

MicroCisco



Cisco Networking Academy Program

CCNA® 1 and 2

Versión 3.1

Curriculum en formato pdf
por **staky**

MicroCisco - staky



CCNA 1: Conceptos básicos sobre networking v3.1

CCNA 1: "Conceptos básicos sobre networking" es el primero de los cuatro cursos necesarios para obtener la certificación como Asociado de Red Certificado de Cisco (CCNA). CCNA 1 introduce a los estudiantes del Programa de la Academia de Networking de Cisco al campo de networking. El curso se centra en la terminología y los protocolos de red, redes de área local (LAN), redes de área amplia (WAN), modelos de Internetworking de sistemas abiertos (OSI), cableado, herramientas de cableado, routers, programación del router, Ethernet, direccionamiento de Protocolo Internet (IP) y estándares de red.

Módulo 1: Introducción a networking

Descripción general

Para entender el rol que los computadores juegan en un sistema de networking, considere la Internet. La Internet es un recurso valioso y estar conectado a ella es fundamental para la actividad empresarial, la industria y la educación. La creación de una red que permita la conexión a Internet requiere una cuidadosa planificación. Aun para conectar computadores personales individuales (PC) a Internet, se requiere alguna planificación y la toma de ciertas decisiones. Se deben considerar los recursos computacionales necesarios para la conexión a Internet. Esto incluye el tipo de dispositivo que conecta el PC a Internet, tal como una tarjeta de interfaz de red (NIC) o modem. Se deben configurar protocolos o reglas antes que un computador se pueda conectar a Internet. También es importante la selección correcta de un navegador de web.

Los estudiantes que completen esta lección deberán poder:

- Comprender la conexión física que debe producirse para que un computador se conecte a Internet.
- Reconocer los componentes que comprende el computador.
- Instalar y diagnosticar las fallas de las NIC y los módems.
- Configurar el conjunto de protocolos necesarios para la conexión a Internet.
- Probar la conexión a Internet mediante procedimientos de prueba básicos.
- Demostrar una comprensión básica del uso de los navegadores de Web y plug-ins.

1.1 Conexión a la Internet

1.1.1 Requisitos para la conexión a Internet

La Internet es la red de datos más importante del mundo. La Internet se compone de una gran cantidad de redes grandes y pequeñas interconectadas. Computadores individuales son las fuentes y los destinos de la información a través de la Internet. La conexión a Internet se puede dividir en conexión física, conexión lógica y aplicaciones. ¹

Los requisitos para la conexión a Internet:

- Conexión física
- Conexión lógica
- Aplicaciones que interpretan los datos y muestran la información

Figura 1

Se realiza una conexión física conectando un tarjeta adaptadora, tal como un módem o una NIC, desde un PC a una red. La conexión física se utiliza para transferir las señales entre los distintos PC dentro de la red de área local (LAN) y hacia los dispositivos remotos que se encuentran en Internet.

La conexión lógica aplica estándares denominados protocolos. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen la manera en que se comunican los dispositivos de una red; las conexiones a Internet pueden utilizar varios protocolos. El conjunto Protocolo de control de transporte/protocolo Internet (TCP/IP) es el principal conjunto de protocolos que se utiliza en Internet. Los protocolos del conjunto TCP/IP trabajan juntos para transmitir o recibir datos e información.

La aplicación que interpreta los datos y muestra la información en un formato comprensible es la última parte de la conexión. Las aplicaciones trabajan junto con los protocolos para enviar y recibir datos a través de Internet. Un navegador Web muestra el código HTML como una página Web. Ejemplos de navegadores Web incluyen Internet Explorer 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.

Esta es simplemente una introducción a Internet y, por la forma en que lo presentamos aquí, puede parecer un proceso sumamente simple. A medida que exploremos el tema con mayor profundidad, se verá que el envío de datos a través de la Internet es una tarea complicada.

1.1.2 Principios básicos de los PC

Como los computadores son importantes elementos básicos de desarrollo de redes, es necesario poder reconocer y nombrar los principales componentes de un PC. Muchos dispositivos de networking son de por sí computadores para fines especiales, que poseen varios de los mismos componentes que los PC normales.

Para poder utilizar un computador como un medio confiable para obtener información, por ejemplo para acceder al currículum basado en Web, debe estar en buenas condiciones. Para mantener un PC en buenas condiciones es necesario realizar de vez en cuando el diagnóstico simple de fallas del hardware y del software del computador. Por lo tanto, es necesario reconocer los nombres y usos de los siguientes componentes de PC:

Componentes pequeños separados

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

Subsistemas del PC

- **Placa de circuito impreso (PCB, Printed Circuit Board):** Una placa que tiene pistas conductoras superpuestas o impresas, en una o ambas caras. También puede contener capas internas de señal y planos de alimentación eléctrica y tierra. Microprocesadores, chips, circuitos integrados y otros componentes electrónicos se montan en las PCB.
- **Unidad de CD-ROM:** Unidad de disco compacto con memoria de sólo lectura, que puede leer información de un CD-ROM
- **Unidad de procesamiento central (CPU):** La parte de un computador que controla la operación de todas las otras partes. Obtiene instrucciones de la memoria y las decodifica. Realiza operaciones matemáticas y lógicas y traduce y ejecuta instrucciones. ¹



Figura 1

- **Unidad de disquete:** Una unidad de disco que lee y escribe información a una pieza circular con un disco plástico cubierto de metal de 3.5 pulgadas. Un disquete estándar puede almacenar aproximadamente 1 MB de información. ²



Figura 2

- **Unidad de disco duro:** Un dispositivo de almacenamiento computacional que usa un conjunto de discos rotatorios con cubierta magnética para almacenar datos o programas. Los discos duros se pueden encontrar en distintas capacidades de almacenamiento.
- **Microprocesador:** Un microprocesador es un procesador que consiste en un chip de silicio diseñado con un propósito especial y físicamente muy pequeño. El microprocesador utiliza tecnología de circuitos de muy alta integración (VLSI , Very Large-Scale Integration) para integrar memoria , lógica y señales de control en un solo chip. Un microprocesador contiene una CPU.
- **Placa madre:** La placa de circuito impreso más importante de un computador. La placa madre contiene el bus, el microprocesador y los circuitos integrados usados para controlar cualquier dispositivo tal como teclado, pantallas de texto y gráficos, puertos seriales y paralelos, joystick e interfaces para el mouse. ³

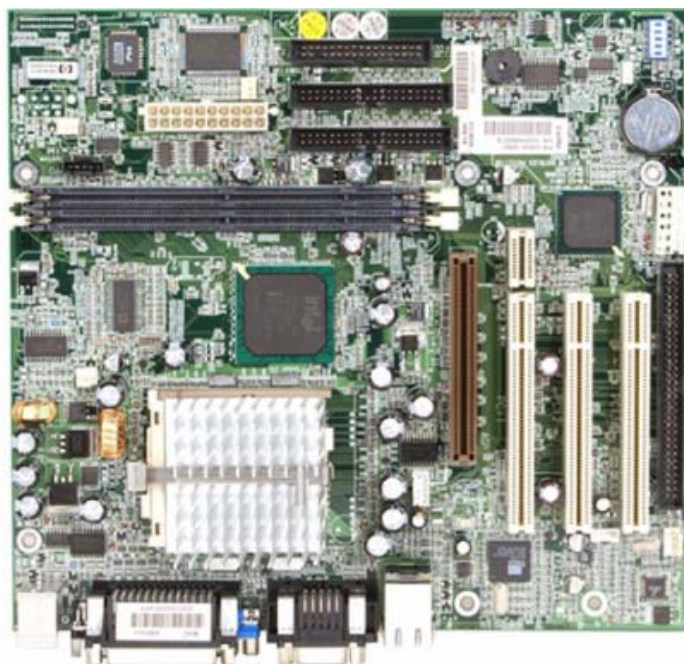
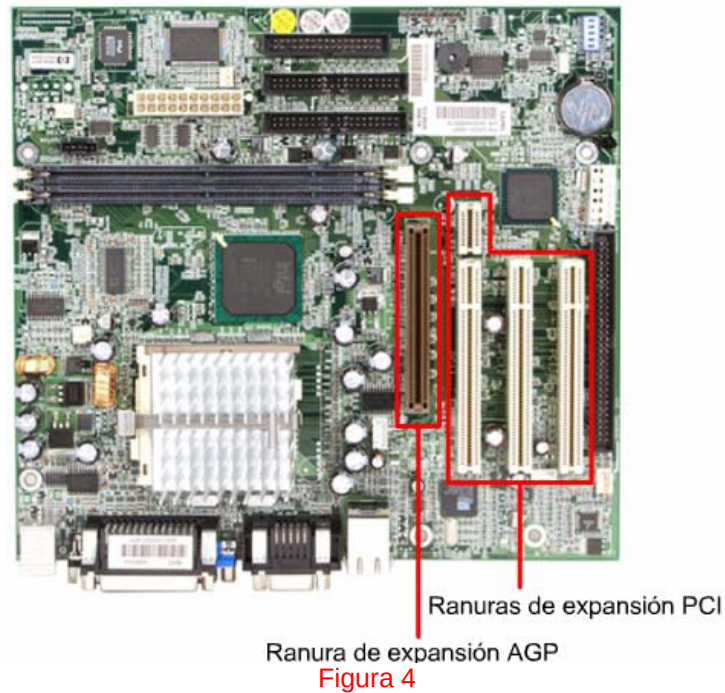


Figura 3

- **Bus:** Un conjunto de pistas eléctricas en la placa madre a través del cual se transmiten señales de datos y temporización de una parte del computador a otra.
- **Memoria de acceso aleatorio (RAM):** También conocida como memoria de lectura/escritura; en ella se pueden escribir nuevos datos y se pueden leer los datos almacenados. La RAM requiere energía eléctrica para mantener el almacenamiento de datos. Si el computador se apaga o se le corta el suministro de energía, todos los datos almacenados en la RAM se pierden.
- **Memoria de sólo lectura (ROM):** Memoria del computador en la cual hay datos que han sido pregrabados. Una vez que se han escrito datos en un chip ROM, estos no se pueden eliminar y sólo se pueden leer.
- **Unidad del sistema:** La parte principal del PC, que incluye el armazón, el microprocesador, la memoria principal, bus y puertos. La unidad del sistema no incluye el teclado, monitor, ni ningún otro dispositivo externo conectado al computador.
- **Ranura de expansión:** Un receptáculo en la placa madre donde se puede insertar una placa de circuito impreso para agregar capacidades al computador, La figura ⁴ muestra las ranuras de expansión PCI (Peripheral Component Interconnect/Interconexión de componentes periféricos) y AGP (Accelerated Graphics Port/Puerto de gráficos acelerado). PCI es una conexión de alta velocidad para placas tales como NIC, módems internos y tarjetas de video. El puerto AGP provee una conexión de alta velocidad entre dispositivos gráficos y la memoria del sistema. La ranura AGP provee una conexión de alta velocidad para gráficos 3-D en sistemas computacionales.
- **Fuente de alimentación:** Componente que suministra energía a un computador



Componentes del backplane

- **Backplane:** Un backplane es una placa de circuito electrónico que contiene circuitería y sócalos en los cuales se pueden insertar dispositivos electrónicos adicionales en otras placas de circuitos; en un computador, generalmente sinónimo de o parte de la tarjeta madre.
- **Tarjeta de interfaz de red (NIC):** Placa de expansión insertada en el computador para que se pueda conectar a la red.
- **Tarjeta de video:** Placa que se introduce en un PC para otorgarle capacidades de visualización
- **Tarjeta de sonido:** Placa de expansión que permite que el computador manipule y reproduzca sonidos
- **Puerto paralelo:** Interfaz que puede transferir más de un bit simultáneamente y que se utiliza para conectar dispositivos externos tales como impresoras
- **Puerto serial:** Interfaz que se puede utilizar para la comunicación serial, en la cual sólo se puede transmitir un bit a la vez.
- **Puerto de ratón:** Puerto diseñado para conectar un ratón al PC
- **Cable de alimentación:** Cable utilizado para conectar un dispositivo eléctrico a un tomacorrientes a fin de suministrar energía eléctrica al dispositivo.
- **Puerto USB:** Un conector de Bus Serial Universal (Universal Serial Bus). Un puerto USB conecta rápida y fácilmente dispositivos tales como un mouse o una impresora
- **Firewire:** Una norma de interfaz de bus serial que ofrece comunicaciones de alta velocidad y servicios de datos isócronos de tiempo real.

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 una pequeña red informática.

1.1.3 Tarjeta de interfaz de red

Una tarjeta de interfaz de red (NIC), o adaptador LAN, provee capacidades de comunicación en red desde y hacia un PC. En los sistemas computacionales de escritorio, es una tarjeta de circuito impreso que reside en una ranura en la tarjeta madre y provee una interfaz de conexión a los medios de red. ¹En los sistemas computacionales portátiles, está comunmente integrado en los sistemas o está disponible como una pequeña tarjeta PCMCIA, del tamaño de una tarjeta de crédito. ²PCMCIA es el acrónimo para Personal Computer Memory Card International Association (Asociación Internacional de Tarjetas de Memoria de Computadores Personales). Las tarjetas PCMCIA también se conocen como tarjetas PC.



Figura 1



Figura 2

La NIC se comunica con la red a través de una conexión serial y con el computador a través de una conexión paralela. La NIC utiliza una Petición de interrupción (IRQ), una dirección de E/S y espacio de memoria superior para funcionar con el sistema operativo. Un valor IRQ (petición de interrupción) es número asignado por medio del cual donde el computador puede esperar que un dispositivo específico lo interrumpa cuando dicho dispositivo envía al computador señales acerca de su operación. Por ejemplo, cuando una impresora ha terminado de imprimir, envía una señal de interrupción al computador. La señal interrumpe momentáneamente al computador de manera que este pueda decidir que procesamiento realizar a continuación. Debido a que múltiples señales al computador en la misma línea de interrupción pueden no ser entendidas por el computador, se debe especificar un valor único para cada dispositivo y su camino al computador. Antes de la existencia de los dispositivos Plug-and-Play (PnP), los usuarios a menudo tenían que configurar manualmente los valores de la IRQ, o estar al tanto de ellas, cuando se añadía un nuevo dispositivo al computador.

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

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

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 al computador 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 ¹o bien, pueden conectarse externamente al computador una interfaz de puerto serie ó USB. ²



Figura 1



Figura 2

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. Los computadores notebook pueden tener una interfaz incorporada o utilizar una tarjeta PCMCIA. La Figura ³muestra 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 ⁴llamado NIC, o un adaptador de red externo ⁵que se conecta a la red a través del puerto USB.



Figura 3



Figura 4



Figura 5

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.
- Cambio a un tipo diferente de NIC tal como una tarjeta wireless.
- Instalación de una NIC secundaria o de respaldo por razones de seguridad de red.

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

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

1.1.5 Descripción general de la conectividad de alta velocidad y de acceso telefónico

A principios de la década de 1960, se introdujeron los módems para proporcionar conectividad desde las terminales no inteligentes a un computador central. Muchas empresas solían alquilar tiempo en sistemas de computación, debido al costo prohibitivo que implicaba tener un sistema en sus propias instalaciones. La velocidad de conexión era muy lenta, 300 bits por segundo (bps), lo que significaba aproximadamente 30 caracteres por segundo.

A medida que los PC se hicieron más accesibles en la década de 1970, aparecieron los Sistemas de tableros de boletín (BBS). Estos BBS permitieron que los usuarios se conectaran y enviaran o leyeran mensajes en un tablero de discusiones. La velocidad de 300 bps era aceptable, ya que superaba la velocidad a la cual la mayoría de las personas pueden leer o escribir. A principios de la década de 1980 el uso de los tableros de boletín aumentó exponencialmente y la velocidad de 300 bps resultó demasiado lenta para la transferencia de archivos de gran tamaño y de gráficos. En la década de 1990, los módems funcionaban a 9600 bps y alcanzaron el estándar actual de 56 kbps (56.000 bps) para 1998.

Inevitablemente, los servicios de alta velocidad utilizados en el entorno empresarial, tales como la Línea de suscriptor digital (DSL) y el acceso de módem por cable, se trasladaron al mercado del consumidor. Estos servicios ya no exigían el uso de un equipo caro o de una segunda línea telefónica. Estos son servicios "de conexión permanente" que ofrecen acceso inmediato y no requieren que se establezca una conexión para cada sesión. Esto brinda mayor confiabilidad y flexibilidad y ha permitido que pequeñas oficinas y redes hogareñas puedan disfrutar de la comodidad de la conexión a Internet.

1.1.6 Descripción y configuración TCP/IP

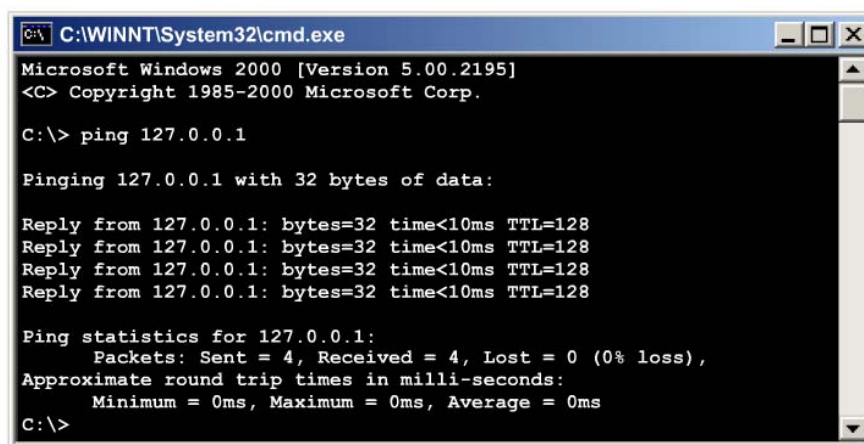
El Protocolo de control de transporte/protocolo Internet (TCP/IP) es un conjunto de protocolos o reglas desarrollados para permitir que los computadores que cooperan entre sí puedan compartir recursos a través de una red. Para habilitar TCP/IP en la estación de trabajo, ésta debe configurarse utilizando las herramientas del sistema operativo. Ya sea que se utilice un sistema operativo Windows o Mac, el proceso es muy similar.

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** 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. ¹
- **ping dirección IP del computador host**: Un ping a un PC host verifica la configuración de la dirección TCP/IP para el host local y la conectividad al host.
- **ping dirección IP de gateway por defecto**: Un ping al gateway por defecto verifica si se puede alcanzar el 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.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-2000 Microsoft Corp.

C:\> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 1

1.1.8 Navegadores de Web y plug-ins

Un navegador de Web realiza las siguientes funciones:

- Inicia el contacto con un servidor de Web
- Solicita información
- Recibe información
- Muestra los resultados en pantalla

Un navegador de Web es un software que interpreta el lenguaje de etiquetas por hipertexto (HTML), que es uno de los lenguajes que se utiliza para codificar el contenido de una página Web. Otros lenguajes de etiqueta con funciones más avanzadas son parte de la tecnología emergente. HTML el lenguaje de etiquetas más común, puede mostrar gráficos en pantalla, ejecutar sonidos, películas y otros archivos multimediales. Los hipervínculos están integrados en una página web y permiten establecer un vínculo rápido con otra ubicación en la misma página web o en una totalmente distinta.

Dos de los navegadores de Web de mayor popularidad son Internet Explorer (IE) y Netscape Communicator. Aunque son idénticos en el tipo de tareas que realizan, existen algunas diferencias entre estos dos navegadores. Algunos sitios Web no admiten el uso de uno o del otro y puede resultar útil tener ambos programas instalados en el computador.

Netscape Navigator: ¹

- Primer navegador popular
- Ocupa menos espacio en disco
- Pone en pantalla archivos HTML, realiza transferencias de correo electrónico y de archivos y desempeña otras funciones



Figura 1

Internet Explorer (IE): 2

- 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

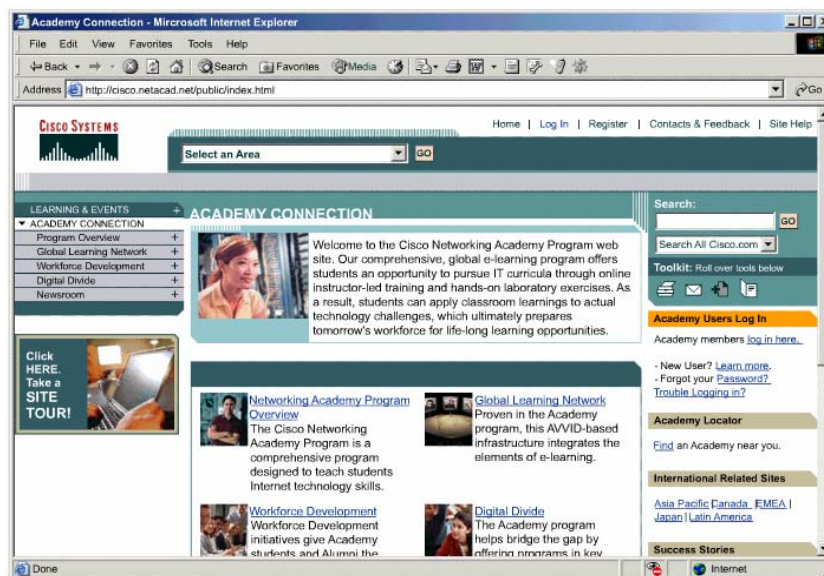


Figura 2

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

Además de establecer la configuración del computador para visualizar el currículum de la Academia Cisco, los computadores permiten realizar muchas tareas de gran utilidad. En el campo empresarial, los empleados usan regularmente un conjunto de aplicaciones de productividad o "de oficina", tal como el Microsoft Office. Las aplicaciones de oficina normalmente incluyen lo siguiente:

- Un software de hoja de cálculo contiene tablas compuestas por columnas y filas que se utilizan con frecuencia con fórmulas, para procesar y analizar datos.
- Un procesador de texto es una aplicación que se utiliza para crear y modificar documentos de texto. Los procesadores de texto modernos permiten crear documentos sofisticados, que incluyen gráficos y texto con riqueza de formato.
- El software de gestión de bases de datos se utiliza para almacenar, mantener, organizar, seleccionar y filtrar registros. Un registro es un conjunto de información que se identifica con un tema común como puede ser el nombre del cliente.
- El software de presentación se utiliza para diseñar y desarrollar presentaciones destinadas a reuniones, clases o presentaciones de ventas.
- Los administradores de información personal incluyen elementos como utilidades de correo electrónico, listas de contacto, una agenda y una lista de tareas a realizar.

Las aplicaciones de oficina forman parte en la actualidad de la vida laboral diaria, tal como ocurría con las máquinas de escribir antes de la llegada de los computadores personales.

1.1.9 Diagnóstico de los problemas de conexión a Internet

En esta práctica de laboratorio de diagnóstico de fallas, los problemas se encuentran en el hardware, en el software y en las configuraciones de red. El objetivo es ubicar y solucionar problemas en un lapso predeterminado de tiempo, lo que con el tiempo permitirá el acceso al currículum. Esta práctica de laboratorio demostrará lo compleja que puede resultar la configuración incluso del sencillo proceso de acceder a la web. Esto incluye los procesos y procedimientos relacionados con el diagnóstico de fallas de hardware, software y sistemas de red de un computador.

1.2 Matemática de redes

1.2.1 Representación binaria de datos

Los computadores manipulan y almacenan los datos usando interruptores electrónicos que están ENCENDIDOS o APAGADOS. Los computadores sólo pueden entender y usar datos 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 computador. 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 computador. ¹ASCII usa dígitos binarios para representar los símbolos que se escriben con el teclado. Cuando los computadores 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

Figura 1

Debido a que los computadores 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 computadores. De modo que los números binarios del computador 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).

