letra.

Fuera de línea. Información que no puede ser accesada si no esta la computadora conectada a otras computadoras.

Función. Una operación definida con anticipación que realiza operaciones matemáticas, lógicas, estadísticas o financieras

Generador de código: Lenguaje de programación donde programadores especifican las tareas de procesamiento que se deben realizar.

Gigabit (Gb): Mil millones de bits.

Gigabyte (GB): Mil millones de bytes.

Gráfica de barras: Una gráfica que contiene barras verticales que representan valores numéricos, generalmente usado en una hoja de cálculo.

Gráficas de estructura: Una gráfica que ilustra el concepto de un sistema de información como una jerarquía de módulos.

Lector-ordenador MICR: Dispositivo de entrada que lee los datos magnéticos de reconocimiento de caracteres en los documentos bancarios.

Lenguaje de consulta estructurado (SQI, Structured Query Language): Lenguaje de consulta estándar ANSI e ISO para acceso de datos para bases de datos relaciónales.

Lenguaje de control de tareas (JCL, Job-control language): Lenguaje que se usa para indicar a la computadora el orden en que se deben ejecutar los programas.

Lenguaje de la cuarta generación (4GL): Lenguaje de programación que usa instrucciones de alto nivel para recuperar y dar forma a la información.

Lenguaje máquina: Lenguaje de programación que la máquina interpreta y ejecuta directamente.

Lenguaje de programación de alto nivel: Lenguaje con instrucciones que combinan varias instrucciones a nivel máquina en una instrucción.

Lenguaje de programación de bajo nivel: Lenguaje que comprende el conjunto fundamental de instrucciones de una computadora particular.

Lenguaje de programación: Lenguaje que los programadores usan para comunicar instrucciones a una computadora y poder ejecutar un programa.

Lenguaje de- tercera generación (3GL): Lenguaje de computación orientado a procedimientos como COBOL y BASIC.

Lenguaje ensamblador: Lenguaje simbólico de bajo nivel con un conjunto de instrucciones que esencialmente es ideal para el lenguaje máquina.

Línea conmutada. Una línea telefónica que se usa como un canal regular de comunicaciones de datos.

Línea dúplex completo. Un canal de comunicaciones que transmite datos en ambas direcciones al mismo tiempo.

Línea multipunto. La conexión de mis de una terminal a un solo canal de comunicaciones.

Línea privada. Un canal de comunicaciones dedicado entre dos puntos cualesquiera en una red de computadoras.

Macintosh (MAC): Computadora creada por Apple Computer.

Macro: Secuencia de operaciones que se usan con frecuencia o combinaciones de teclas que se invocan para acelerar la interacción del usuario con el software de productividad de la computadora.

Microcomputadora: Una computadora pequeña (es lo mismo que computadora de escritorio, computadora personal, PC.)

Microcomputadora multiusuario: Una microcomputadora que da servicio a más de un usuario en un momento determinado.

Microprocesador: El componente de procesamiento de una computadora.

Microsegundo: Una millonésima de segundo.

Milisegundo: Una milésima de segundo.

Minicomputadora: Una computadora de tamaño mediano.

Módem (MOdidator-DEModulator; modulador-desmodulador): Un dispositivo que se usa para convertir señales compatibles con la computadora en señales utilizables en las instalaciones de transmisión de datos y viceversa utilizando una línea telefónica.

Modo de emulación de terminal: Software instalado en un computadora en la cual emula una terminal.

Modo de inserción: Modo de captura de datos en que el carácter capturado se inserta en la posición del cursor.

Modo de sobreescritura: Un modo de captura de datos en que el carácter que se captura se sobrepone al carácter que está en la posición del cursor.

Módulo: Un programa puede constar de diferentes módulos y cada cual actúa de independientemente del otro.

Monitor: Pantalla similar a la de un televisor para salida de copia blanda en un sistema de computación.

Monitor de panel plano: Un monitor, delgado de la parte posterior a la anterior, que usa cristal liquido y tecnología de plasma de gas.

Monitor RGB (red green and blue): Un monitor a color que combina rojo, verde y azul para lograr un espectro de colores.

Monitores de pantalla de contacto. Monitores con pantallas sensibles al contacto que permite que los usuarios seleccionen entre las opciones disponibles mediante el simple contacto con un dedo del icono o el menú deseado.

MS-DOS (Microsoft Disk Operating System; sistema operativo de disco Microsoft): Un sistema operativo de microcomputadora creado por la compañía Microsoft.