Los computadores están diseñados para usar agrupaciones de ocho bits. Esta agrupación de ocho bits se denomina byte. ¹En un computador, un byte representa una sola ubicación de almacenamiento direccionable. Estas ubicaciones de almacenamiento representan un valor o un solo carácter de datos como, por ejemplo, un código ASCII. La cantidad total de combinaciones de los ocho interruptores que se encienden y se apagan es de 256. El intervalo de valores de un byte es de 0 a 255. De modo que un byte es un concepto importante que se debe entender si uno trabaja con computadores y redes.

Unidades	Definición	Bytes*	Bits*	Ejemplos
Bit (b)	Dígito binario, un 1 o un 0	1	1	Conectado/Desconectado; Abierto/Cerrado; +5 voltios o 0 voltios
Byte (B)	8 bits	1	8	Representar la letra "X" como código ASCII
Kilobyte (KB)	1 kilobyte = 1024 bytes	1000	8,000	Correo electrónico típico = 2 KB Informe de 10 páginas = 10 KB Los primeros PC = 64 KB de
Megabyte (MB)	1 megabyte = 1024 kilobytes = 1.048.576 bytes	1 millón	8 millones	Disquetes = 1,44 MB RAM típica = 32 MB CDROM = 650 MB
Gigabyte (GB)	1 gigabyte = 1024 megabytes = 1.073.741.824 bytes	Mil millones	8 mil millones	Disco duro típico = 40 GB o superior
Terabyte (TB)	1 terabyte = 1024 gigabytes = 1.099.511.627.778 bytes	1 billón	8 billones	Cantidad de datos que teóricamente se pueden transmitir por fibra óptica en un segundo

* Bytes o bits comunes o aproximados

Figura 1

1.2.3 Sistema numérico de Base 10

Los sistemas numéricos están compuestos por símbolos y por las normas utilizadas para interpretar estos símbolos. El sistema numérico que se usa más a menudo es el sistema numérico decimal, o de Base 10. El sistema numérico de Base 10 usa diez símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Estos símbolos se pueden combinar para representar todos los valores numéricos posibles.

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 10^0 (1), mientras que la segunda posición representa 10^1 ($10 \times 1 = 10$). La tercera posición representa 10^2 ($10 \times 10 = 100$). La séptima posición a la izquierda representa 10^6 ($10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1.000.000$). Esto siempre funciona, sin importar la cantidad de columnas que tenga el número. ¹

Valor posición	<u>1000</u> <u>100</u> <u>10</u> <u>1</u>
Base Exponente	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Cantidad de símbolos	10
Símbolos	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Razonamiento	Número típico de dedos igual a diez

Figura 1

Ejemplo:

$$2134 = (2 \times 10^3) + (1 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$$

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

Los computadores reconocen y procesan datos utilizando el sistema numérico binario, o de Base 2. ¹El sistema numérico binario usa sólo dos símbolos, 0 y 1, en lugar de los diez símbolos que se utilizan en el sistema numérico decimal. La posición, o el lugar, que ocupa cada dígito de derecha a izquierda en el sistema numérico binario representa 2, el número de base, elevado a una potencia o exponente, comenzando desde 0. Estos valores posicionales son, de derecha a izquierda, 2^0 , 2^1 , 2^2 , 2^3 , 2^4 , 2^5 , 2^6 y 2^7 , o sea, 1, 2, 4, 8, 16, 32, 64 y 128, respectivamente.

Valor posición	<u>128</u> <u>64</u> <u>32</u> <u>16</u> <u>8</u> <u>4</u> <u>2</u> <u>1</u>
Base Exponente	$2^7 = 128$ $2^3 = 8$ $2^6 = 64$ $2^2 = 4$ $2^5 = 32$ $2^1 = 2$ $2^4 = 16$ $2^0 = 1$
Cantidad de símbolos	2
Símbolos	0, 1
Razonamiento	Los sistemas de voltaje de dos estados (valor binario diferenciado) creados con transistores pueden ser variados, potentes, económicos, pequeños y relativamente inmunes al ruido.

Figura 1

Ejemplo:

$$10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22 \quad (16 + 0 + 4 + 2 + 0)$$

Al leer el número binario (10110_2) de izquierda a derecha, se nota que hay un 1 en la posición del 16, un 0 en la posición del 8, un 1 en la posición del 4, un 1 en la posición del 2 y un 0 en la posición del 1, que sumados dan el número decimal 22.

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 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.

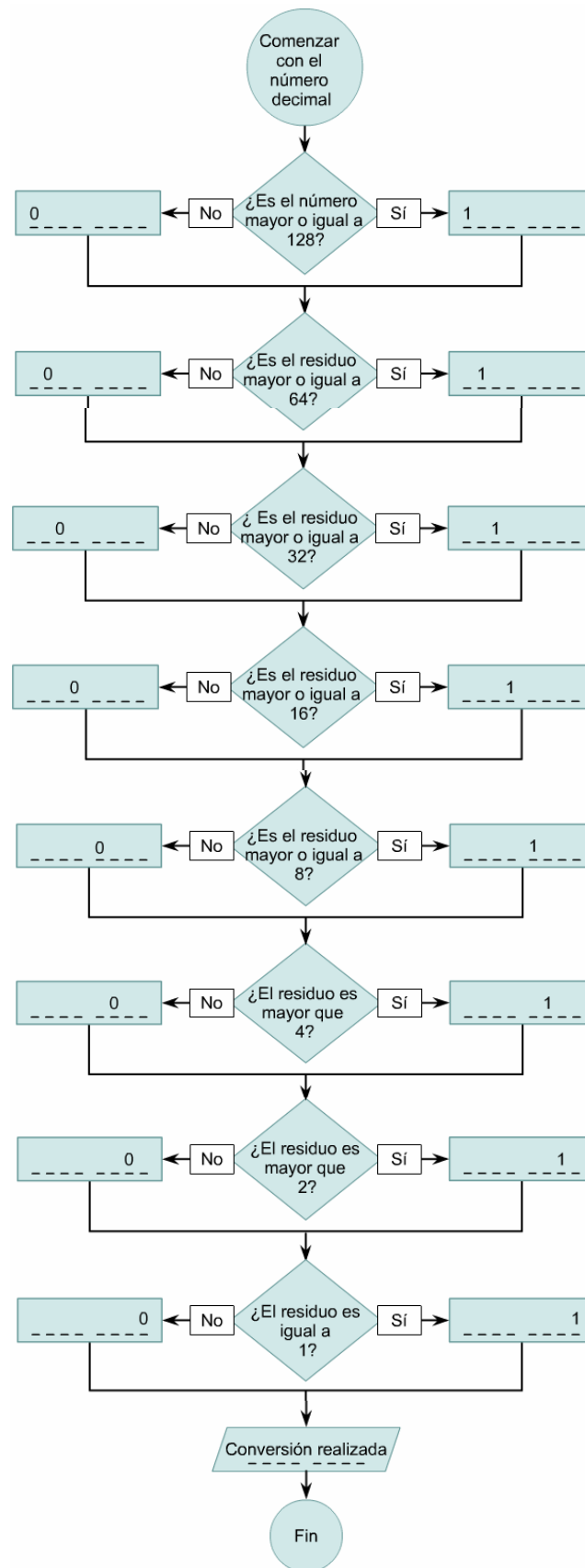


Figura 1

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.

1.2.6 Conversión de números binarios de 8 bits en números decimales

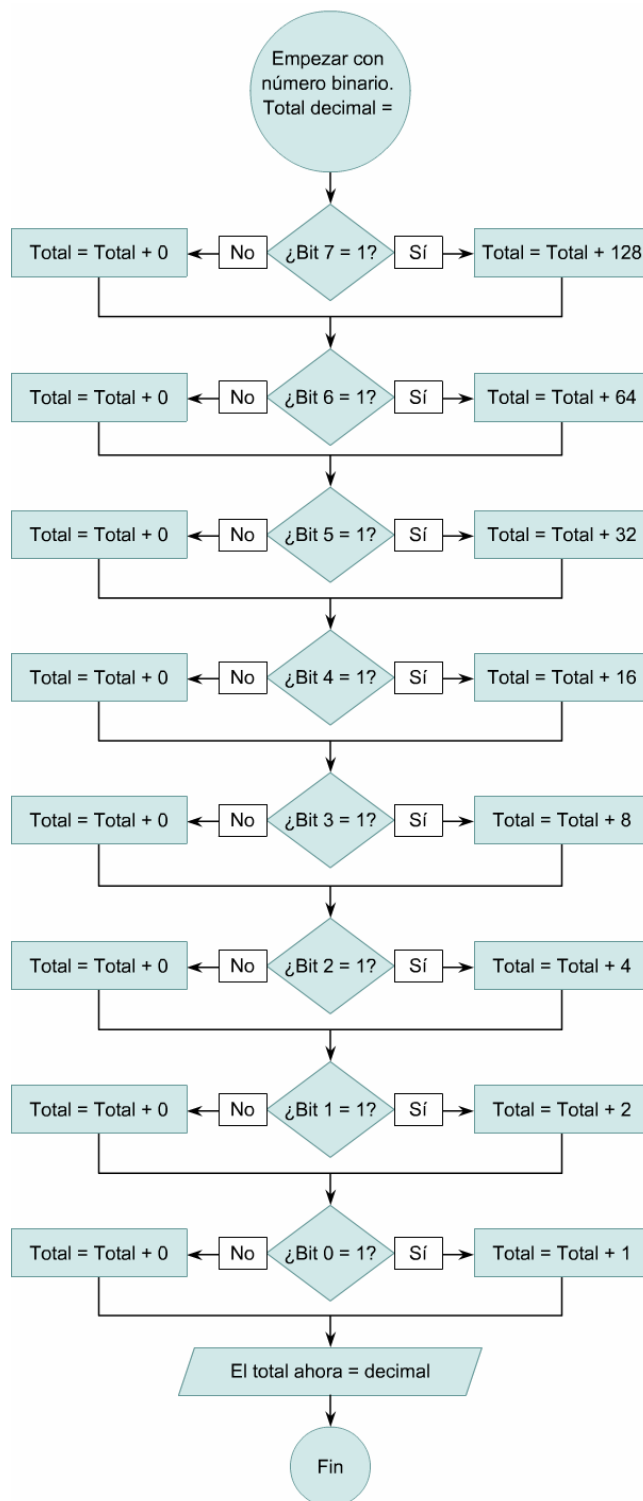


Figura 1

Existen dos formas básicas para convertir números binarios en decimales. El diagrama de flujo que se muestra en la Figura 1 describe uno de estos métodos.

También se pueden convertir los números binarios en decimales multiplicando los dígitos binarios por el número base del sistema, que es de Base 2, y elevados al exponente de su posición.

Ejemplo:

Convierta el número binario 01110000 en decimal.

NOTA:

La operación debe realizarse de derecha a izquierda. Recuerde que cualquier número elevado a la potencia 0 es igual a 1. Por lo tanto, $2^0 = 1$

$$0 \times 2^0 = 0$$

$$0 \times 2^1 = 0$$

$$0 \times 2^2 = 0$$

$$0 \times 2^3 = 0$$

$$1 \times 2^4 = 16$$

$$1 \times 2^5 = 32$$

$$1 \times 2^6 = 64$$

$$0 \times 2^7 = 0$$

$$=112$$

NOTA:

La suma de las potencias de 2 que tienen un 1 en su posición

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 computadores en Internet son números binarios de 32 bits. 1 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 la página anterior.

Binario	11001000		01110010		00000110		00110011
Decimal	200		114		6		51
	número	punto	número	punto	número	punto	número

Figura 1

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.

1.2.8 Hexadecimal

El sistema numérico hexadecimal (hex) se usa frecuentemente cuando se trabaja con computadores porque se puede usar para representar números binarios de manera más legible. 1 El computador ejecuta cálculos en números binarios, pero hay varios casos en los que el resultado del computador en números binarios se expresa en números hexadecimales para facilitar su lectura.

La conversión de un número hexadecimal en binario, y de un número binario en hexadecimal, es una tarea común cuando se trabaja con el registro de configuración de los routers de Cisco. Los routers de Cisco poseen un registro de configuración de 16 bits de longitud. El número binario de 16 bits se puede representar como un número hexadecimal de cuatro dígitos. Por ejemplo, 0010000100000010 en números

binarios es igual a 2102 en números hexadecimales. La palabra hexadecimal a menudo se abrevia como 0x cuando se utiliza con un valor como el que aparece en el número anterior. 0x2102.

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Figura 1

Al igual que los sistemas binario y decimal, el sistema hexadecimal se basa en el uso de símbolos, potencias y posiciones. ² Los símbolos que se usan en hexadecimal son los números 0 - 9 y las letras A, B, C, D, E y F. ³

Binary	Hexadecimal	Binary	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

Figura 2

Binary	Hexadecimal	Decimal	Binary	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

Figura 3

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.

El sistema hexadecimal reduce un número de ocho bits a sólo dos dígitos hexadecimales. Esto reduce la confusión que se puede generar al leer largas cadenas de números binarios y la cantidad de espacio que exige la escritura de números binarios. Recuerde que "hexadecimal" a veces se abrevia como 0x, de modo que hexadecimal 5D también puede aparecer escrito como "0x5D".

Para realizar la conversión de números hexadecimales a binarios, simplemente se expande cada dígito hexadecimal a su equivalente binario de cuatro bits. [4](#) [5](#)

Conversión de número binario a número hexadecimal

100100100010111110111110111001001

Se convierte en:
0001 0010 0100 0101 1111 0111 1101 1100 1001

Se convierte en:
1 2 4 5 F 7 D C 9

De modo que:
100100100010111110111110111001001 binario
= 1245F7DC9 hexadecimal

Figura 4

Conversión de número hexadecimal a número binario

0x2102

Se convierte en:
2 1 0 2
0010 0001 0000 0010

De modo que:
2102 hexadecimal se convierte en: 0010 0001 0000 0010 binario

Figura 5

1.2.9 Lógica booleana o binaria

La lógica booleana se basa en circuitos digitales que aceptan uno o dos voltajes entrantes. [1](#) Basándose en los voltajes de entrada, se genera el voltaje de salida. Para los fines de los computadores, la diferencia de voltaje se asocia con dos estados, activado (encendido) o desactivado (apagado). Estos dos estados, a su vez, se asocian como un 1 o un 0, que son los dos dígitos del sistema numérico binario.

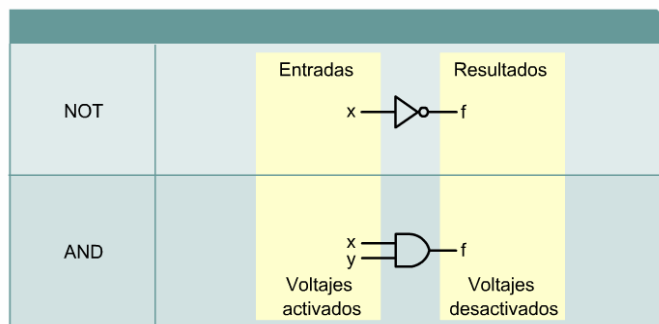


Figura 1

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. [2](#) 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.

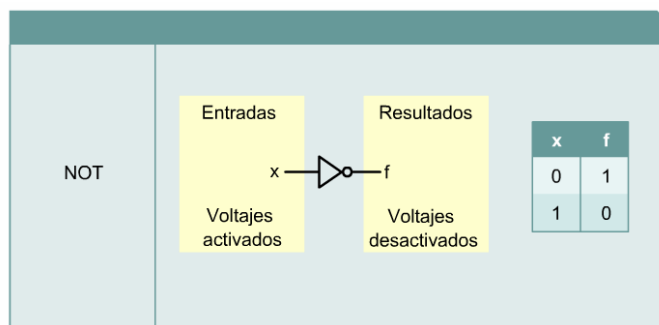


Figura 2

La operación AND toma dos valores de entrada. Si ambos valores son 1, la compuerta lógica genera un resultado de 1. ³De 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.

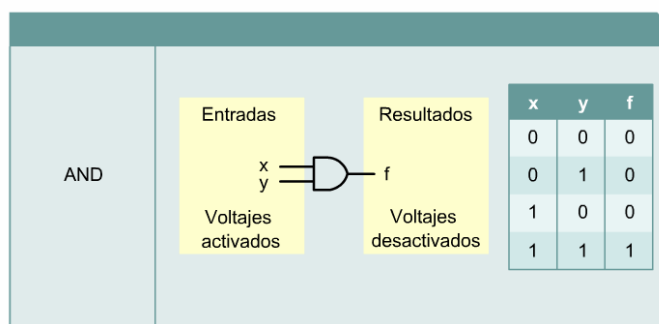


Figura 3

La operación OR también toma dos valores de entrada. ⁴Si 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.

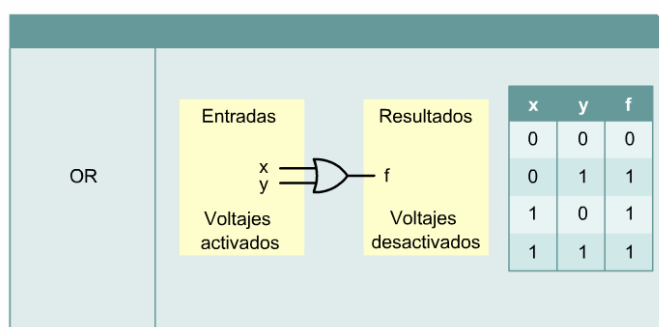


Figura 4

Las dos operaciones de networking que utilizan la lógica booleana son las máscaras wildcard y de subred. Las operaciones de máscara brindan una manera de filtrar direcciones. Las direcciones identifican a los dispositivos de la red y permiten que las direcciones se agrupen o sean controladas por otras operaciones de red. Estas funciones se explicarán en profundidad más adelante en el currículum.

1.2.10 Direcciones IP y máscaras de red

Las direcciones binarias de 32 bits que se usan en Internet se denominan direcciones de Protocolo Internet (IP). ¹En esta sección se describe la relación entre las direcciones IP y las máscaras de red.

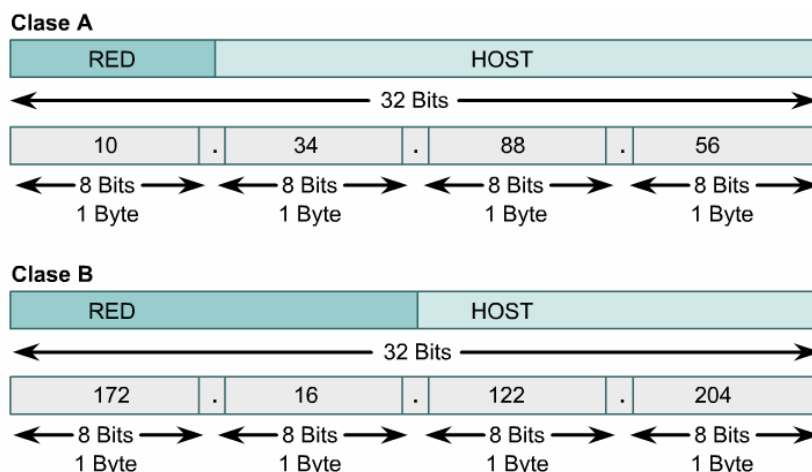


Figura 1

Cuando se asignan direcciones IP a los computadores, algunos de los bits del lado izquierdo del número IP de 32 bits representan una red. La cantidad de bits designados depende de la clase de dirección. Los bits restantes en la dirección IP de 32 bits identifican un computador de la red en particular. El computador se denomina host. La dirección IP de un computador está formada por una parte de red y otra de host que representa a un computador en particular de una red en particular.

Para informarle al computador cómo se ha dividido la dirección IP de 32 bits, se usa un segundo número de 32 bits denominado máscara de subred. Esta máscara es una guía que indica cómo se debe interpretar la dirección IP al identificar cuántos de los bits se utilizan para identificar la red del computador. La máscara de subred completa los unos desde la parte izquierda de la máscara de forma secuencial. Una máscara de subred siempre estará formada por unos hasta que se identifique la dirección de red y luego estará formada por ceros desde ese punto hasta el extremo derecho de la máscara. Los bits de la máscara de subred que son ceros identifican al computador o host en esa red. 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.

Resumen

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

- La conexión física que se debe producir para que un computador se conecte a Internet
- Los componentes principales de un computador
- La instalación y el diagnóstico de fallas de las tarjetas de interfaz de red y/o módems
- Los procedimientos de prueba básicos para probar la conexión a Internet
- La selección y configuración del navegador de Web
- El sistema numérico de Base 2
- La conversión de números binarios a decimales
- El sistema numérico hexadecimal
- La representación binaria de direcciones IP y máscaras de red
- La representación decimal de direcciones IP y máscaras de red

Módulo 2: Aspectos básicos de networking

Descripción general

El ancho de banda es un componente fundamental de networking. Las decisiones sobre el ancho de banda figuran entre las más importantes al diseñar una red. En este módulo se analiza la importancia del ancho de banda, y se explica cómo calcularlo y cómo medirlo.

Las funciones de networking se describen usando modelos divididos en capas. Este módulo abarca los dos modelos más importantes, que son el modelo de Internetworking de Sistemas Abiertos (OSI) y el modelo de Protocolo de control de transmisión/Protocolo Internet (TCP/IP). En el módulo también se exponen las diferencias y similitudes entre ambos modelos.

Además, este módulo presenta una breve historia de networking. También describe los dispositivos de red, al igual que las disposiciones físicas, lógicas y del cableado. Este modulo además define y compara las LAN, MAN, WAN, SAN y VPN.

Los estudiantes que completen este módulo deberán poder:

- Explicar la importancia del ancho de banda en networking.
- Explicar lo que es el ancho de banda a partir de una analogía basada en su propia experiencia.
- Identificar bps, kbps, Mbps, y Gbps como unidades de ancho de banda.
- Explicar la diferencia entre ancho de banda y tasa de transferencia.
- Calcular velocidades de transferencia de datos.
- Explicar por qué se utilizan modelos divididos en capas para describir la comunicación de datos.
- Explicar el desarrollo del modelo de Internetworking de Sistemas Abiertos (OSI).
- Detallar las ventajas de un enfoque dividido en capas.
- Identificar cada una de las siete capas del modelo OSI.
- Identificar las cuatro capas del modelo TCP/IP.
- Describir las similitudes y diferencias entre ambos modelos.
- Poder relatar brevemente la historia de networking.
- Identificar los dispositivos utilizados en networking.
- Comprender la función de los protocolos en networking.
- Definir LAN, WAN, MAN y SAN.
- Explicar las VPN y sus ventajas.
- Describir las diferencias entre redes internas y externas.

2.1 Terminología de networking

2.1.1 Redes de datos

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. ¹Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores mainframe, por lo cual no había una manera eficaz de compartir datos entre varios computadores. ²Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

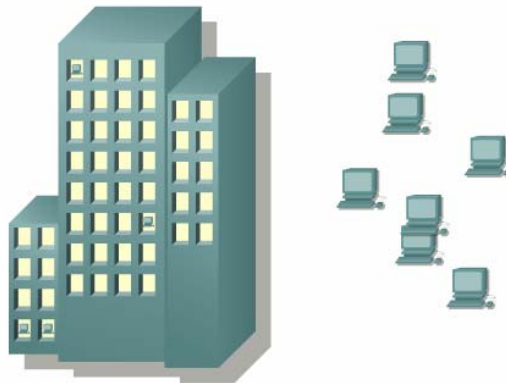


Figura 1

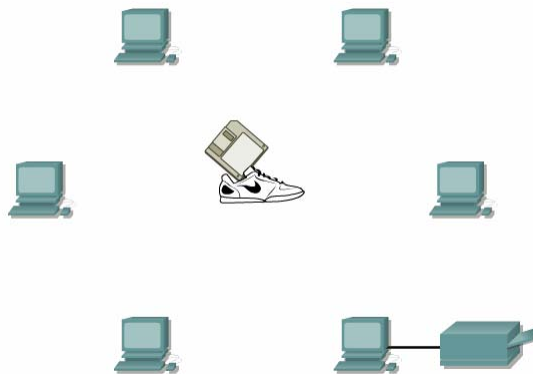


Figura 2

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de Red de área local (LAN - Local Area Network, en inglés). ³ Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN.

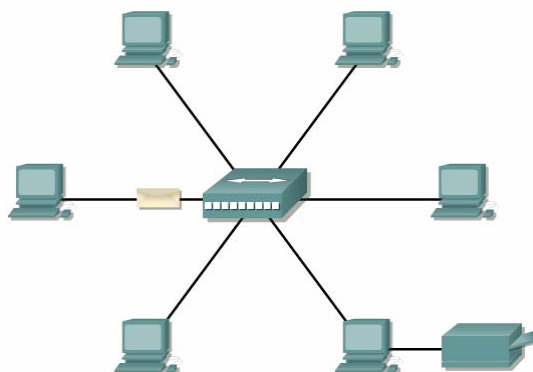


Figura 3

En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. ⁴

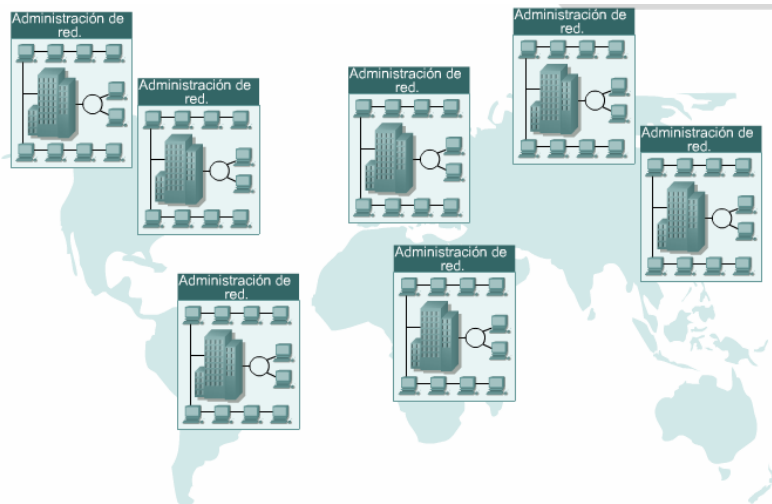


Figura 4

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. ⁵La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias. La Figura ⁶ resume las dimensiones relativas de las LAN y las WAN.

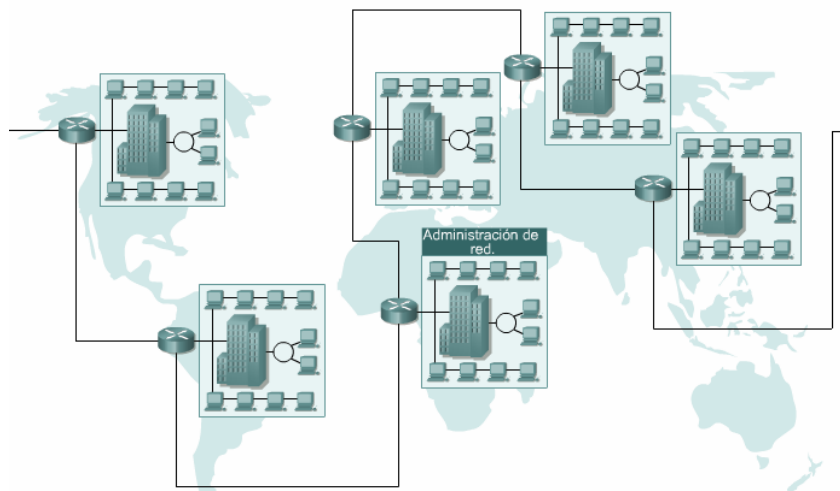


Figura 5

Distancia entre las CPU	Ubicación de las CPU	Nombre
0.1 m	Placa de circuito impreso/Asistente personal de datos	Motherboard Red de área personal (PAN)
1.0 m	Milímetro Mainframe	Red del sistema de la computadora
10 m	Habitación	Red de área local (LAN) Su aula
100 m	Edificio	Red de área local (LAN) Su escuela
1000 m = 1 km	Campus	Red de área local (LAN) Universidad de Stanford
100,000 m = 100 km	País	Red de área amplia (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continente	Red de área amplia (WAN) África
10,000,000 m = 10,000 km	Planeta	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Red de área amplia (WAN) Tierra y satélites artificiales

Figura 6

2.1.2 Historia de las redes informáticas

La historia de networking informática es compleja. ¹ 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. Los procesos de creación y comercialización son mucho más complicados, pero es útil analizar el desarrollo fundamental.

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	Inención 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 1980	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 1

En la década de 1940, los computadores eran enormes dispositivos electromecánicos que eran propensos a sufrir fallas. En 1947, la invención del transistor semiconductor permitió la creación de computadores más pequeños y confiables. En la década de 1950 los computadores mainframe, que funcionaban con programas en tarjetas perforadas, comenzaron a ser utilizados habitualmente por las grandes instituciones. A fines de esta década, se creó el circuito integrado, que combinaba muchos y, en la actualidad, millones de transistores en un pequeño semiconductor. En la década de 1960, los mainframes con terminales eran comunes, y los circuitos integrados comenzaron a ser utilizados de forma generalizada.

Hacia fines de la década de 1960 y durante la década de 1970, se inventaron computadores más pequeños, denominados minicomputadores. Sin embargo, estos minicomputadores seguían siendo muy voluminosos en comparación con los estándares modernos. En 1977, la Apple Computer Company presentó el microcomputador, conocido también como computador personal. En 1981 IBM presentó su primer computador personal. El equipo Mac, de uso sencillo, el PC IBM de arquitectura abierta y la posterior microminiaturización de los circuitos integrados dieron como resultado el uso difundido de los computadores personales en hogares y empresas.

A mediados de la década de 1980 los usuarios con computadores autónomos comenzaron a usar módems para conectarse con otros computadores y compartir archivos. Estas comunicaciones se denominaban comunicaciones punto-a-punto o de acceso telefónico. El concepto se expandió a través del uso de computadores que funcionaban como punto central de comunicación en una conexión de acceso telefónico. Estos computadores se denominaron tableros de boletín. Los usuarios se conectaban a los tableros de boletín, donde depositaban y levantaban mensajes, además de cargar y descargar archivos. La desventaja de este tipo de sistema era que había poca comunicación directa, y únicamente con quienes conocían el tablero de boletín. Otra limitación era la necesidad de un módem por cada conexión al computador del tablero de boletín. Si cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco líneas telefónicas diferentes. A medida que crecía el número de usuarios interesados, el sistema no pudo soportar la demanda. Imagine, por ejemplo, que 500 personas quisieran conectarse de forma simultánea. A partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos (DoD) desarrolló redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico. Esta tecnología era diferente de la comunicación punto-a-punto usada por los tableros de boletín. Permitía la internetworking de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión. La WAN del DoD finalmente se convirtió en la Internet.

2.1.3 Dispositivos de networking

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos. El primer grupo está compuesto por los dispositivos de usuario final. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario. 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.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. ¹Estos 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. ²Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computador, o puede ser un dispositivo periférico. También se denomina adaptador de red. Las NIC para computadores portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. ³Cada 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 1

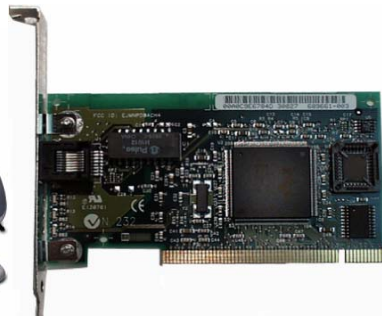


Figura 2



Figura 3

No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. ⁴ Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.

Dispositivos del usuario final	
PC	Impresora
MAC	Servidor de archivos
Computadora portátil	Mainframe IBM

Figura 4

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. ⁵ Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers. Todos los dispositivos de red que aquí se mencionan, se tratarán con mayor detalle más adelante en el curso. Por ahora se brinda una breve descripción general de los dispositivos de networking.

Dispositivos de red	
Repetidor	Puente
Hub 10BASE-T	Switch de grupo de trabajo
Hub 100BASE-T	Router
Hub	Nube de red

Figura 5

Un repetidor 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. ⁶

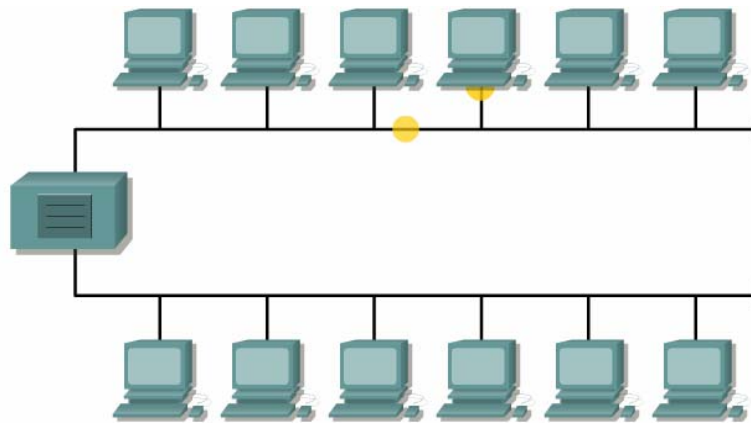


Figura 6

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. ⁷ 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.

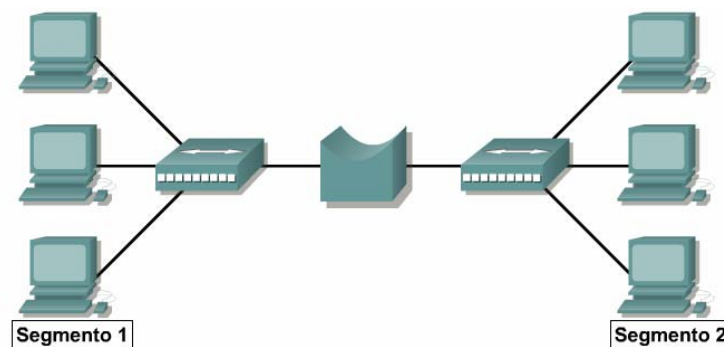


Figura 7

Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. ⁸ No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

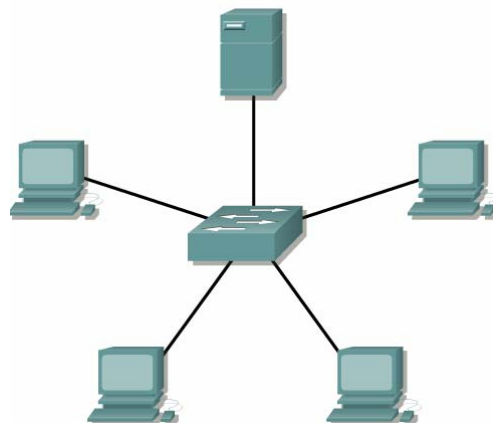


Figura 8

Los routers poseen todas las capacidades indicadas arriba. ⁹ Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

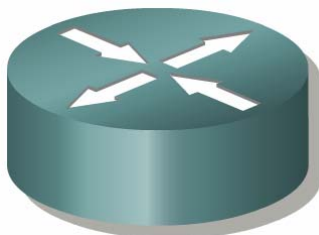


Figura 9

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: ¹ ²

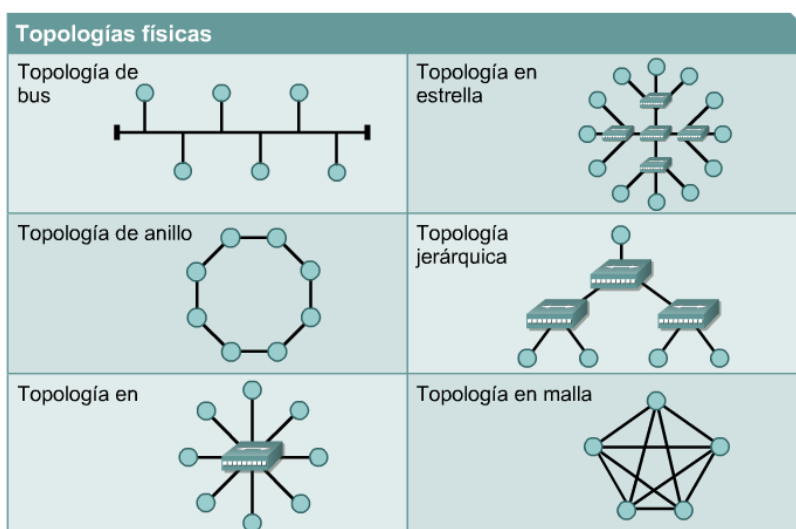


Figura 1

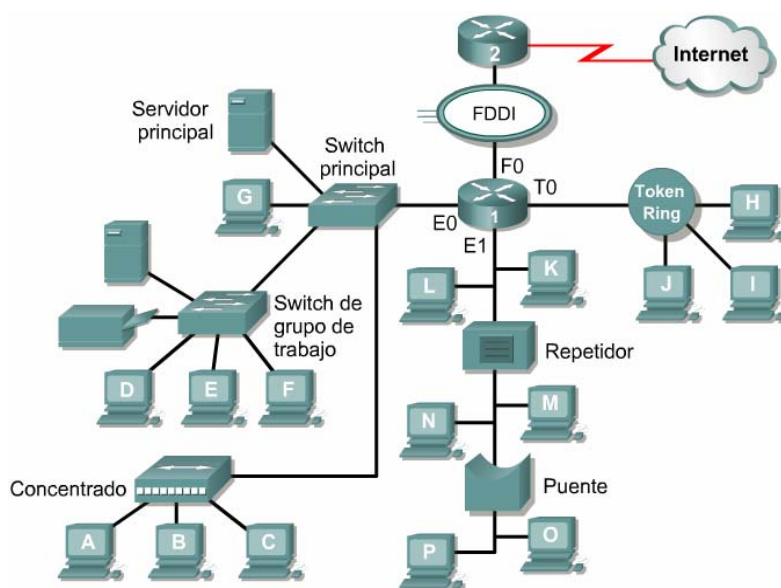


Figura 2

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

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

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada. Ethernet funciona así, tal como se explicará en el curso más adelante.

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

El diagrama en la Figura 2 muestra diferentes topologías conectadas mediante dispositivos de red. Muestra una LAN de complejidad moderada que es típica de una escuela o de una pequeña empresa. Tiene muchos símbolos, y describe varios conceptos de networking que lleva cierto tiempo aprender.

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, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador. 1

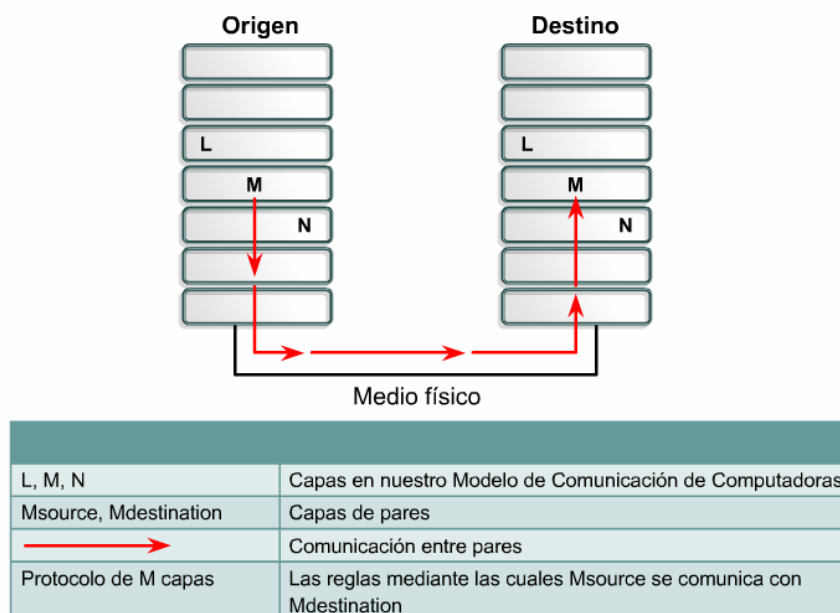


Figura 1

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

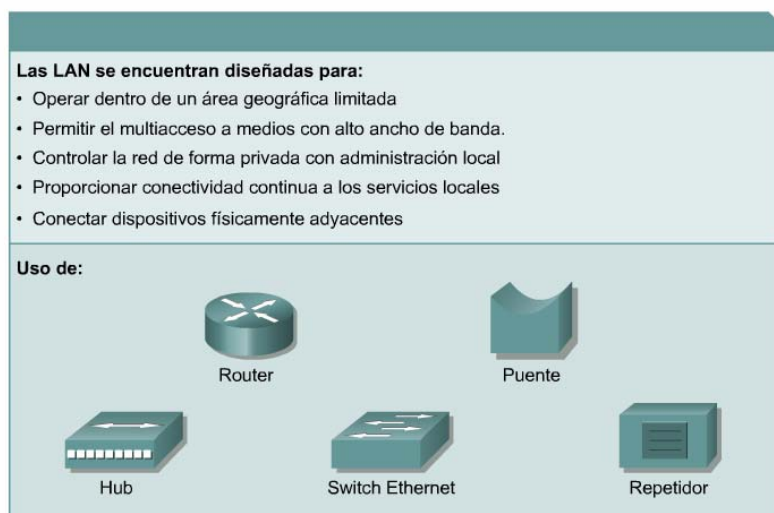
- Cómo se construye la red física
- Cómo los computadores se conectan a la red
- Cómo se formatean los datos para su transmisión
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de diferentes 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).

2.1.6 Redes de área local (LAN)

Las LAN constan de los siguientes componentes:

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



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

Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI

2.1.7 Redes de área amplia (WAN)

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidos por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

Las WAN están diseñadas para realizar lo siguiente:

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



Algunas de las tecnologías comunes de WAN son:

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

2.1.8 Redes de área metropolitana (MAN)

La MAN 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.

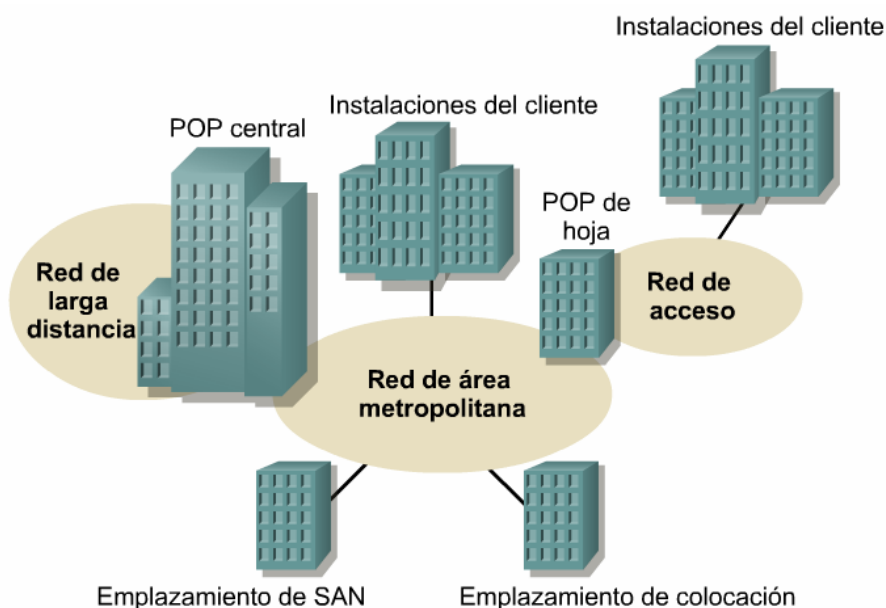
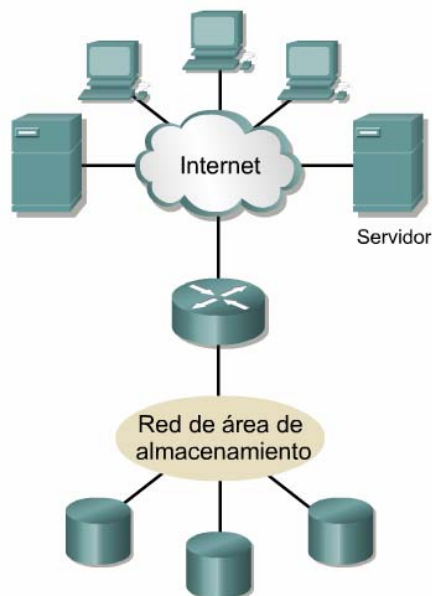


Figura 1

2.1.9 Redes de área de almacenamiento (SAN)

Una SAN es una red dedicada, de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores.

La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

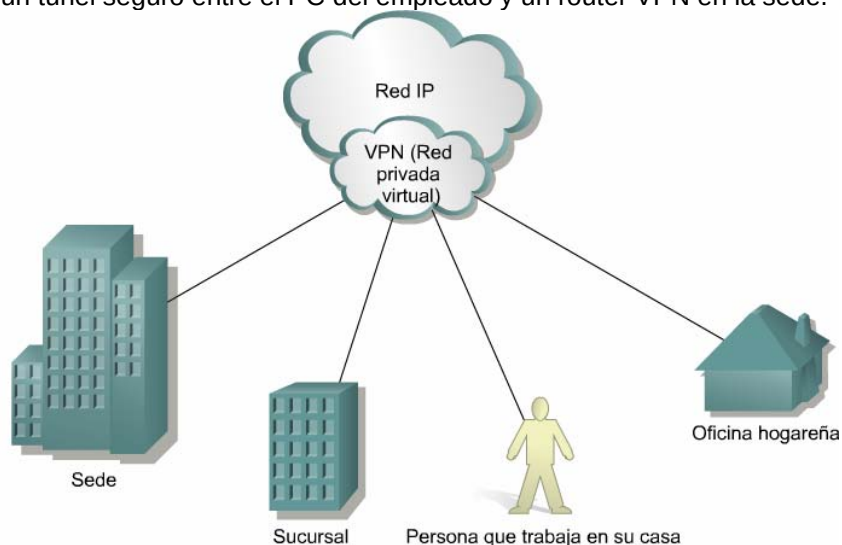


Las SAN poseen las siguientes características:

- **Rendimiento:** Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.
- **Disponibilidad:** Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de 10 kilómetros (km) o 6,2 millas.
- **Escalabilidad:** Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías. Esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

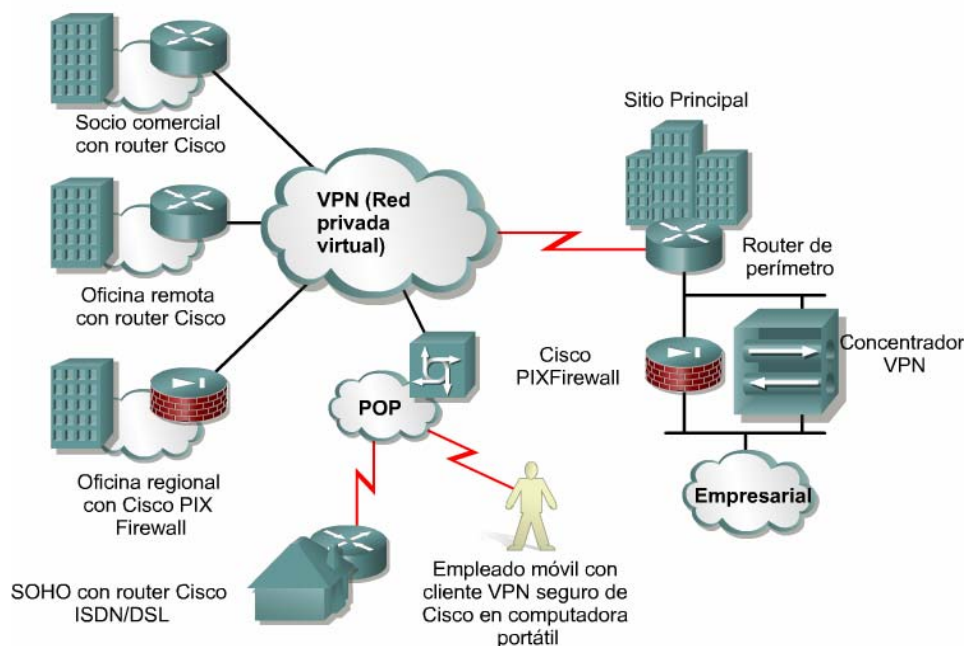
2.1.10 Red privada virtual (VPN)

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



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.