Multimedia: Aplicaciones de computación que implican la integración de texto, sonido, gráficas, videos y animación.

Organización secuencial indexada: Un esquema de almacenamiento de datos de acceso directo que usa un índice para localizar y accesar datos almacenados en un disco magnético.

OS/2: Un sistema operativo multitareas para PC creado por IBM.

Página: Segmento de un programa que se carga al almacenamiento primario sólo si es necesario que se ejecute.

Pantalla de ayuda: Pantalla que se despliega en el monitor al invocar el comando de ayuda.

Paquete de software: Aplicaciones diseñadas para realizar una tarea de procesamiento particular.

Parámetro: Descriptor que puede tomar diferentes valores.

Parche (Patch): Modificación de un programa o sistema de información.

Pascal: Lenguaje de programación orientado a procedimientos con usos varios.

Patrón de documentos: Texto existente en una aplicación de procesamiento de palabras que se puede personalizar para usarse en una variedad de aplicaciones de procesamiento de texto.

PC (Personal Computer; computadora personal): Computadora de escritorio y microcomputadora.

Piratería de software: Duplicación ilegal del software.

Piratería por plagio: Caso especial de piratería de software en que una compañía compra un producto de software sin contrato de licencia, luego lo copia y distribuye dentro de la compañía.

Pixel (picture element, elemento gráfico): Punto en una pantalla a la que se proyectar luz.

Plantilla: Modelo para una aplicación de software de microcomputadora particular.

Plataforma: Denominación que se les da a diferentes sistemas operativos, por ejemplo, Windows, Macintosh, Unix, etc.

Procesamiento de entrada en un sistema: Procedimiento por medio del cual un usuario accesa el sistema de computación.

Procesador: Componente lógico de un sistema de computación que interpreta y ejecuta instrucciones de programas.

Procesador anfitrión paralelo: Procesador dual que trabaja junto al procesador principal y es usado como respaldo complementario.

Procesador anfitrión: Procesador primario del control general de un sistema de computación.

Programador: Alguien que programa por medio de un lenguaje de programación para optimizar el uso de del sistema de la computadora.

Programador de aplicaciones: Un programador que escribe programas para aplicaciones empresariales especificas.

Programador de sistemas: Un programador que desarrolla y mantiene el software del sistema.

Programador/analista: Título que se da a de quien realiza tanto funciones de programación como de análisis de sistemas.

Programas de captura de pantalla: Programas residentes en memoria que permiten que los usuarios transfieran toda la imagen de la pantalla actual o parte de la misma a un archivo de disco.

PROM (Programmable Read-Only Memory; Memoria programable de sólo lectura): ROM en que el usuario puede cargar programas y datos de sólo lectura.

Protocolos de comunicaciones: Medios de comunicación establecidas para regir la manera en que se transmiten los datos en una red de computadoras (TCP/IP, IPX, etc.)

Proyector de imágenes de pantalla: Un dispositivo de salida que puede proyectar una imagen generada por computadora sobre una pantalla grande.

Pseudocódigo: El código no ejecutable de un programa que se usa como una ayuda para desarrollar y documentar programas estructurados.

Puerto: Un punto de acceso en un sistema de computación que permite la comunicación entre la computadora y un dispositivo periférico.

Puerto en serie: Una conexión directa con el bus de la microcomputadora que facilita la transmisión en serie de datos, un bit a la vez.

Puerto paralelo: Una conexión directa con el bus de la microcomputadora que facilita la transmisión paralela de datos, normalmente de un byte a la vez.

RAM (Random-Access Memory; memoria de acceso aleatorio): Area de la memoria en que deben residir todos lo programas y datos antes de que se puedan ejecutar los programas o manejar los datos.

Rango: Una celda o un grupo de celdas adyacentes en una hoja de cálculo.

Ranuras de expansión: Ranuras dentro del componente de procesamiento de una microcomputadora en los que se pueden insertar tableros de circuitos de expansión opcionales.

Rastreador (lector) de imágenes: Un dispositivo que usa una cámara para rastrear y digitalizar una imagen que se puede almacenar en un disco y manejar en una computadora.

Sector: Un concepto de almacenamiento en discos de una parte en forma de rebanada de pastel de un disco o disco flexible en que se almacenan registros y se recuperan posteriormente.

Seguridad física: Aspecto de la seguridad de un centro de cómputo que se ocupa del acceso a las computadoras y los dispositivos periféricos.

Semiconductor: Una sustancia cristalina cuya conductividad eléctrica permite la fabricación de circuitos integrados.