A continuación se describen los tres principales tipos de VPN:

- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.
- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.
- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

2.1.12 Redes internas y externas

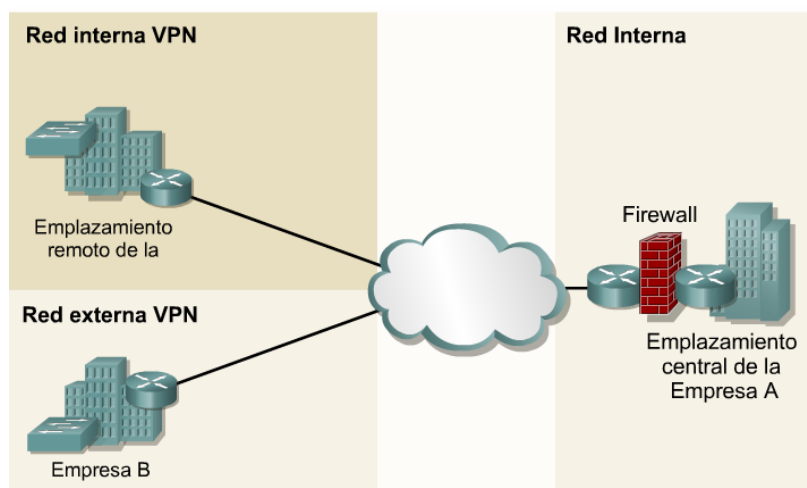


Figura 1

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet". Los servidores de Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas. ¹

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

Por qué es importante el ancho de banda:

- El ancho de banda se encuentra limitado por razones físicas y tecnológicas
- El ancho de banda no es gratuito
- Los requisitos de ancho de banda aumentan a gran velocidad
- El ancho de banda es fundamental para el desempeño de la red

Figura 1

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 kbps 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.
2. **El ancho de banda no es gratuito.** Es posible adquirir equipos para una red de área local (LAN) capaz de brindar un ancho de banda casi ilimitado durante un período extendido de tiempo. Para conexiones de red de área amplia (WAN), casi siempre hace falta comprar el ancho de banda de un proveedor de servicios. En ambos casos, comprender el significado del ancho de banda, y los cambios en su demanda a través del tiempo, pueden ahorrarle importantes sumas de dinero a un individuo o a una empresa. Un administrador de red necesita tomar las decisiones correctas con respecto al tipo de equipo y servicios que debe adquirir.
3. **El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender la Internet.** Un profesional de networking debe comprender el fuerte impacto del ancho de banda y la tasa de transferencia en el rendimiento y el diseño de la red. La información fluye en una cadena de bits de un computador a otro en todo el mundo. Estos bits representan enormes cantidades de información que fluyen de ida y de vuelta a través del planeta en segundos, o menos. En cierto sentido, puede ser correcto afirmar que la Internet es puro ancho de banda.
4. **La demanda de ancho de banda no para de crecer.** No bien se construyen nuevas tecnologías e infraestructuras de red para brindar mayor ancho de banda, se crean nuevas aplicaciones que aprovechan esa mayor capacidad. La entrega de contenidos de medios enriquecidos a través de la red, incluyendo video y audio fluido, requiere muchísima cantidad de ancho de banda. Hoy se instalan comúnmente sistemas telefónicos IP en lugar de los tradicionales sistemas de voz, lo que

contribuye a una mayor necesidad de ancho de banda. Un profesional de networking exitoso debe anticiparse a la necesidad de mayor ancho de banda y actuar en función de eso.

2.2.2 El escritorio

El ancho de banda se define como la cantidad de información que puede fluir a través de una red en un período dado. La idea de que la información fluye, sugiere dos analogías que podrían facilitar la visualización del ancho de banda en una red. Ya que se dice que el agua y el tráfico fluyen, vea las siguientes analogías:

1. **El ancho de banda es similar al diámetro de un caño.** ¹Una red de tuberías trae agua potable a los hogares y las empresas y se lleva las aguas servidas. Esta red de agua está compuesta de tuberías de diferentes diámetros. Las principales tuberías de agua de una ciudad pueden medir dos metros de diámetro, en tanto que la tubería de un grifo de cocina puede medir apenas dos centímetros. El ancho de la tubería determina su capacidad de transporte de agua. Por lo tanto, el agua es como los datos, y el ancho de la tubería es como el ancho de banda. Muchos expertos en networking dicen que necesitan poner tuberías más grandes si desean agregar capacidad para transportar información.

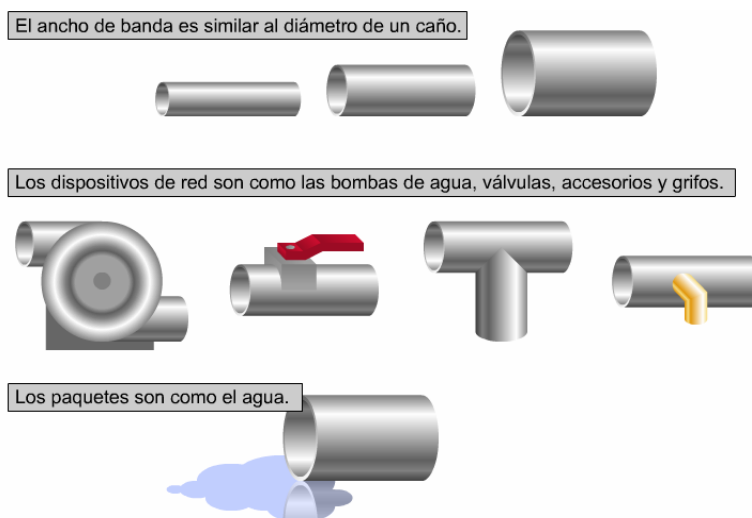


Figura 1



Figura 2

2. **El ancho de banda también puede compararse con la cantidad de carriles de una autopista.** ²Una 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 aquellas 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.

2.2.3 Medición

En los sistemas digitales, la unidad básica del ancho de banda es bits por segundo (bps). El ancho de banda es la medición de la cantidad de información, o bits, que puede fluir desde un lugar hacia otro en un período de tiempo determinado, o segundos. Aunque el ancho de banda se puede describir en bits por segundo, se suelen usar múltiplos de bits por segundo. En otras palabras, el ancho de banda de una red generalmente se describe en términos de miles de bits por segundo (kbps), millones de bits por segundo (Mbps), miles de millones de bits por segundo (Gbps) y billones de bits por segundo (Tbps). ¹A pesar de que las expresiones ancho de banda y velocidad a menudo se usan en forma indistinta, no significan exactamente lo mismo. Se puede decir, por ejemplo, que una conexión T3 a 45Mbps opera a una velocidad mayor que una conexión T1 a 1,544Mbps. No obstante, si sólo se utiliza una cantidad pequeña de su capacidad para transportar datos, cada uno de estos tipos de conexión transportará datos a aproximadamente la misma velocidad. Por ejemplo, una cantidad pequeña de agua fluirá a la misma velocidad por una tubería pequeña y por una tubería grande. Por lo tanto, suele ser más exacto decir que una conexión T3 posee un mayor ancho de banda que una conexión T1. Esto es así porque la conexión T3 posee la capacidad para transportar más información en el mismo período de tiempo, y no porque tenga mayor velocidad.

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 1

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
Fibra Óptica Monomodo (9/125µm) (1000BASE-LX Ethernet)	1000 Mbps	5000 m

Figura 1

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 señalar y detectar señales de red.

Por ejemplo, la actual comprensión de la física de los cables de cobre de par trenzado no blindados (UTP) establece el límite teórico del ancho de banda en más de un gigabit por segundo (Gbps). Sin embargo, en la realidad, el ancho de banda queda determinado por el uso de Ethernet 10BASE-T, 100BASE-TX, o 1000BASE-TX. En otras palabras, el ancho de banda real queda determinado por los métodos de señalización, las tarjetas de interfaz de red (NIC) y los demás equipos de red seleccionados. Por lo tanto, el ancho de banda no sólo queda determinado por las limitaciones de los medios.

La figura 1 muestra algunos tipos comunes de medios de networking y los límites de distancia y ancho de banda al usar la tecnología de networking indicada.

La figura 2 resume los servicios WAN comunes y el ancho de banda asociado con cada servicio.

Servicio WAN	Usuario Típico	Ancho de Banda
Modem	Individuos	56 kbps = 0.056 Mbps
DSL	Individuos, teleconmuters, y pequeños negocios	128 kbps to 6.1 Mbps = 0.128 Mbps to 6.1 Mbps
ISDN	Teleconmuters y pequeños negocios	128 kbps = 0.128 Mbps
Frame Relay	Instituciones pequeñas (escuelas", WANs confiables	56 kbps to 44.736 Mbps (U.S.) or 34.368 Mbps (Europe) = 0.056 Mbps to 44.736 Mbps (U.S.) or 34.368 Mbps (Europe)
T1	Grandes Instituciones	1.544 Mbps
E1	Grandes Instituciones	2.048 Mbps
T3	Grandes Instituciones	44.736 Mbps
E3	Grandes Instituciones	34.368 Mbps
STS-1 (OC-1)	Compañías Telefónicas, Backbones de Compañías de Comunicación de Datos	51.840 Mbps
STM-1	Compañías Telefónicas, Backbones de Compañías de Comunicación de Datos	155.52 Mbps
STS-3 (OC-3)	Compañías Telefónicas, Backbones de Compañías de Comunicación de Datos	155.251 Mbps
STM-3	Compañías Telefónicas, Backbones de Compañías de Comunicación de Datos	466.56 Mbps
STS-48 (OC-48)	Compañías Telefónicas, Backbones de Compañías de Comunicación de Datos	2.488320 Gbps

Figura 2

2.2.5 Tasa de transferencia

El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo. Por lo tanto, la cantidad de ancho de banda disponible es un punto crítico de la especificación de la red. Una LAN típica se podría construir para brindar 100 Mbps a cada estación de trabajo individual, pero esto no significa que cada usuario pueda realmente mover cien megabits de datos a través de la red por cada segundo de uso. 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. 1A continuación se detallan algunos de los factores que determinan la tasa de transferencia:

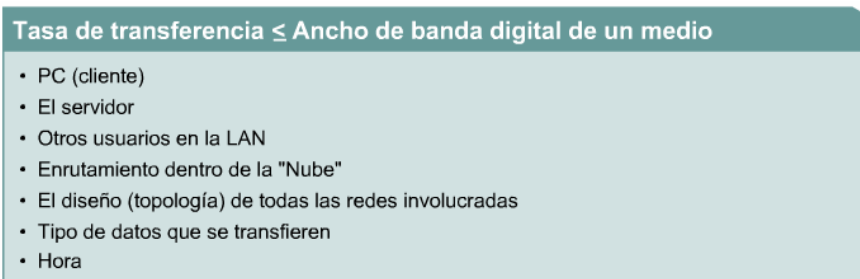


Figura 1

- Dispositivos de internetworking
- Tipo de datos que se transfieren
- Topología de la red
- Cantidad de usuarios en la red
- Computador del usuario
- Computador 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 ($T = T_m / AB$), 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. ¹



BW	Máximo ancho de banda teórico del "enlace más lento" entre el host origen y el host objetivo (medido en bits por segundo).
P	Tasa de transferencia real en el momento de la transferencia (medida en bits por segundo)
T	Tiempo en el que se debe producir la transferencia de archivos (medido en segundos)
S	Tamaño del archivo en bits

Figura 1

Hay dos puntos importantes a considerar al realizar este cálculo:

- El resultado no es más que un estimado, porque el tamaño del archivo no incluye el gasto agregado por el encapsulamiento.

- Es probable que el resultado sea el tiempo de transferencia en el mejor de los casos, ya que el ancho de banda disponible casi nunca está en el máximo teórico para el tipo de red. Se puede obtener un estimado más preciso sustituyendo el ancho de banda por la tasa de transferencia en la ecuación.

Aunque el cálculo de transferencia de datos es muy sencillo, es importante asegurarse de usar las mismas unidades a lo largo de toda la ecuación. En otras palabras, si el ancho de banda se mide en megabits por segundo (Mbps), el tamaño del archivo debe expresarse en megabits (Mb), y no en megabytes (MB). Como el tamaño de los archivos se suele expresar en megabytes, es posible que sea necesario multiplicar la cantidad de megabytes por ocho para convertirla a megabits.

Intente responder la siguiente pregunta, aplicando la fórmula $T = T_m / AB$. Asegúrese de convertir las unidades de medida según sea necesario.

¿Llevaría menos tiempo enviar el contenido de un disquete (1,44 MB) lleno de datos a través de una línea RSDI, o enviar el contenido de un disco duro de 10 GB lleno de datos a través de una línea OC-48?

2.2.7 Digital versus analógico

Hasta hace poco, las transmisiones de radio, televisión y teléfono se enviaban por aire y por cables utilizando ondas electromagnéticas. Estas ondas se denominan analógicas porque poseen la misma forma que las ondas de luz y sonido producidas por los transmisores. 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. ¹

El ancho de banda (digital) es como el ancho de banda analógico.



Los dispositivos de red son como los teléfonos, radios AM/FM y reproductores de CD ROM.



Los paquetes son como la música.



Figura 1

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.

2.3 Modelos de networking

2.3.1 Uso de capas para analizar problemas en un flujo de materiales

El concepto de capas se utiliza para describir la comunicación entre dos computadores. La figura 1 muestra un conjunto de preguntas relacionadas con flujo, que se define como el movimiento de objetos físicos o lógicos, a través de un sistema. Estas preguntas muestran cómo el concepto de capas ayuda a describir los detalles del proceso de flujo. Este proceso puede referirse a cualquier tipo de flujo, desde el flujo del tráfico en un sistema de autopistas, al flujo de datos a través de una red. La figura 2 muestra varios ejemplos de flujo, y formas en las que se puede desglosar el proceso de flujo en detalles o en capas.

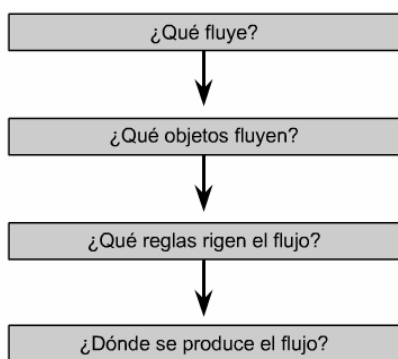


Figura 1

Red	Qué fluye	Distintas formas	Reglas	Dónde
Agua	Agua	Caliente, fría, potable, servida	Reglas de acceso (abrir o cerrar grifos); vaciar el agua del inodoro; no echar ciertas cosas en las cañerías	Caños
Autopista	Vehículos	Camiones, autos, motocicletas y bicicletas	Leyes de tránsito y reglas de cortesía	Rutas y autopistas
Servicio postal	Objetos	Cartas (información escrita); paquetes	Reglas para el empaquetado y franqueo	Buzones, oficinas, camiones, aviones, carteros
Teléfono	Información	Idiomas hablados	Reglas de acceso al teléfono y reglas de cortesía	Cables telefónicos, ondas electromagnéticas, etc.

Figura 2

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 computadores envían información a través de una red, todas las comunicaciones se generan en un origen y luego viajan a un destino. ³

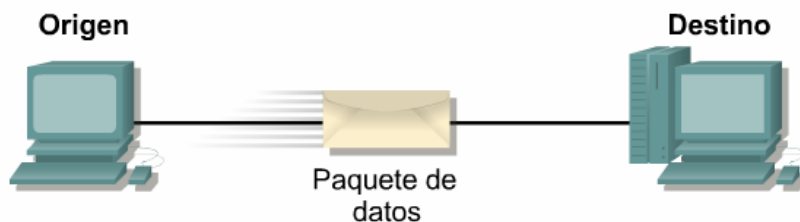


Figura 3

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 computador.

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

2.3.2 Uso de capas para describir la comunicación de datos

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Por ejemplo, al pilotar un avión, los pilotos obedecen reglas muy específicas para poder comunicarse con otros aviones y con el control de tráfico aéreo.

Un protocolo de comunicaciones de datos es un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.

La Capa 4 del computador de origen se comunica con la Capa 4 del computador de destino. ¹ Las normas y convenciones utilizadas para esta capa reciben el nombre de protocolos de la Capa 4. Es importante recordar que los protocolos preparan datos en forma lineal. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

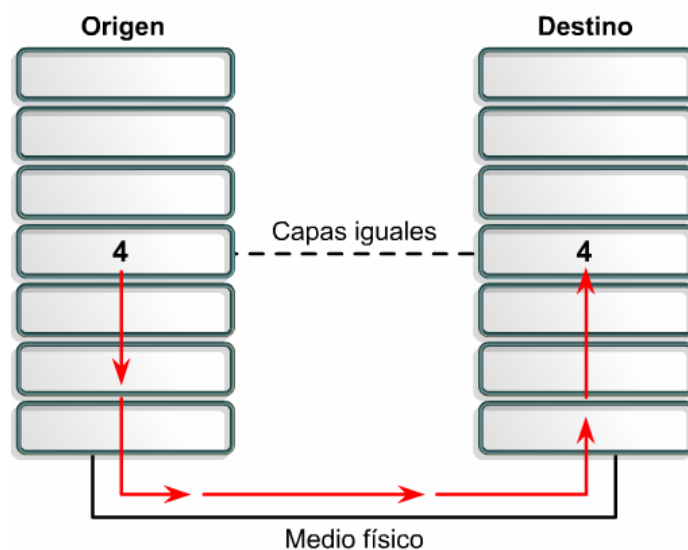


Figura 1

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente.

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. ¹

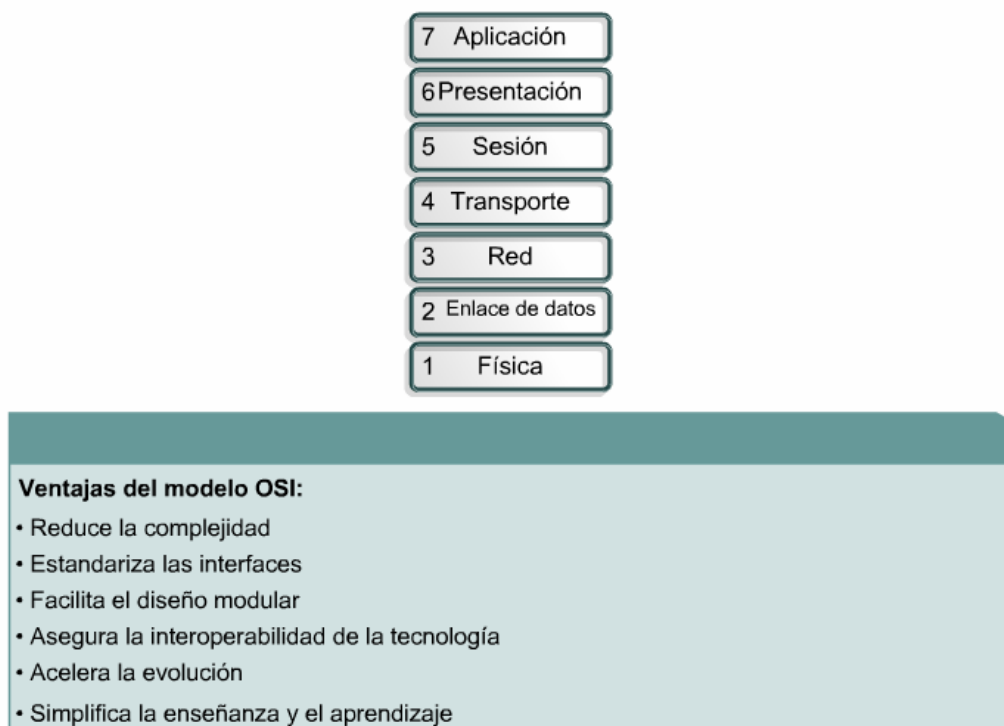


Figura 1

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

2.3.4 Las capas del modelo OSI

El modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. El modelo de referencia OSI explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. 1- 7 La división de la red en siete capas permite obtener las siguientes ventajas:

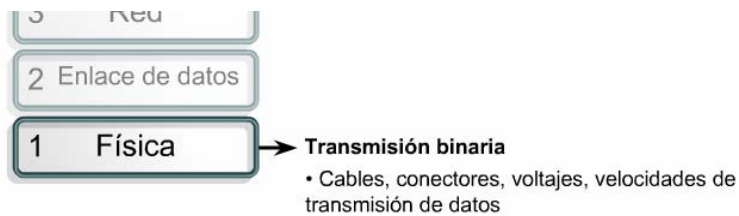


Figura 1



Figura 2

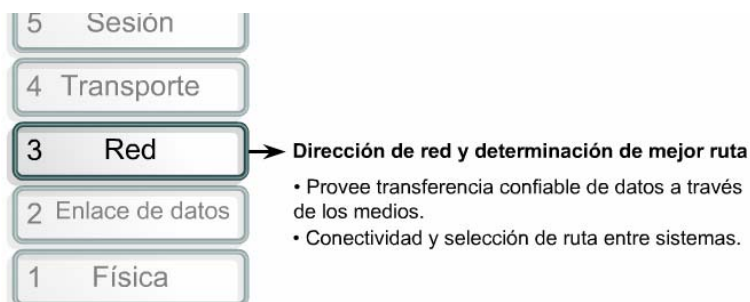


Figura 3

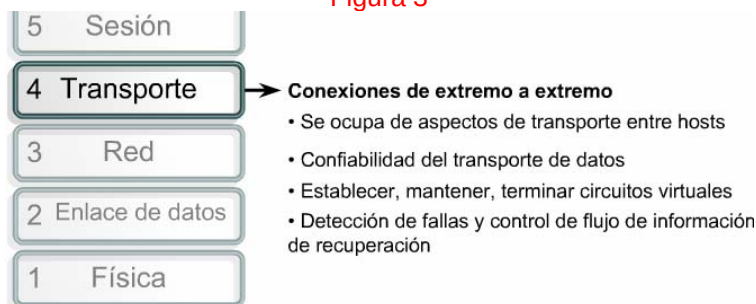


Figura 4



Figura 5

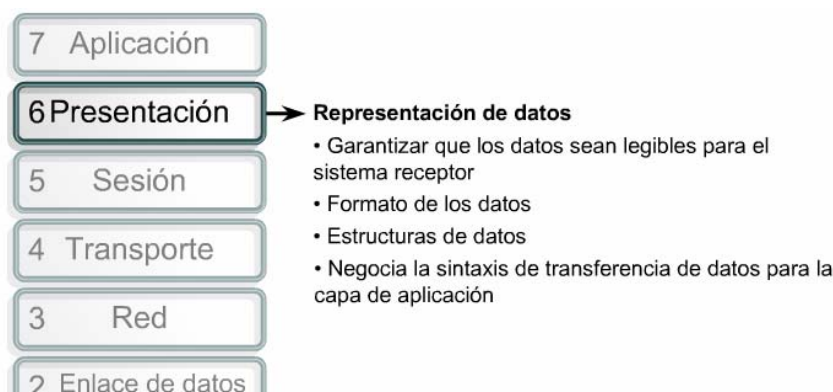


Figura 6

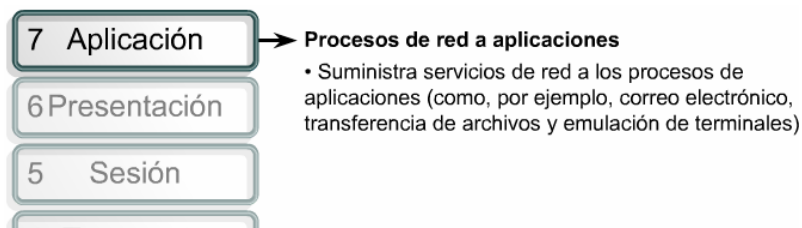


Figura 7

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

2.3.5 Comunicaciones de par a par

Para que los datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino. Esta forma de comunicación se conoce como de par-a-par. Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo (PDU). Cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino, como lo ilustra la figura 1.

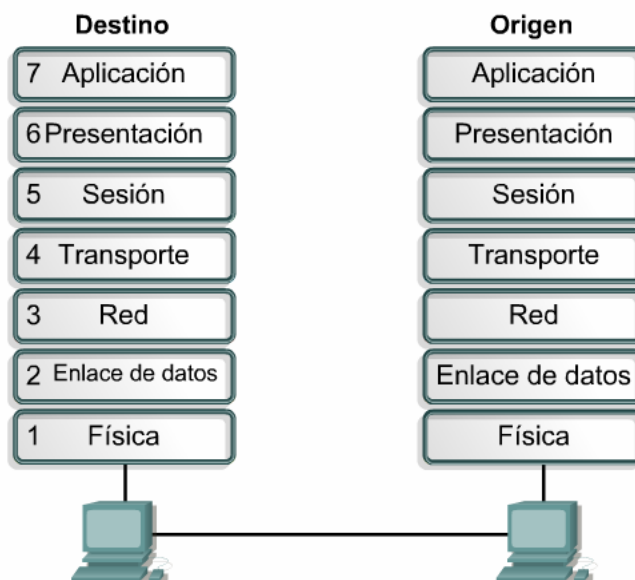


Figura 1

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. ²

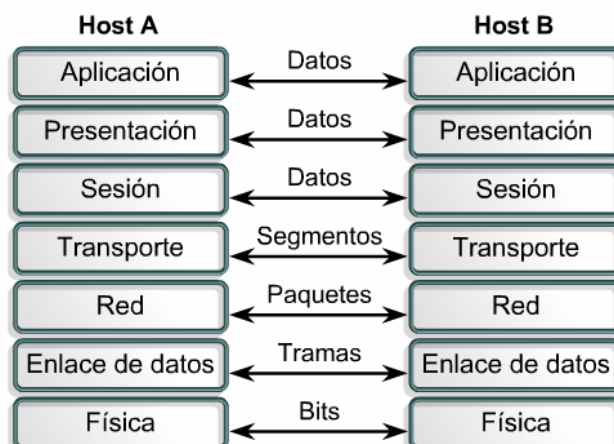


Figura 2

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.

La capa física también suministra un servicio a la capa de enlace de datos. La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1.

2.3.6 Modelo TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

A diferencia de las tecnologías de networking propietarias mencionadas anteriormente, el TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar.

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red ¹

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. Lo más notable es que la capa de aplicación posee funciones diferentes en cada modelo.

Los diseñadores de TCP/IP sintieron que la capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.



Figura 1

La capa de transporte se encarga de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.

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 computadores 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 física y de enlace de datos del modelo OSI.

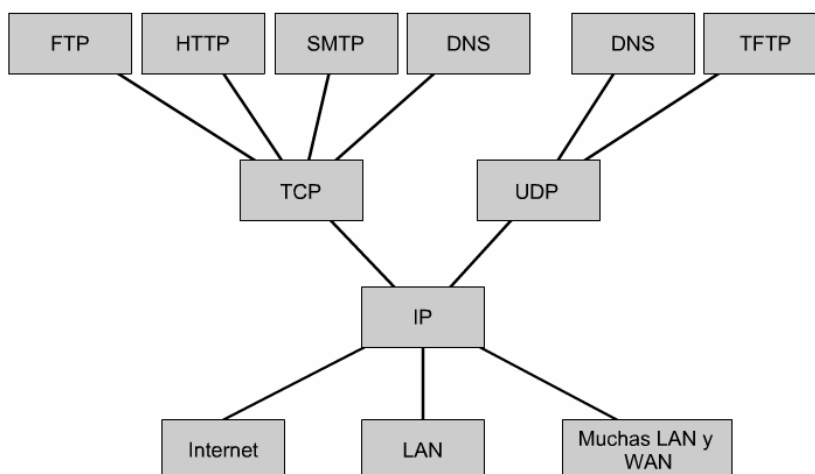


Figura 2

La figura 2 ilustra algunos de los protocolos comunes especificados por las capas del modelo de referencia TCP/IP. Algunos de los protocolos de capa de aplicación más comúnmente usados incluyen los siguientes:

- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Sistema de denominación de dominios (DNS)
- Protocolo Trivial de Transferencia de Archivos (TFTP)

Los protocolos de capa de transporte comunes incluyen:

- Protocolo para el Control del Transporte (TCP)
- Protocolo de Datagrama de Usuario (UDP)

El protocolo principal de la capa Internet es:

- Protocolo Internet (IP)

La capa de acceso de red se refiere a cualquier tecnología en particular utilizada en una red específica.

Independientemente de los servicios de aplicación de red que se brinden y del protocolo de transferencia que se utilice, existe un solo protocolo de Internet, IP. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

Comparando el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias. [3](#)

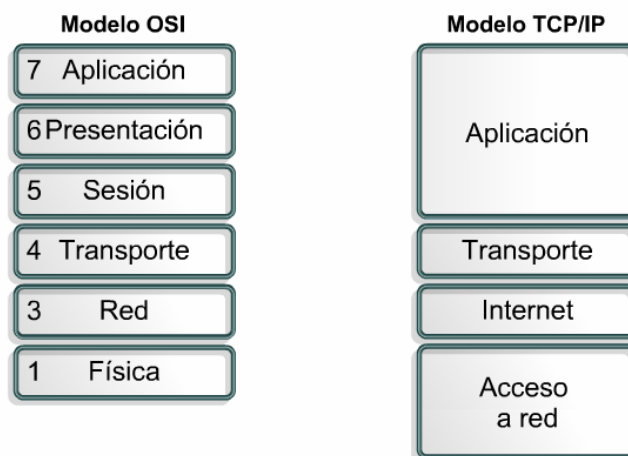


Figura 3

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 el currículum 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

Recuerden que hay una diferencia entre un modelo y un protocolo que realmente se utiliza en networking. Se utilizará el modelo OSI para describir protocolos TCP/IP. [4](#)

Modelo OSI	Protocolos TCP/IP y Ethernet
7 Aplicación	FTP, TFTP, HTTP, SMTP, DNS, TELNET, SNMP
6 Presentación	Enfoque muy reducido
5 Sesión	
4 Transporte	TCP
3 Red	IP
1 Física	Ethernet

Figura 4

2.3.7 Proceso detallado de encapsulamiento

Todas las comunicaciones de una red parten de un origen y se envían a un destino. La información que se envía a través de una red se denomina datos o paquetes de datos. Si un computador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

Para ver cómo se produce el encapsulamiento, examine la forma en que los datos viajan a través de las capas como lo ilustra la figura [1](#). Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendente. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las capas realizan sus funciones para los usuarios finales. Como lo muestra la figura [2](#), las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

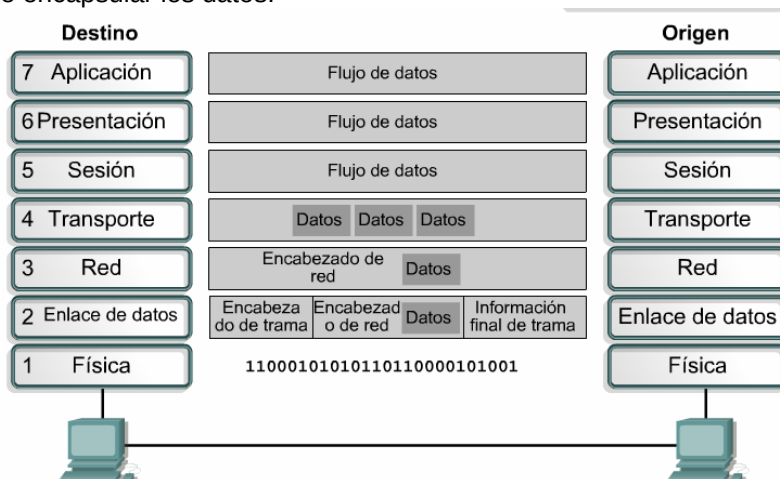


Figura 1

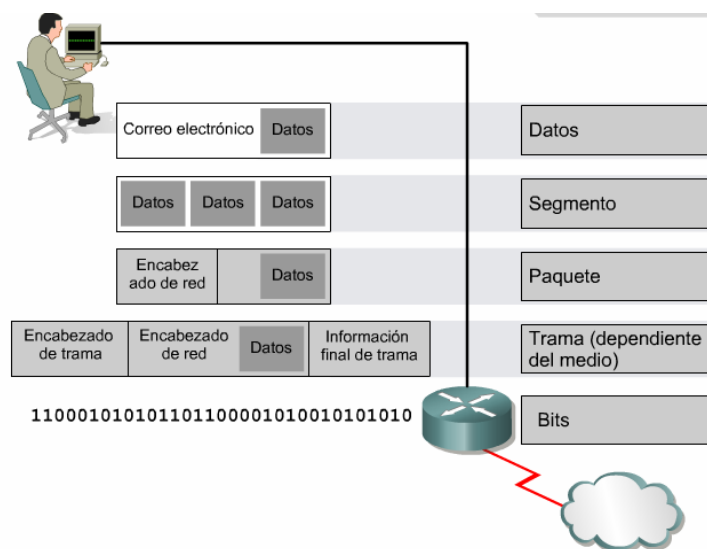


Figura 2

1. **Crear los datos.** Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.
2. **Empaquetar los datos para ser transportados de extremo a extremo.** Los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts de mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.
3. **Agregar la dirección de red IP al encabezado.** Los datos se colocan en un paquete o datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.
4. **Agregar el encabezado y la información final de la capa de enlace de datos.** Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.
5. **Realizar la conversión a bits para su transmisión.** La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio. Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de una universidad y salir por un enlace WAN hasta llegar a su destino en otra LAN remota.

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, el computador del usuario y el servidor
- Se puede usar la fórmula $T = T_m / AB$ (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.

Módulo 3: Medios de networking

Descripción general

El cable de cobre se utiliza en casi todas las LAN. Hay varios tipos de cable de cobre disponibles en el mercado, y cada uno presenta ventajas y desventajas. La correcta selección del cableado es fundamental para que la red funcione de manera eficiente. Debido a que el cobre transporta información utilizando corriente eléctrica, es importante comprender algunos principios básicos de la electricidad a la hora de planear e instalar una red.

La fibra óptica es el medio utilizado con mayor frecuencia en las transmisiones de punto a punto de mayor distancia y alto ancho de banda que requieren los backbones de LAN y las WAN. En los medios ópticos, se utiliza la luz para transmitir datos a través de una delgada fibra de vidrio o de plástico. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por la fibra. El host receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. Sin embargo, no hay electricidad en el cable de fibra óptica en sí. De hecho, el vidrio utilizado en el cable de fibra óptica es un muy buen aislante eléctrico.

La conectividad física permitió un aumento en la productividad permitiendo que se compartan impresoras, servidores y software. Los sistemas tradicionales de red requieren que las estaciones de trabajo permanezcan estacionarias permitiendo movimientos sólo dentro del alcance de los medios y del área de la oficina.

La introducción de la tecnología inalámbrica elimina estas limitaciones y otorga portabilidad real al mundo de la computación. En la actualidad, la tecnología inalámbrica no ofrece las transferencias a alta velocidad, la seguridad o la confiabilidad de tiempo de actividad que brindan las redes que usan cables. Sin embargo, la flexibilidad de no tener cables justifica el sacrificio de estas características.

A menudo, los administradores tienen en cuenta las comunicaciones inalámbricas al instalar una nueva red o al actualizar una red existente. Una red inalámbrica puede empezar a funcionar sólo unos pocos minutos después de encender las estaciones de trabajo. Se proporciona la conectividad a Internet a través de una conexión con cable, router, cablemódem o módem DSL y un punto de acceso inalámbrico que sirve de hub para los nodos inalámbricos. En el entorno residencial o de una pequeña oficina, es posible combinar estos dispositivos en una sola unidad.

Los estudiantes que completen este módulo deberán poder:

- Discutir las propiedades eléctricas de la materia.
- Definir voltaje, resistencia, impedancia, corriente y circuitos.
- Describir las especificaciones y el rendimiento de los distintos tipos de cable.
- Describir el cable coaxial y sus ventajas y desventajas en comparación con otros tipos de cable.
- Describir el cable de par trenzado blindado (STP) y sus usos.
- Describir el cable de par trenzado no blindado (UTP) y sus usos.
- Discutir las características de los cables derechos, cruzados y transpuestos y dónde se utiliza cada uno.
- Explicar los principios básicos del cable de fibra óptica.
- Describir cómo las fibras pueden guiar la luz a través de largas distancias.
- Describir la fibra monomodo y multimodo.
- Describir cómo se instala la fibra.
- Describir el tipo de conectores y equipos que se utilizan con el cable de fibra óptica.
- Explicar cómo se prueba la fibra para asegurarse de que funcione correctamente.
- Discutir los temas de seguridad relacionados con la fibra óptica.

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.

Para poder comprender mejor las propiedades eléctricas de los elementos/materiales, busque "helio" (He) en la tabla periódica. **1**El número atómico del helio es 2, lo que significa que tiene 2 protones y 2 electrones. Su peso atómico es 4. Si se le resta el número atómico (2) al peso atómico (4), se puede determinar que el helio también tiene 2 neutrones.

1 H																	2 He				
3 Li	4 Be															5 B	6 C	7 N	8 O	9 F	10 Ne
11 Na	12 Mg															13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr				
37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe				
55 Cs	56 Ba	71 Lu	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn				
87 Fr	88 Ra	103 Lr	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Uuu	112 Uub	113 Uut	114 Uuq	115 Uup	116 Uuh	117 Uus	118 Uuo				

57 La	58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb
89 Ac	90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No

Figura 1

El físico danés Niels Bohr desarrolló un modelo simplificado para ilustrar el átomo. ²El gráfico muestra el modelo correspondiente al átomo de helio Si los protones y los neutrones de un átomo tuvieran el tamaño de una pelota de fútbol Nro. 5, en el medio de un estadio de fútbol, la única cosa más pequeña que la pelota serían los electrones. Los electrones tendrían el tamaño de una cereza, y estarían orbitando cerca de los últimos asientos del estadio. En otras palabras, el volumen total de este átomo, incluido el recorrido de los electrones, tendría el tamaño del estadio. El núcleo del átomo donde se encuentran los protones y los neutrones tendría el tamaño de la pelota de fútbol.

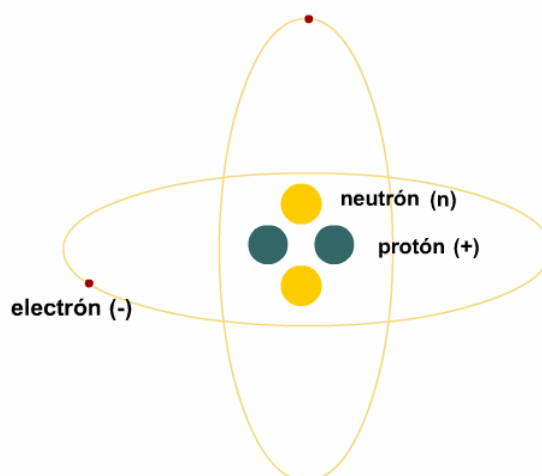


Figura 2

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. 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. 3

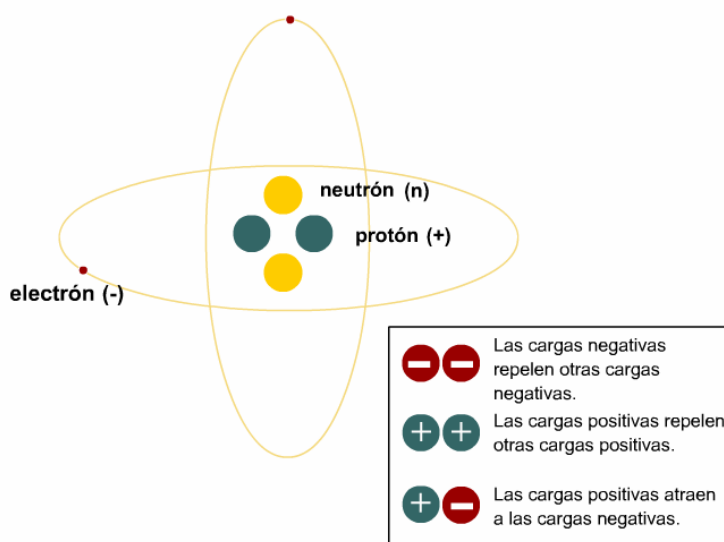


Figura 3

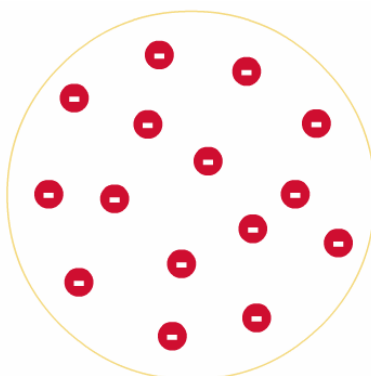
Examine el modelo de Bohr del átomo de helio. Si la ley de Coulomb es verdadera, y si el modelo de Bohr describe los átomos de helio como estables, entonces deben intervenir otras leyes de la naturaleza. ¿Cómo es posible que ambas sean verdaderas?

- **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.

Los electrones se mantienen en órbita aun cuando los protones atraen a los electrones. Los electrones tienen la velocidad justa y necesaria para mantenerse en órbita y para no caer en el núcleo, tal como ocurre con la Luna con respecto a la Tierra.

Los protones no se repelen entre sí porque existe una fuerza nuclear que está relacionada con los neutrones. La fuerza nuclear es una fuerza increíblemente poderosa que actúa como si fuera un pegamento que mantiene unidos a los protones.

Los protones y los neutrones permanecen unidos entre sí mediante una fuerza muy poderosa. Sin embargo, una fuerza mucho más débil es la que mantiene a los electrones en su órbita alrededor del núcleo. Los electrones de algunos átomos, como los de los metales, pueden liberarse del átomo y ponerse en movimiento. Este mar de electrones, débilmente unidos a los átomos, es lo que hace que la electricidad sea posible. La electricidad es un flujo libre de electrones.



Los electrones que se agrupan no se mueven porque los campos eléctricos que repelen a los electrones alcanzan el equilibrio. El resultado es una fuerza eléctrica neta de valor cero.

Figura 4

Se denomina electricidad estática a los electrones libres que permanecen en un lugar, sin moverse y con una carga negativa. ⁴ Si estos electrones estáticos tienen la oportunidad de saltar hacia un conductor, se

puede producir una descarga electrostática (ESD). La explicación sobre los conductores aparece más adelante en este capítulo.

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 del computador, o ambas cosas, de forma aleatoria. Los circuitos lógicos de los chips de los computadores son sumamente sensibles a las descargas electrostáticas. Tenga cuidado al trabajar en el interior de un computador, router u otro dispositivo.

Se puede hacer referencia a los átomos, o a los grupos de átomos denominados moléculas, como materiales. Los materiales pueden clasificarse en tres grupos, según la facilidad con la que la electricidad, o los electrones libres, fluya a través de ellos.

La base de todo dispositivo electrónico es el conocimiento de cómo los aislantes, los conductores y los semiconductores controlan el flujo de los electrones y trabajan juntos en distintas combinaciones.

3.1.2 Voltaje

El voltaje se denomina a veces "fuerza electromotriz" (EMF). La EMF es una fuerza eléctrica o presión que se produce cuando los electrones y protones se separan. La fuerza que se crea va empujando hacia la carga opuesta y en dirección contraria a la de la carga de igual polaridad. Este proceso se produce en una batería, donde la acción química hace que los electrones se liberen de la terminal negativa de la batería. Entonces, los electrones viajan a la terminal opuesta, o positiva, a través de un circuito EXTERNO. Los electrones no viajan a través de la batería en sí. Recuerde que el flujo de electricidad es, en realidad, el flujo de los electrones. También es posible crear voltaje de tres otras formas: La primera es por fricción o electricidad estática. La segunda es por magnetismo o un generador eléctrico. La última forma en que se puede crear voltaje es por medio de la luz o las células solares.

El voltaje está representado por la letra V y, a veces, por la letra E, en el caso de la fuerza electromotriz. La unidad de medida del voltaje es el voltio (V). ¹El voltio es la cantidad de trabajo por unidad de carga necesario para separar las cargas.

- El voltaje se denomina a veces "fuerza electromotriz" (EMF)
 - El voltaje se representa a través de la letra V y a veces a través de la letra E, que corresponde a fuerza electromotriz.
- La unidad de medida del voltaje es el voltio (V)

Figura 1

3.1.3 Resistencia e impedancia

Los materiales a través de los cuales fluye la corriente presentan distintos grados de oposición, o resistencia, al movimiento de los electrones. Los materiales que presentan muy poca o ninguna resistencia se denominan conductores. Aquellos que no permiten que la corriente fluya, o que restringen severamente el flujo, se denominan aislantes. El grado de resistencia depende de la composición química de los materiales.

Todos los materiales que conducen electricidad presentan un cierto grado de resistencia al movimiento de electrones a través de ellos. Estos materiales también tienen otros efectos denominados capacitancia e inductancia, asociados a la corriente de electrones. Las tres características constituyen la impedancia, que es similar a e incluye la resistencia.

El término atenuación es fundamental a la hora de aprender sobre redes. La atenuación se relaciona a la resistencia al flujo de electrones y la razón por la que una señal se degrada a medida que recorre el conducto.

La letra R representa la resistencia. La unidad de medición de la resistencia es el ohmio (Ω). El símbolo proviene de la letra griega " Ω ", omega.

Los aislantes eléctricos, o aislantes, son materiales que no permiten que los electrones fluyan a través de ellos sino con gran dificultad o no lo permiten en absoluto. Ejemplos de aislantes eléctricos son el plástico,

el vidrio, el aire, la madera seca, el papel, el caucho y el gas helio. Estos materiales poseen estructuras químicas sumamente estables, en las que los electrones orbitan fuertemente ligados a los átomos.

Los conductores eléctricos, generalmente llamados simplemente conductores, son materiales que permiten que los electrones fluyan 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.