Servidor de archivos (File Server): Una microcomputadora con un disco de alta capacidad para el almacenamiento de datos y programas compartidos por los usuarios de una LAN.

Servidor de comunicaciones: El componente de la LAN que proporciona medios de comunicaciones externas.

Servidor de impresión. Una computadora con base en una LAN que maneja tareas de impresión del usuario de una LAN y controla por lo menos una impresora.

Servidor: Un componente de la LAN que pueden compartir las aplicaciones y archivos de una LAN entre varios usuarios.

Shell: Software que permite una interfaz gráfica de usuario como una alterativa al software controlado por comandos.

Shell de sistema experto: El software que permite el desarrollo de sistemas expertos.

Sintaxis: Las reglas que rigen la formulación de las instrucciones en un programa de computación.

Sintetizadores de voz: Dispositivos que convierten datos brutos en voz producida electrónicamente.

Sistema de administración de base de datos relacional (RDBMS): Una base de datos en que los datos se accesan por contenido mas que por dirección.

Sistema de administración de bases de datos (DBMS; Database management system): Un paquete de software de sistema para la creación, el manejo y el mantenimiento de la base de datos.

Sistema de administración de información (MIS; Management information system): Una estructura integrada de bases de datos y flujos de información a través de todos los niveles y componentes de una organización, donde la recopilación, la transferencia y la presentación de información se optimiza para cubrir las necesidades de la organización.

Sistema de codificación: Un sistema que permite la codificación de caracteres alfanuméricos en términos de bits.

Software de supervisión de rendimiento: Software de sistema que se usa para supervisor, analizar e informar sobre el rendimiento del sistema general de computación y sus componentes.

Software gráfico: Software que permite crear gráficos de diseños lineales, arte y presentación.

Subrutina: Una secuencia de instrucciones del programa que se llaman y ejecutan conforme es necesario.

Supercomputadora: La categoría que incluye las computadoras más grandes y poderosas.

Tablero de sistema (Motherboard): tablero de circuitos de una microcomputadora que contiene el microprocesador, los circuitos electrónicos para manejar tareas tales como las señales de entrada/salida de los dispositivos periféricos y chips de memoria.

Tableros de expansión: Tableros contienen los circuitos electrónicos para una amplia variedad de funciones relacionadas con la computadora.

Tarjeta de expansión de multifunción: Un tablero de circuitos de expansión que realiza más de una función.

Tarjeta inteligente: Una tarjeta o un gafete con un microprocesador integrado.

TCP/IP: (Transmision Control Protocol / Internet Protocol) Protocolo de Control de Transmisión / Protocol de Internet. Es la suite de los protocolos que define el Internet. Se diseño originalmente para los sistemas operativo UNIX. El software de TCP/IP está disponible para cualquier sistema operativo actualmente. Para estar en la Internet es necesario que su computadora tenga software TCP/IP para que sea eficiente.

Tecla de función: Una tecla de función especial del teclado que se puede usar para dar instrucciones a la computadora para que ejecute una operación especifica.

Teclado: Un dispositivo que se usa para la captura de caracteres.

Teclado numérico: La parte de un teclado que permite la captura rápida de caracteres datos numéricos.

Teclas de control del cursor: Las teclas con flechas del teclado que mueven el cursor de texto verticalmente un renglón a la vez y horizontalmente un carácter a la vez.

Tecnología de la información: Una referencia colectiva a los campos combinados de las computadoras y los sistemas de información.

Telecomunicaciones: Comunicación entre dispositivos remotos.

Unidad aritmética y Lógica: La parte de una computadora que realiza operaciones aritméticas y lógicas.

Unidad de control: La parte del procesador que interpreta las instrucciones de programa y dirige operaciones internas, así como el flujo de entrada/salda de una memoria principal.

UNIX: Sistema operativo multiusuario.

Usuario final (End user): Individuo que introduce datos a la computadora o que que trabaja con ella.

Windows: Sistema operativo producido por Microsoft Corporation que ofrece una interfaz gráfica para el usuario y capacidad de multitareas.

WAN: (Wide Area Network) Red de área amplia. Es una red que cubre mas extensión que la de un edificio o complejo de edificios.

WWW (Web): (World Wide Web) Tiene 2 significados: Primero, y el más usado, es el conjunto o constelación de recursos que se pueden accesar usando Gopher, FTP, telnet, USENET, WAIS y algunas otras herramientas. La segunda, el universo de servidores de hipertexto (HTTP) que permiten texto, gráficos, archivos de sonido, etc., y que se pueden mezclar.