La tabla periódica clasifica en categorías a algunos grupos de átomos ordenándolos en columnas. Los átomos de cada columna forman familias químicas específicas. Aunque tengan distintas cantidades de protones, neutrones y electrones, sus electrones externos tienen órbitas similares y se comportan de forma similar, al interactuar con otros átomos y moléculas. Los mejores conductores son metales como el cobre (Cu), la plata (Ag) y el oro (Au), porque tienen electrones que se liberan con facilidad. Entre los demás conductores se incluyen la soldadura, una mezcla de plomo (Pb) y estaño (Sn), y el agua ionizada. Un ion es un átomo que tiene una cantidad de electrones que es mayor o menor que la cantidad de protones en el núcleo del átomo. Aproximadamente un 70% del cuerpo humano consta de agua ionizada, lo que significa que el cuerpo humano también es conductor.

Los semiconductores son materiales en los que la cantidad de electricidad que conducen puede ser controlada de forma precisa. Estos materiales se agrupan en una misma columna de la tabla periódica. Entre los ejemplos de estos materiales se incluyen el carbono (C), el germanio (Ge) y la aleación de arseniuro de galio (GaAs). El semiconductor más importante, que permite fabricar los mejores circuitos electrónicos microscópicos, es el silicio (Si).

El silicio es muy común y se puede encontrar en la arena, el vidrio y varios tipos de rocas. La región alrededor de San José, California, se denomina Silicon Valley (Valle del Silicio) porque la industria informática, que depende de los microchips de silicio, se inició en esta área. ¹

Aislantes	Conductores	Semiconductores
Los electrones circulan con dificultad	Los electrones circulan fácilmente	La corriente de electrones se puede controlar con precisión
Plástico Caucho Aire Papel Madera seca Vidrio	Cobre (Cu) Plata (Ag) Oro (Au) Soldadura Agua ionizada Seres humanos	Carbono (C) Germanio (Ge) Arsenio de galio (GaAs) Silicio (Si)

Figura 1

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. ¹ La 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.

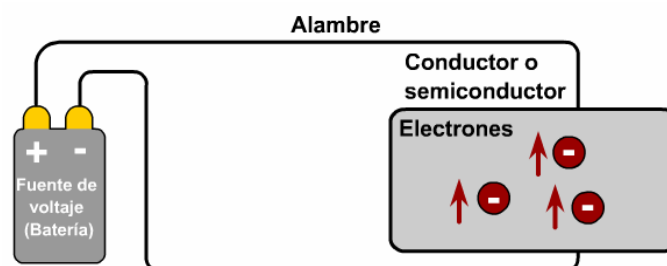


Figura 1

Si se piensa en el amperaje o corriente como la cantidad o volumen de tránsito de electrones que fluyen, entonces, se puede pensar que el voltaje es la velocidad del tránsito de los electrones. La combinación de amperaje y voltaje es equivalente al vatiaje. Los dispositivos eléctricos tales como las ampollitas, los motores y las fuentes de alimentación para computadores se clasifican en términos de vatios. Un vatio es la cantidad de energía que un dispositivo consume o produce.

Es la corriente o el amperaje de un circuito eléctrico la que en realidad hace el trabajo. Por ejemplo, la electricidad estática tiene un voltaje muy alto, tanto que puede saltar una brecha de una pulgada o más. Sin embargo, tiene muy bajo amperaje y, como resultado, puede producir un choque pero no daños permanentes. El motor de arranque de un automóvil opera a tan sólo 12 voltios pero requiere un amperaje muy alto para generar la energía suficiente para hacer que el motor del auto arranque. Un rayo tiene un voltaje muy alto y un amperaje alto y así puede causar graves daños o lesiones.

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. Si la corriente se produce en un circuito de CA, entonces la cantidad de corriente dependerá de la cantidad de impedancia presente. Si la corriente se produce en un circuito de CC, entonces la cantidad de corriente dependerá de la cantidad de resistencia presente. La bomba de agua es como una batería. Suministra presión para que el flujo continúe en movimiento. ¹

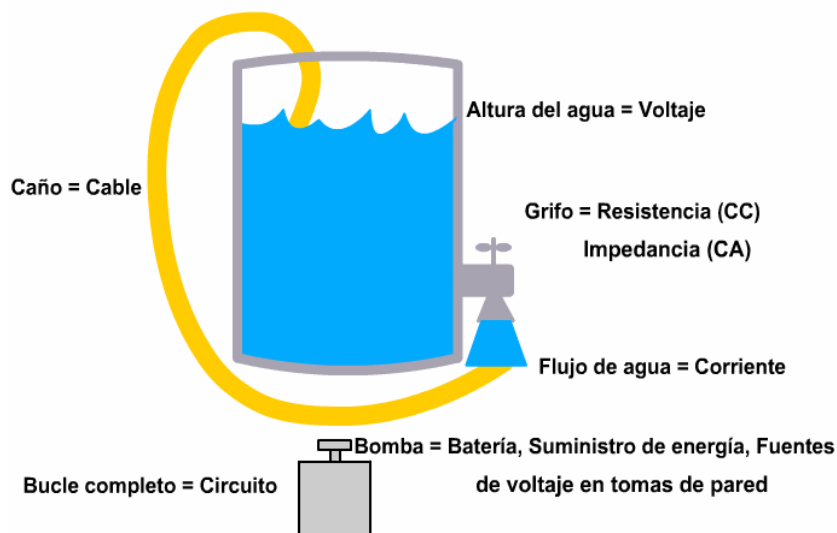


Figura 1

La relación entre el voltaje, la resistencia y la corriente es voltaje (V) = corriente (I) multiplicada por resistencia (R). En otras palabras, $V=I \cdot R$. Esta es la Ley de Ohm, llamada así en honor al científico que investigó estos temas.

Las dos formas en que fluye la corriente son: Corriente Alterna (CA) y Corriente Continua (CC). La corriente alterna (CA) y sus correspondientes voltajes varían con el tiempo, cambiando su polaridad o dirección. La CA fluye en una dirección, luego invierte su dirección y fluye en sentido contrario para luego repetir el proceso. El voltaje de la CA es positivo en una terminal y negativo en otra. Entonces, el voltaje de la CA invierte su polaridad, de modo que la terminal positiva se convierte en negativa y la terminal negativa en positiva. Este proceso se repite de forma continua.

La corriente continua (CC) siempre fluye en la misma dirección, y los voltajes de CC siempre tienen la misma polaridad. Una terminal es siempre positiva y la otra es siempre negativa. Estas direcciones no se modifican ni se invierten.

El osciloscopio es un dispositivo electrónico que se utiliza para medir las señales eléctricas en relación al tiempo. Un osciloscopio expresa las ondas, los pulsos y los patrones eléctricos en forma de gráfico. Tiene un eje "x" que representa el tiempo y un eje "y" que representa el voltaje. ² Generalmente existen dos ejes "y" que corresponden a dos voltajes de entrada para que se puedan observar y medir dos ondas al mismo tiempo.

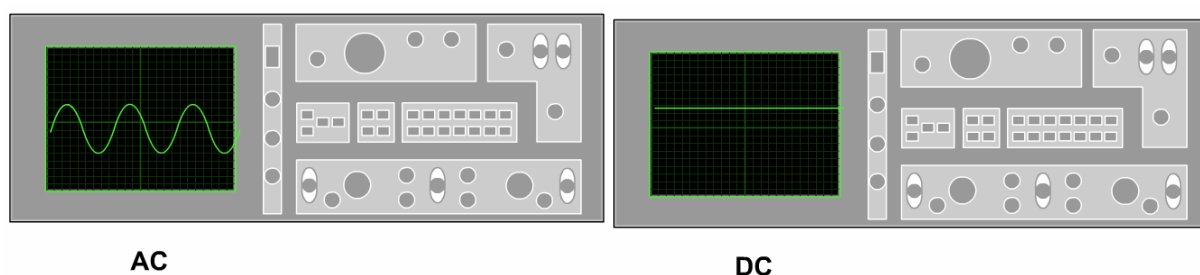


Figura 2

Las líneas de alimentación transportan electricidad en forma de CA porque ésta puede ser conducida por largas distancias, de forma eficiente. La CC se encuentra en las baterías para linternas, baterías de automóviles y como energía para los microchips de la motherboard de un computador, donde sólo necesita recorrer una corta distancia.

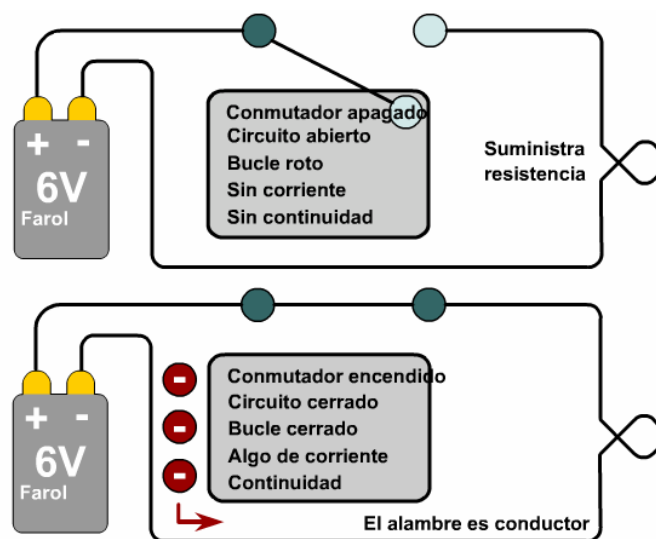


Figura 3

Los electrones fluyen en circuitos cerrados, o bucles completos. La Figura ³ muestra un circuito simple. Los procesos químicos que se producen en la batería causan una acumulación de cargas. Esto proporciona un voltaje o presión eléctrica que permite que los electrones fluyan a través de los distintos dispositivos. 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 4 muestra parte de un circuito eléctrico que lleva energía a un hogar u oficina.

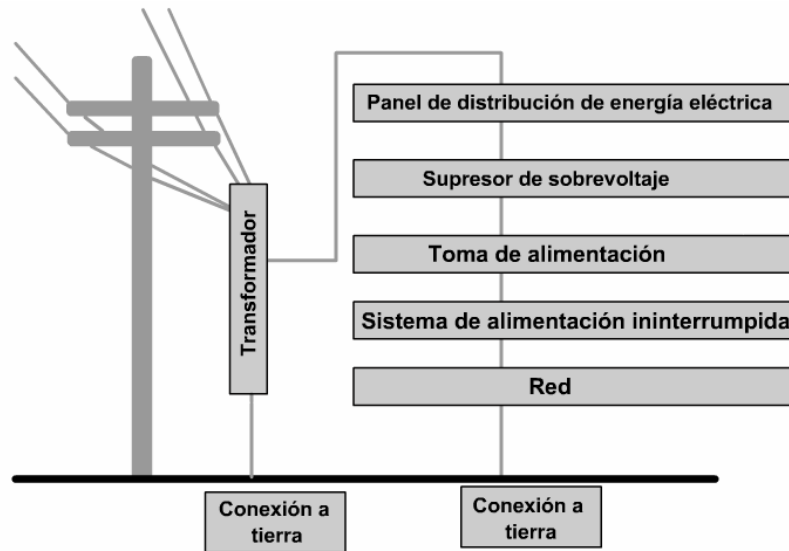
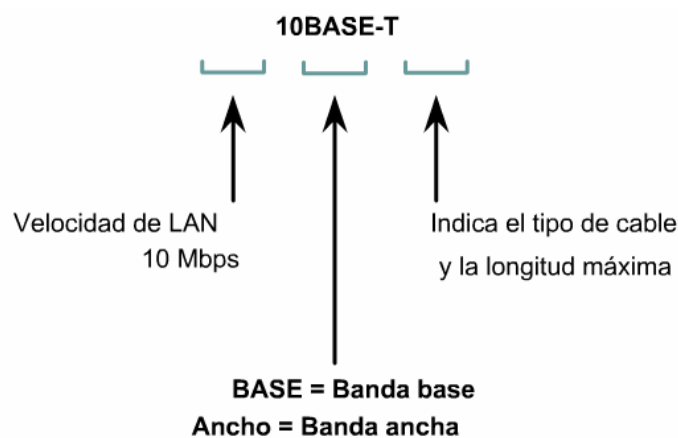


Figura 4

3.1.6 Especificaciones de cables

Los cables tienen distintas especificaciones y generan distintas expectativas acerca de su rendimiento.

- ¿Qué velocidad de transmisión de datos se puede lograr con un tipo particular de cable? La velocidad de transmisión de bits por el cable es de suma importancia. El tipo de conducto utilizado afecta la velocidad de la transmisión.
- ¿Qué tipo de transmisión se planea? ¿Serán las transmisiones digitales o tendrán base analógica? La transmisión digital o de banda base y la transmisión con base analógica o de banda ancha son las dos opciones.
- ¿Qué distancia puede recorrer una señal a través de un tipo de cable en particular antes de que la atenuación de dicha señal se convierta en un problema? En otras palabras, ¿se degrada tanto la señal que el dispositivo receptor no puede recibir e interpretar la señal correctamente en el momento en que la señal llega a dicho dispositivo? La distancia recorrida por la señal a través del cable afecta directamente la atenuación de la señal. La degradación de la señal está directamente relacionada con la distancia que recorre la señal y el tipo de cable que se utiliza.



Algunos ejemplos de las especificaciones de Ethernet que están relacionadas con el tipo de cable son:

- 10BASE-T
- 10BASE5
- 10BASE2

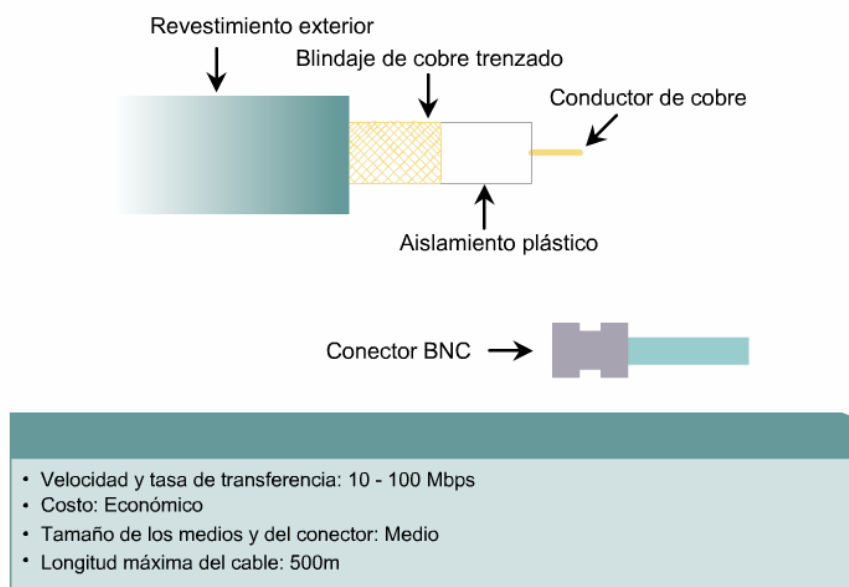
10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.

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. 10BASE5 a menudo se denomina "Thicknet". Thicknet es, en realidad, un tipo de red, mientras que 10BASE5 es el cableado que se utiliza en dicha red.

10BASE2 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 2, en 10BASE2, se refiere a la longitud máxima aproximada del segmento de 200 metros antes que la atenuación perjudique la habilidad del receptor para interpretar apropiadamente la señal que se recibe. La longitud máxima del segmento es en realidad 185 metros. 10BASE2 a menudo se denomina "Thinnet". Thinnet es, en realidad, un tipo de red, mientras que 10BASE2 es el cableado que se utiliza en dicha red.

3.1.7 Cable coaxial

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



Para las LAN, el cable coaxial ofrece varias ventajas. Puede tenderse a mayores distancias que el cable de par trenzado blindado STP, y que el cable de par trenzado no blindado, UTP, sin necesidad de repetidores. Los repetidores regeneran las señales de la red de modo que puedan abarcar mayores distancias. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos, incluida la televisión por cable.

Al trabajar con cables, es importante tener en cuenta su tamaño. A medida que aumenta el grosor, o diámetro, del cable, resulta más difícil trabajar con él. 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.

En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para las instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación de thinnet era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet (red barata). El trenzado externo metálico o de cobre del cable coaxial abarca la mitad del circuito eléctrico. Se debe tener especial cuidado de asegurar una sólida conexión eléctrica en ambos extremos, brindando así una correcta conexión a tierra. La incorrecta conexión del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial. Los problemas de conexión resultan en un ruido eléctrico que interfiere con la transmisión de señales sobre los medios de networking. Por esta razón, thinnet ya no se usa con frecuencia ni está respaldado por los estándares más recientes (100 Mbps y superiores) para redes Ethernet.

3.1.8 Cable STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. **1**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.

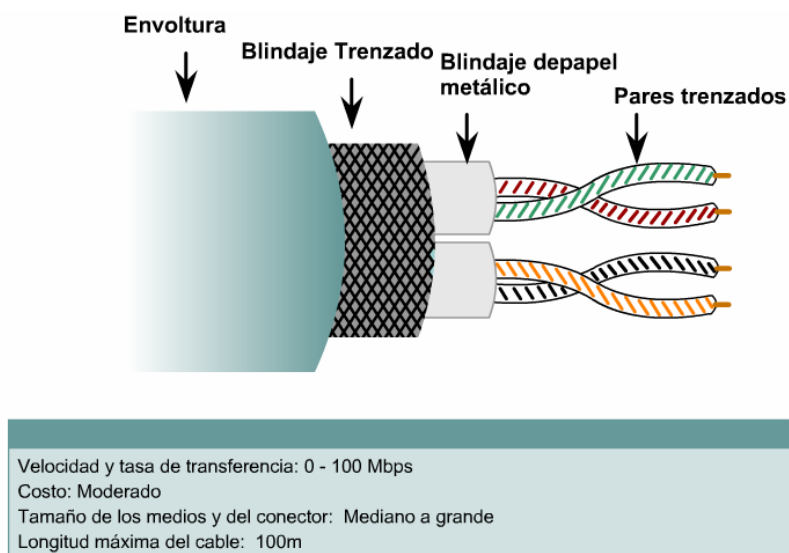


Figura 1

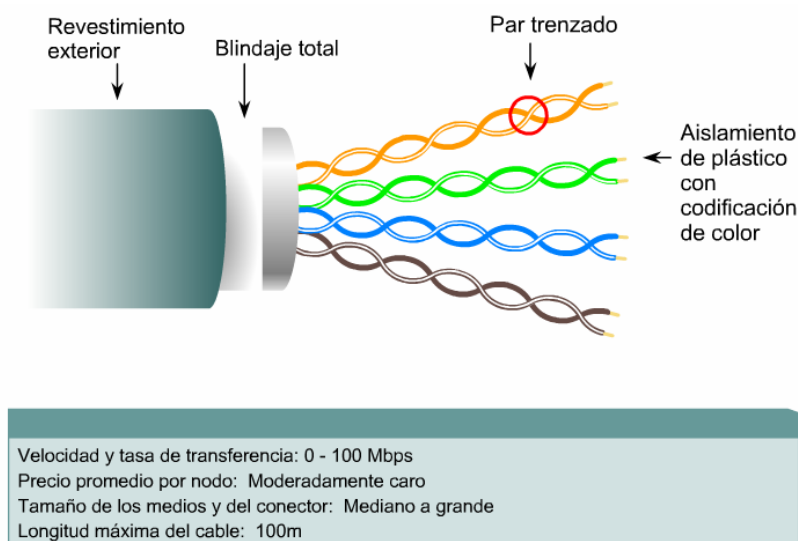


Figura 2

Un nuevo híbrido de UTP con STP tradicional se denomina UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El ScTP consiste, básicamente, en cable UTP envuelto en un blindaje de papel metálico. ScTP, como UTP, es también un cable de 100 Ohms. Muchos fabricantes e instaladores de cables pueden usar el término STP para describir el cable ScTP. Es importante entender que la mayoría de las referencias hechas a STP hoy en día se refieren en realidad a un cable de cuatro pares apantallado. Es muy improbable que un verdadero cable STP sea usado durante un trabajo de instalación de cable.

Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están adecuadamente conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP y el ScTP se pueden volver susceptibles a graves problemas de ruido. Son susceptibles porque permiten que el blindaje actúe como una antena que recoge las señales no deseadas. Sin embargo, este efecto funciona en ambos sentidos. El blindaje no sólo evita que ondas electromagnéticas externas produzcan ruido en los cables de datos sino que también minimiza la irradiación de las ondas electromagnéticas internas. Estas ondas podrían producir ruido en otros dispositivos. Los cables STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios de networking (tales como el cable coaxial y la fibra óptica) sin que se repita la señal. El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable. Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra. Sin embargo, el STP y el ScTP todavía desempeñan un papel importante, especialmente en Europa o en instalaciones donde exista mucha EMI y RFI cerca de los cables.

3.1.9 Cable UTP

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

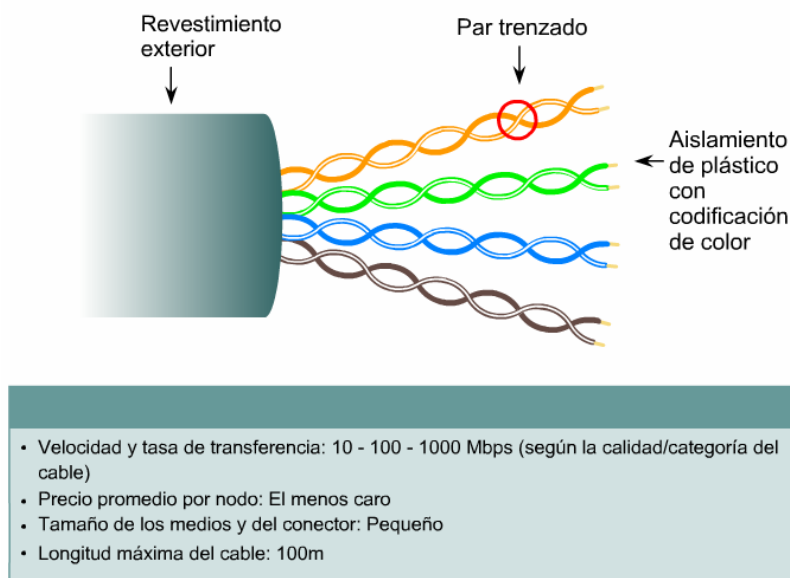


Figura 1

El estándar TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas, y los procedimientos de medición necesarios para verificar los cables de par trenzado balanceado. Exige el tendido de dos cables, uno para voz y otro para datos en cada toma. De los dos cables, el cable de voz debe ser UTP de cuatro pares. El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones. Sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red. El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la Categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

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

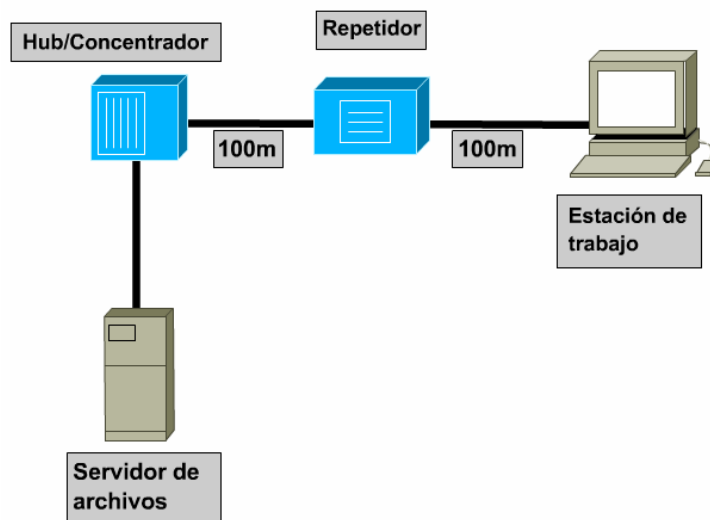


Figura 2

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, un switch de LAN se conecta a un computador. El cable que se conecta desde el puerto del switch al puerto de la NIC del computador recibe el nombre de cable directo. 4

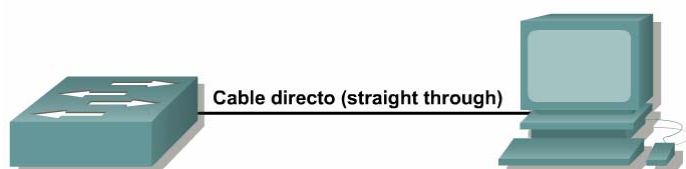


Figura 3

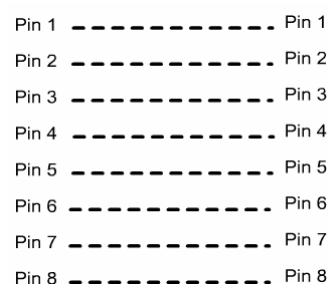


Figura 4

En la Figura 5, dos switch aparecen conectados entre sí. El cable que conecta un puerto de un switch al puerto de otro switch recibe el nombre de cable de conexión cruzada. 6

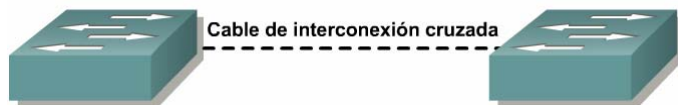


Figura 5

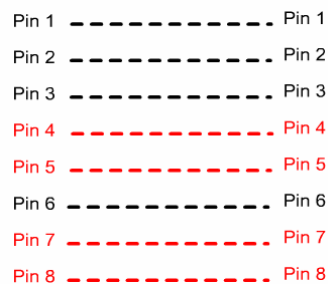
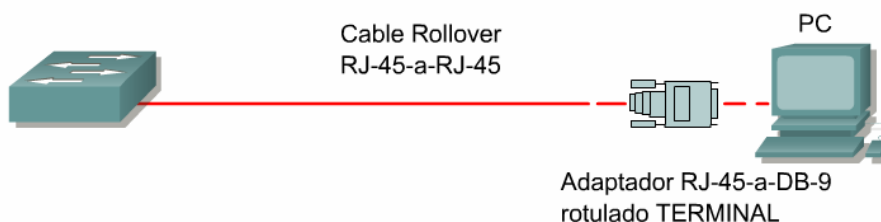


Figura 6

En la Figura 7, el cable que conecta el adaptador de RJ-45 del puerto COM del computador al puerto de la consola del router o switch recibe el nombre de cable rollover.

Dispositivo con consola



- Las PC requieren un adaptador de RJ-45 a DB-9 o RJ-45 a DB-25.
- Las configuraciones de puerto COM son 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, sin control de flujo.
- Esto proporciona acceso de consola fuera de banda.
- El puerto de switch AUX se puede usar para una consola conectada por módem.

Figura 7

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 pines nº 1 y nº 2 aparecerán en el otro extremo en los pines nº 3 y nº 6, y viceversa. Esto ocurre porque los pines 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. 8

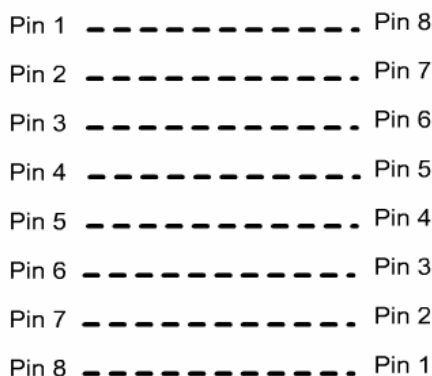


Figura 8

3.2 Medios de fibra óptica

3.2.1 El espectro electromagnético

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. ¹

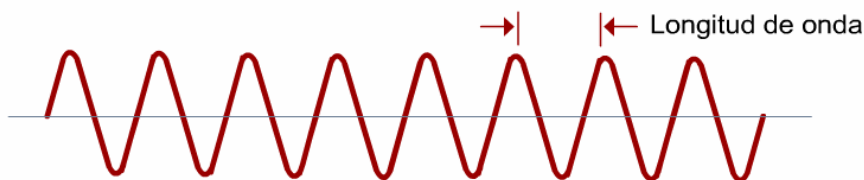


Figura 1

La radio, las microondas, el radar, la luz visible, los rayos x y los rayos gama parecen ser todos muy diferentes. Sin embargo, todos ellos son tipos de energía electromagnética. Si se ordenan todos los tipos de ondas electromagnéticas desde la mayor longitud de onda hasta la menor, se crea un continuo denominado espectro electromagnético.

La longitud de onda de una onda electromagnética es determinada por la frecuencia a la que la carga eléctrica que genera la onda se mueve hacia adelante y hacia atrás. Si la carga se mueve lentamente hacia adelante y hacia atrás, la longitud de onda que genera es una longitud de onda larga. Visualice el movimiento de la carga eléctrica como si fuera una varilla en una charca. Si la varilla se mueve lentamente hacia adelante y hacia atrás, generará movimientos en el agua con una longitud de onda larga entre las partes superiores de las ondas. Si la varilla se mueve rápidamente hacia adelante y hacia atrás, los movimientos en el agua tendrán una longitud de onda mas corta.

Como todas las ondas electromagnéticas se generan de la misma manera, comparten muchas propiedades. Todas las ondas viajan a la misma velocidad en el vacío. La velocidad es aproximadamente 300.000 kilómetros por segundo o 186.283 millas por segundo. Esta es también la velocidad de la luz.

Los ojos humanos están diseñados para percibir solamente la energía electromagnética de longitudes de onda de entre 700 y 400 nanómetros (nm). Un nanómetro es la mil millonésima parte de un metro (0,000000001 metro) de longitud. La energía electromagnética con longitudes de onda entre 700 y 400 nm recibe el nombre de luz visible. Las longitudes de onda de luz más largas que se encuentran cerca de los 700 nm se perciben como el color rojo. Las longitudes de onda más cortas que se encuentran alrededor de los 400 nm aparecen como el color violeta. Esta parte del espectro magnético se percibe como los colores del arco iris. ²

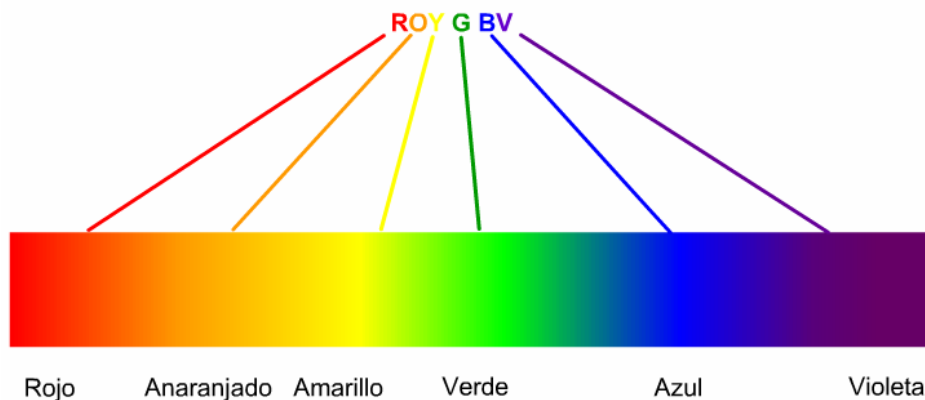


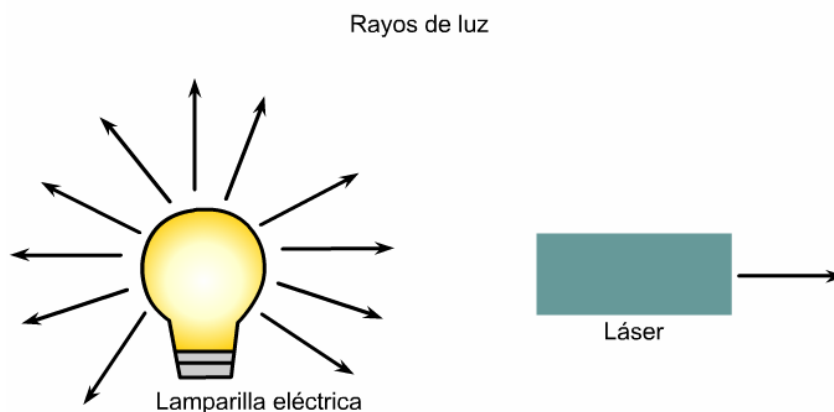
Figura 2

Las longitudes de onda que invisibles al ojo humano son utilizadas para transmitir datos a través de una fibra óptica. Estas longitudes de onda son levemente más larga que las de la luz roja y reciben el nombre de luz infrarroja. La luz infrarroja se utiliza en los controles remotos de los televisores. La longitud de onda de la

luz en la fibra óptica es de 850 nm, 1310 nm o 1550 nm. Se seleccionaron estas longitudes de onda porque pasan por la fibra óptica más fácilmente que otras.

3.2.2 Modelo de rayo de luz

Cuando las ondas electromagnéticas se alejan de una fuente, viajan en líneas rectas. Estas líneas rectas que salen de la fuente reciben el nombre de rayos. ¹Piense en los rayos de luz como delgados haces de luz similares a los generados por un láser. En el vacío del espacio, la luz viaja de forma continua en línea recta a 300.000 kilómetros por segundo. Sin embargo, la luz viaja a velocidades diferentes y más lentas a través de otros materiales como el aire, el agua y el vidrio. Cuando un rayo de luz, denominado rayo incidente, cruza los límites de un material a otro, se refleja parte de la energía de la luz del rayo. Por esta razón, uno puede verse a sí mismo en el vidrio de una ventana. La luz reflejada recibe el nombre de rayo reflejado.



$$\text{Índice de refracción} = n = \frac{\text{Velocidad de la luz en el vacío}}{\text{Velocidad de la luz en material}}$$

Figura 1

La energía de la luz de un rayo incidente que no se refleja entra en el vidrio. El rayo entrante se dobla en ángulo desviándose de su trayecto original. Este rayo recibe el nombre de rayo refractado. El grado en que se dobla el rayo de luz incidente depende del ángulo que forma el rayo incidente al llegar a la superficie del vidrio y de las distintas velocidades a la que la luz viaja a través de las dos sustancias.

Esta desviación de los rayos de luz en los límites de dos sustancias es la razón por la que los rayos de luz pueden recorrer una fibra óptica aun cuando la fibra tome la forma de un círculo.

La densidad óptica del vidrio determina la desviación de los rayos de luz en el vidrio. La densidad óptica se refiere a cuánto la velocidad del rayo de luz disminuye al atravesar una sustancia. Cuanto mayor es la densidad óptica del material, más se desacelera la luz en relación a su velocidad en el vacío. El índice de refracción se define como la velocidad de la luz en el vacío dividido por la velocidad de la luz en el medio. Por lo tanto, la medida de la densidad óptica de un material es el índice de refracción de ese material. Un material con un alto índice de refracción es ópticamente más denso y desacelera más la luz que un material con menor índice de refracción. ²

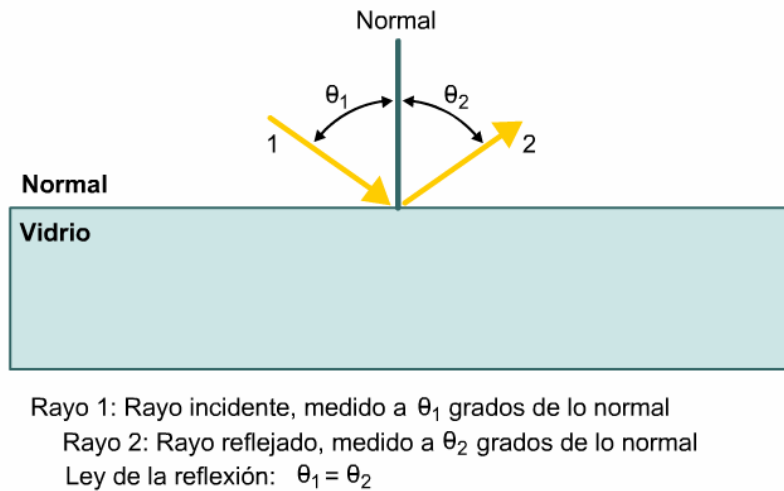
Sustancia	Índice de refracción
Aire	1.000
Vidrio	1.523
Diamante	2.419
Agua	1.333

Figura 2

En una sustancia como el vidrio, es posible aumentar el Índice de Refracción o densidad óptica, agregando productos químicos al vidrio. Si se produce un vidrio muy puro, se puede reducir el índice de refracción. Las siguientes lecciones proporcionan mayor información sobre la reflexión y la refracción y su relación con el diseño y funcionamiento de la fibra óptica.

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. ¹El 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. ²



La luz que viaja a través del aire se refleja en la superficie del vidrio.

Figura 1

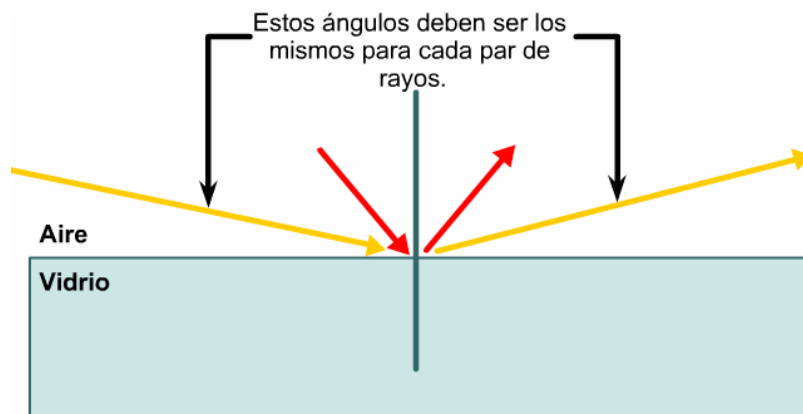


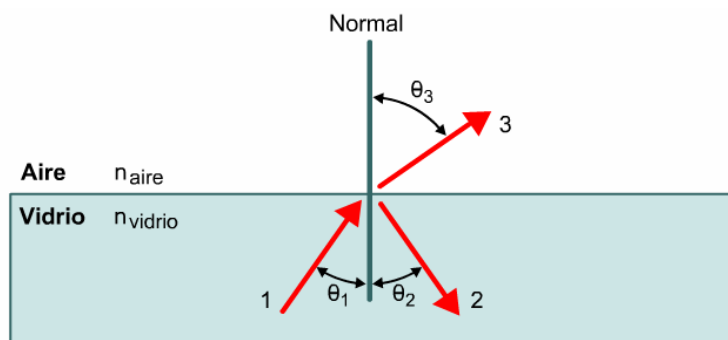
Figura 2

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.

Si el rayo incidente golpea la superficie del vidrio a un ángulo exacto de 90 grados, el rayo entra directamente al vidrio. El rayo no se desvía. Por otro lado, si el rayo incidente no golpea la superficie con un ángulo exacto de 90 grados respecto de la superficie, entonces, el rayo transmitido que entra al vidrio se desvía. La desviación del rayo entrante recibe el nombre de refracción. El grado de refracción del rayo depende del índice de refracción de los dos materiales transparentes. Si el rayo de luz parte de una sustancia cuyo índice de refracción es menor, entrando a una sustancia cuyo índice de refracción es mayor, el rayo refractado se desvía hacia la normal. Si el rayo de luz parte de una sustancia cuyo índice de

refracción es mayor, entrando a una sustancia cuyo índice de refracción es menor, el rayo refractado se desvía en sentido contrario de la normal. ¹



Rayo 1: Rayo incidente

Rayo 2: Rayo reflejado

Rayo 3: Rayo refractado

Ley de la reflexión: $\theta_1 = \theta_2$

Ley de la refracción: como $n_{\text{glass}} > n_{\text{aire}}$, $\theta_3 > \theta_1$

Figura 1

Considere un rayo de luz que pasa con un ángulo que no es de 90 grados por el límite entre un vidrio y un diamante. ² El vidrio tiene un índice de refracción de aproximadamente 1,523. El diamante tiene un índice de refracción de aproximadamente 2,419. Por lo tanto, el rayo que continúa su trayecto por el diamante se desviará hacia la normal. Cuando ese rayo de luz cruce el límite entre el diamante y el aire con un ángulo que no sea de 90 grados, se desviará alejándose de la normal. La razón es que el aire tiene un índice de refracción menor, aproximadamente 1,000, que el índice de refracción del diamante.

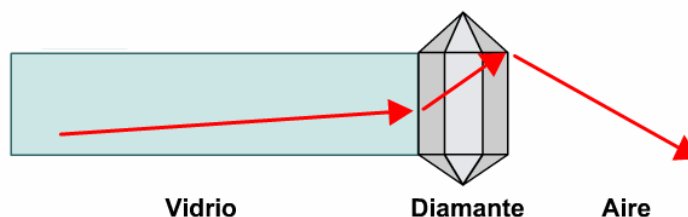


Figura 2

3.2.5 Reflexión interna total

Un rayo de luz que se enciende y apaga para enviar datos (unos y ceros) dentro de una fibra óptica debe permanecer dentro de la fibra hasta que llegue al otro extremo. El rayo no debe refractarse en el material que envuelve el exterior de la fibra. La refracción produciría una pérdida de una parte de la energía de la luz del rayo. Es necesario lograr un diseño de fibra en el que la superficie externa de la fibra actúe como espejo para el rayo de luz que viaja a través de la fibra. Si un rayo de luz que trata de salir por el costado de la fibra se refleja hacia dentro de la fibra a un ángulo tal que lo envíe hacia el otro extremo de la misma, se formaría un buen "conducto" o "guía de ondas" para las ondas de luz. ¹

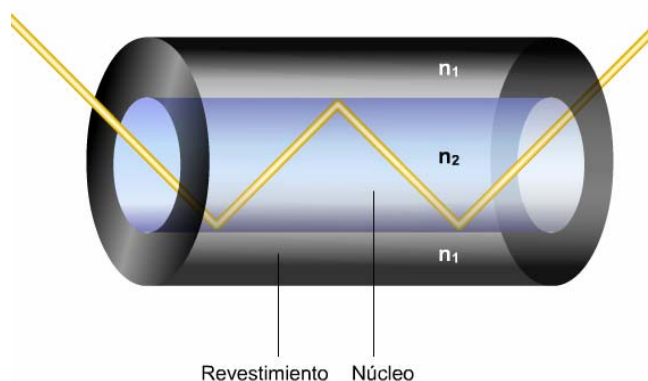


Figura 1

Las leyes de reflexión y de refracción ilustran cómo diseñar una fibra que guíe las ondas de luz a través de la fibra con una mínima pérdida de energía. Se deben cumplir las dos siguientes condiciones para que un rayo de luz en una fibra se refleje dentro de ella sin ninguna pérdida por refracción.

- El núcleo de la fibra óptica debe tener un índice de refracción (n) mayor que el del material que lo envuelve. El material que envuelve al núcleo de la fibra recibe el nombre de revestimiento.
- El ángulo de incidencia del rayo de luz es mayor que el ángulo crítico para el núcleo y su revestimiento. ²

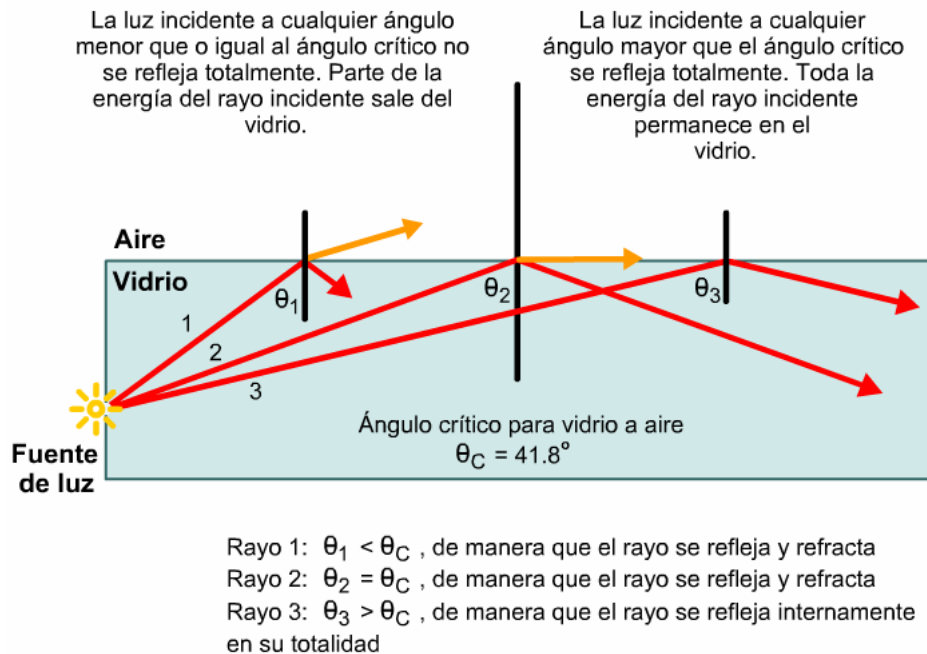


Figura 2

Cuando se cumplen estas dos condiciones, toda la luz que incide en la fibra se refleja dentro de ella. Esto se llama reflexión interna total, que es la base sobre la que se construye una fibra óptica. La reflexión interna total hace que los rayos de luz dentro de la fibra reboten en el límite entre el núcleo y el revestimiento y que continúen su recorrido hacia el otro extremo de la fibra. La luz sigue un trayecto en zigzag a lo largo del núcleo de la fibra.

Resulta fácil crear una fibra que cumpla con esta primera condición. Además, el ángulo de incidencia de los rayos de luz que entran al núcleo puede ser controlado. La restricción de los siguientes dos factores permite controlar el ángulo de incidencia:

- **La apertura numérica de la fibra:** La apertura numérica del núcleo es el rango de ángulos de los rayos de luz incidente que ingresan a la fibra y que son reflejados en su totalidad.
- **Modos:** Los trayectos que puede recorrer un rayo de luz cuando viaja por la fibra. ³ ⁴

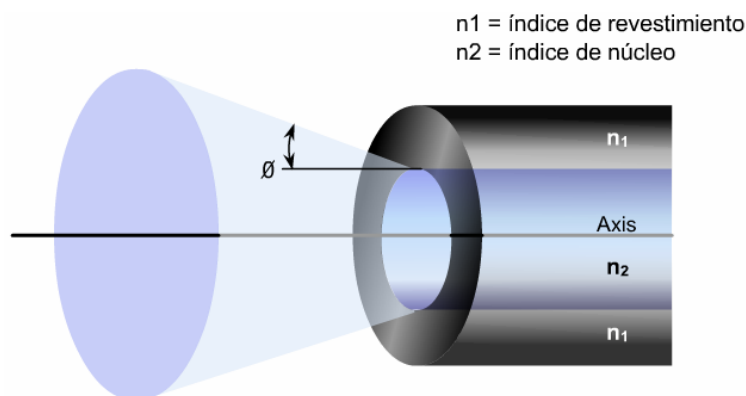


Figura 3

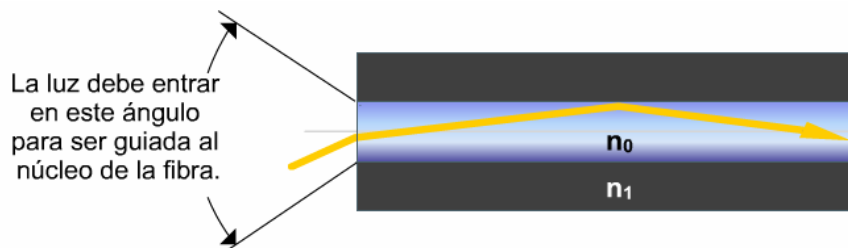


Figura 4

Al controlar ambas condiciones, el tendido de la fibra tendrá reflexión interna total. Esto sirve de guía a la onda de luz que puede ser utilizada para las comunicaciones de datos.

3.2.6 Fibra multimodo

La parte de una fibra óptica por la que viajan los rayos de luz recibe el nombre de núcleo de la fibra. ¹ Los rayos de luz sólo pueden ingresar al núcleo si el ángulo está comprendido en la apertura numérica de la fibra. Asimismo, una vez que los rayos han ingresado al núcleo de la fibra, hay un número limitado de recorridos ópticos que puede seguir un rayo de luz a través de la fibra. Estos recorridos ópticos reciben el nombre de modos. Si el diámetro del núcleo de la fibra es lo suficientemente grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, esta fibra recibe el nombre de fibra "multimodo". La fibra monomodo tiene un núcleo mucho más pequeño que permite que los rayos de luz viajen a través de la fibra por un solo modo. ^{2 3}

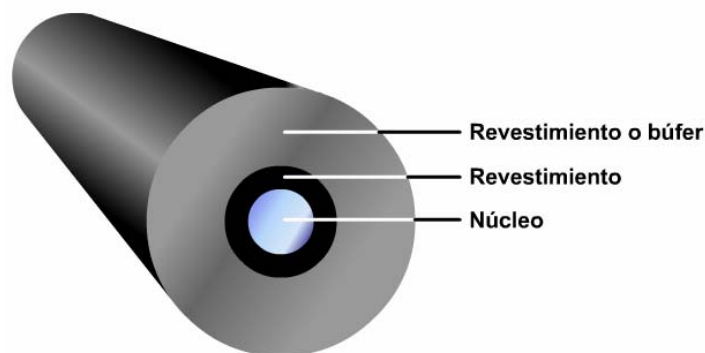


Figura 1

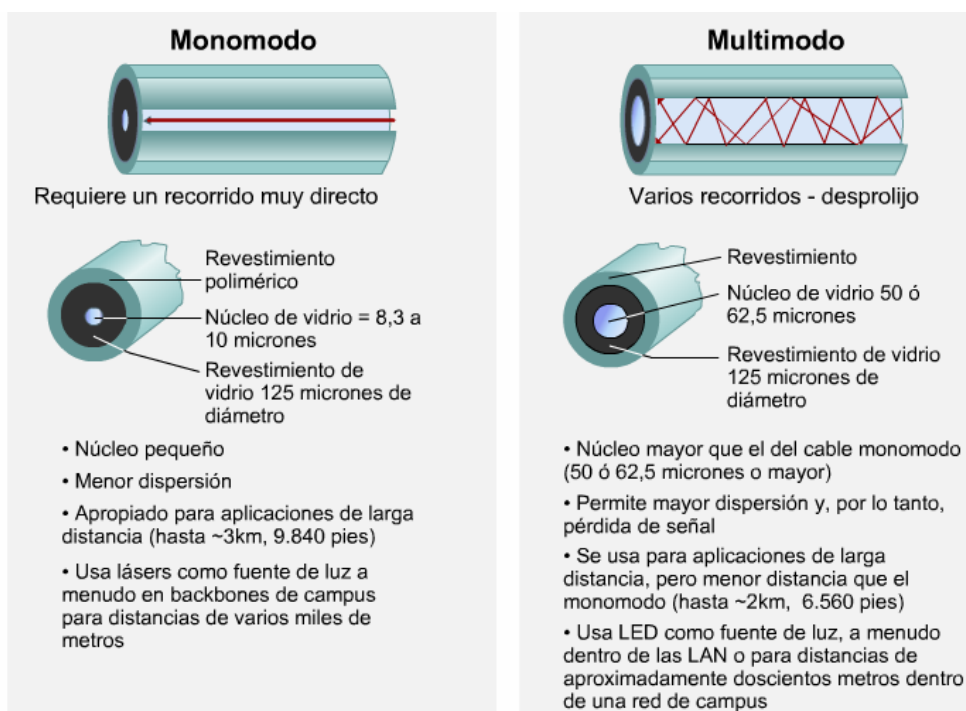


Figura 2

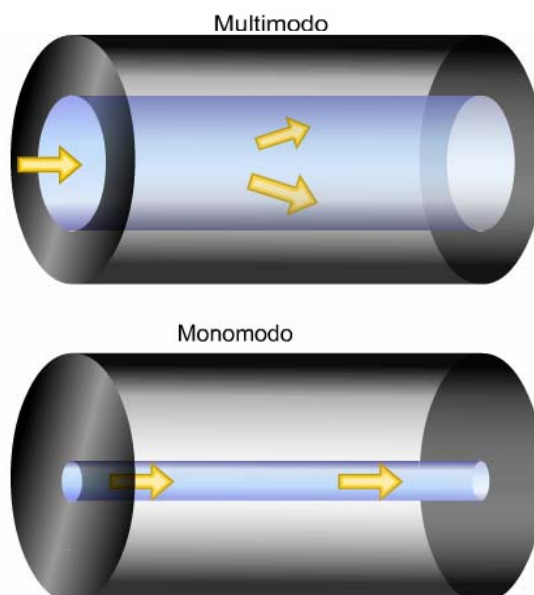


Figura 3

Cada cable de fibra óptica que se usa en networking está compuesto de dos fibras de vidrio envueltas en revestimientos separados. Una fibra transporta los datos transmitidos desde un dispositivo A a un dispositivo B. ⁴La otra transporta los datos desde el dispositivo B hacia el dispositivo A. Las fibras son similares a dos calles de un solo sentido que corren en sentido opuesto. Esto proporciona una comunicación full-duplex. El par trenzado de cobre utiliza un par de hilos para transmitir y un par de hilos para recibir. Los circuitos de fibra óptica usan una hebra de fibra para transmitir y una para recibir.. En general, estos dos cables de fibra se encuentran en un solo revestimiento exterior hasta que llegan al punto en el que se colocan los conectores. ⁵



Figura 4



Figura 5

Hasta que se colocan los conectores, no es necesario blindar ya que la luz no se escapa del interior de una fibra. Esto significa que no hay problemas de diafonía con la fibra óptica. Es común ver varios pares de fibras envueltas en un mismo cable. Esto permite que un solo cable se extienda entre armarios de datos, pisos o edificios. Un solo cable puede contener de 2 a 48 o más fibras separadas. En el caso del cobre, sería necesario tender un cable UTP para cada circuito. La fibra puede transportar muchos más bits por segundo y llevarlos a distancias mayores que el cobre.

En general, un cable de fibra óptica se compone de cinco partes. Estas partes son: el núcleo, el revestimiento, un amortiguador, un material resistente y un revestimiento exterior. ⁶

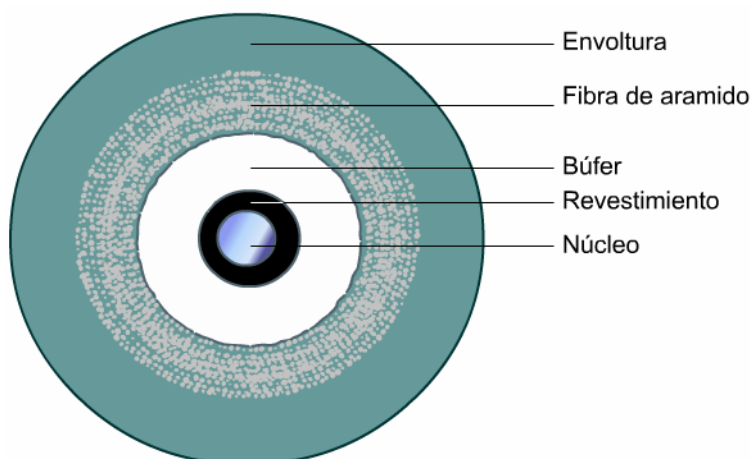


Figura 6

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. La fibra multimodo usa un tipo de vidrio denominado vidrio de índice graduado para su núcleo. Este vidrio tiene un índice de refracción menor hacia el borde externo del núcleo. De esta manera, el área externa del núcleo es ópticamente menos densa que el centro y la luz puede viajar más rápidamente en la parte externa del núcleo. Se utiliza este diseño porque un rayo de luz que sigue un modo que pasa directamente por el centro del núcleo no viaja tanto como un rayo que sigue un modo que rebota en la fibra. Todos los rayos deberían llegar al extremo opuesto de la fibra al mismo tiempo. Entonces, el receptor que se encuentra en el extremo de la fibra, recibe un fuerte flash de luz y no un pulso largo y débil.

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

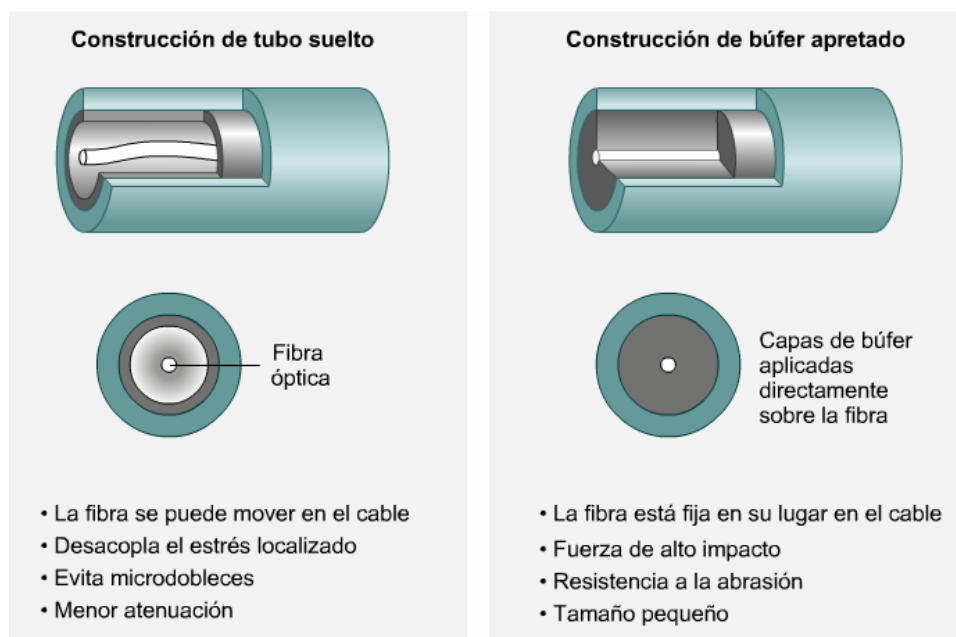


Figura 7

Alrededor del revestimiento se encuentra un material amortiguador que es generalmente de plástico. El material amortiguador ayuda a proteger al núcleo y al revestimiento de cualquier daño. Existen dos diseños básicos para cable. Son los diseños de cable de amortiguación estrecha y de tubo libre. La mayoría de las fibras utilizadas en las redes LAN son de cable multimodo con amortiguación estrecha. Los cables con

amortiguación estrecha tienen material amortiguador que rodea y está en contacto directo con el revestimiento. La diferencia más práctica entre los dos diseños está en su aplicación. El cable de tubo suelto se utiliza principalmente para instalaciones en el exterior de los edificios mientras que el cable de amortiguación estrecha se utiliza en el interior de los edificios.

El material resistente rodea al amortiguador, evitando que el cable de fibra óptica se estire cuando los encargados de la instalación tiran de él. El material utilizado es, en general, Kevlar, el mismo material que se utiliza para fabricar los chalecos a prueba de bala.

El último elemento es el revestimiento exterior. El revestimiento exterior rodea al cable para así proteger la fibra de abrasión, solventes y demás contaminantes. El color del revestimiento exterior de la fibra multimodo es, en general, anaranjado, pero a veces es de otro color.

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

3.2.7 Fibra monomodo

La fibra monomodo consta de las mismas partes que una multimodo. El revestimiento exterior de la fibra monomodo es, en general, de color amarillo. La mayor diferencia entre la fibra monomodo y la multimodo es que la monomodo permite que un solo modo de luz se propague a través del núcleo de menor diámetro de la fibra óptica. El núcleo de una fibra monomodo tiene de ocho a diez micrones de diámetro. Los más comunes son los núcleos de nueve micrones.

La marca 9/125 que aparece en el revestimiento de la fibra monomodo indica que el núcleo de la fibra tiene un diámetro de 9 micrones y que el revestimiento que lo envuelve tiene 125 micrones de diámetro.

En una fibra monomodo se utiliza un láser infrarrojo como fuente de luz. El rayo de luz que el láser genera, ingresa al núcleo en un ángulo de 90 grados.

Como consecuencia, los rayos de luz que transportan datos en una fibra monomodo son básicamente transmitidos en línea recta directamente por el centro del núcleo. ¹

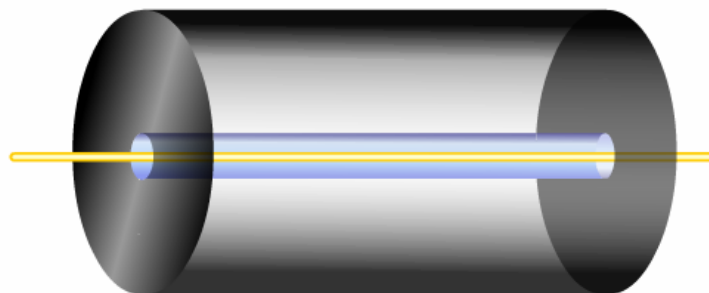


Figura 1

Esto aumenta, en gran medida, tanto la velocidad como la distancia a la que se pueden transmitir los datos. Por su diseño, la fibra monomodo puede transmitir datos a mayores velocidades (ancho de banda) y recorrer mayores distancias de tendido de cable que la fibra multimodo. La fibra monomodo puede transportar datos de LAN a una distancia de hasta 3000 metros. Aunque esta distancia se considera un estándar, nuevas tecnologías han incrementado esta distancia y serán discutidas en un módulo posterior. La fibra multimodo sólo puede transportar datos hasta una distancia de 2000 metros. Las fibras monomodo y el láser son más costosos que los LED y la fibra multimodo. Debido a estas características, la fibra monomodo es la que se usa con mayor frecuencia para la conectividad entre edificios.

ADVERTENCIA:

La luz de láser que se utiliza con la fibra monomodo tiene una longitud de onda mayor que la de la luz visible. El láser es tan poderoso que puede causar graves daños a la vista. **Nunca** mire directamente al interior del extremo de una fibra conectada a un dispositivo en su otro extremo. **Nunca** mire directamente

hacia el interior del puerto de transmisión en una NIC, switch o router. Recuerde mantener las cubiertas protectoras en los extremos de la fibra e insertarlos en los puertos de fibra óptica de switches y routers. Tenga mucho cuidado.

La Figura 2 compara los tamaños relativos del núcleo y el revestimiento para ambos tipos de fibra óptica en distintos cortes transversales. Como la fibra monomodo tiene un núcleo más refinado y de diámetro mucho menor, tiene mayor ancho de banda y distancia de tendido de cable que la fibra multimodo. Sin embargo, tiene mayores costos de fabricación.

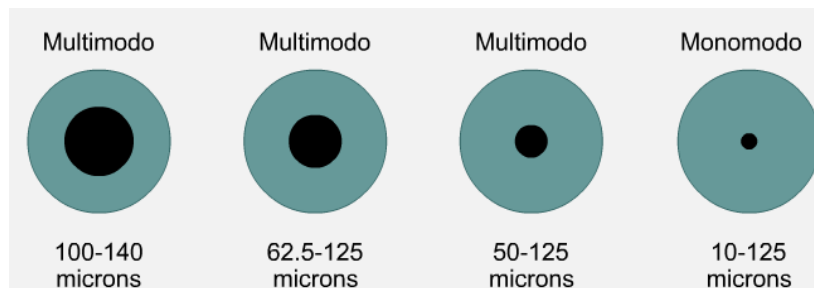


Figura 2

3.2.8 Otros componentes ópticos

La mayoría de los datos que se envían por una LAN se envían en forma de señales eléctricas. Sin embargo, los enlaces de fibra óptica utilizan luz para enviar datos. Hace falta algún elemento para convertir la electricidad en luz y, en el otro extremo de la fibra, para convertir la luz nuevamente en electricidad. Esto significa que se requiere un transmisor y un receptor. 1

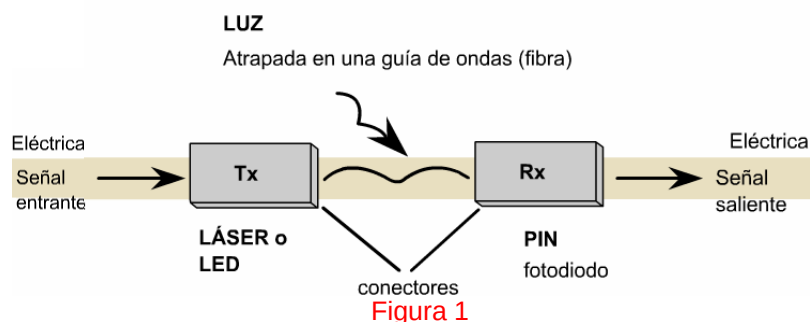


Figura 1

El transmisor recibe los datos que se deben transmitir desde los switches y routers. Estos datos tienen forma de señales eléctricas. El transmisor convierte las señales electrónicas en pulsos de luz equivalentes. Existen dos tipos de fuentes de luz que se utilizan para codificar y transmitir los datos a través del cable:

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

Cada una de estas fuentes de luz puede ser encendida y apagada muy rápidamente para así enviar datos (unos y ceros) a un elevado número de bits por segundo.

En el otro extremo de la fibra óptica conectada al transmisor se encuentra el receptor. El receptor funciona casi como una célula fotoeléctrica en una calculadora a energía solar. Cuando la luz llega al receptor, se genera electricidad. La primera tarea del receptor es detectar el pulso de luz que llega desde la fibra. Luego, el receptor convierte el pulso de luz nuevamente en la señal eléctrica original tal como ingresó al transmisor al otro extremo de la fibra. Ahora, la señal nuevamente adquiere la forma de cambios de voltaje. La señal está lista para ser enviada por el cable de cobre al dispositivo electrónico receptor, como por ejemplo, un computador, switch o router. Los dispositivos semiconductores que se utilizan generalmente como receptores con enlaces de fibra óptica reciben el nombre de diodos p-intrínsecos-n (fotodiodos PIN).

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

Hay conectores unidos a los extremos de las fibras de modo que éstas puedan estar conectadas a los puertos del transmisor y del receptor. El tipo de conector que se usa con mayor frecuencia con la fibra multimodo es el Conector Suscriptor (conector SC). En una fibra monomodo, el conector de Punta Recta (ST) es el más frecuentemente utilizado. [2](#) [3](#)

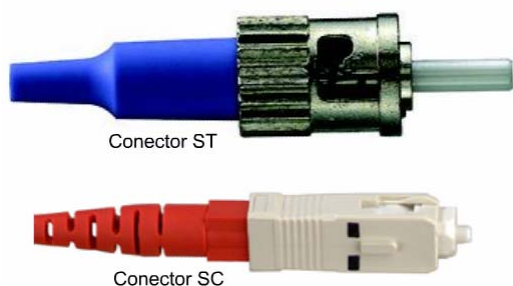


Figura 2



Figura 3

Además de los transmisores, receptores, conectores y fibras que siempre son necesarios en una red óptica, a menudo también se ven repetidores y paneles de conexión de fibra.

Los repetidores son amplificadores ópticos que reciben pulsos de luz atenuante que recorren largas distancias y los convierte a su forma, fuerza y sincronización originales. Las señales restauradas pueden entonces enviarse hasta el receptor que se encuentra en el extremo final de la fibra.

Los paneles de conexión de fibra son similares a los paneles de conexión que se usan con el cable de cobre. Estos paneles aumentan la flexibilidad de una red óptica permitiendo que se realicen rápidos cambios en la conexión de los dispositivos, como por ejemplo, switches o routers con distintos tendidos de fibra o enlaces de cable disponibles. [4](#) [5](#)

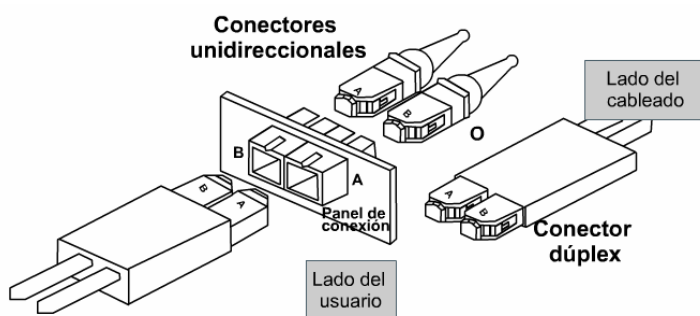


Figura 4

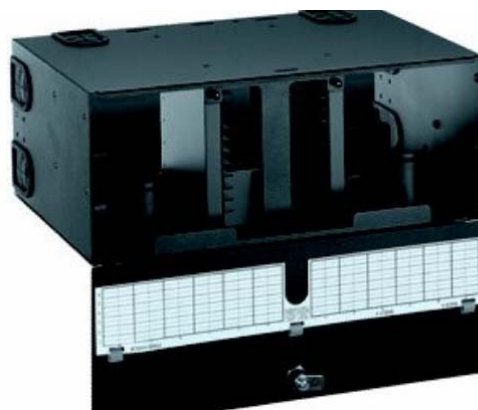


Figura 5

3.2.9 Señales y ruido en las fibras ópticas

El cable de fibra óptica no se ve afectado por las fuentes de ruido externo que causan problemas en los medios de cobre porque la luz externa no puede ingresar a la fibra salvo en el extremo del transmisor. El manto está cubierto por un material amortiguador y una chaqueta exterior que impide que la luz entre o abandone el cable.

Además, la transmisión de la luz en la fibra de un cable no genera interferencia que afecte la transmisión en cualquier otra fibra. Esto significa que la fibra no tiene el problema de diafonía que sí tienen los medios de cobre. De hecho, la calidad de los enlaces de fibra óptica es tan buena que los estándares recientes para Gigabit y 10 Gigabit Ethernet establecen distancias de transmisión que superan de lejos el tradicional

alcance de 2 kilómetros de la Ethernet original. La transmisión por fibra óptica permite que se utilice el protocolo de Ethernet en las Redes de Área Metropolitana (MANs) y en las Redes de Área Ampla (WAN).

Aunque la fibra es el mejor de todos los medios de transmisión a la hora de transportar grandes cantidades de datos a grandes distancias, la fibra también presenta dificultades. Cuando la luz viaja a través de la fibra, se pierde parte de la energía de la luz. Cuanto mayor es la distancia a la que se envía una señal a través de una fibra, más fuerza pierde la señal. Esta atenuación de la señal se debe a diversos factores implícitos en la naturaleza de la fibra en sí. El factor más importante es la dispersión. La dispersión de la luz dentro de una fibra es producida por defectos microscópicos en la uniformidad (distorsiones) de la fibra que reflejan y dispersan parte de la energía de la luz.

La absorción es otra causa de pérdida de la energía de la luz. Cuando un rayo de luz choca algunos tipos de impurezas químicas dentro de una fibra, estas impurezas absorben parte de la energía. Esta energía de la luz se convierte en una pequeña cantidad de energía calórica. La absorción hace que la señal luminosa sea un poco más débil.

Otro factor que causa atenuación en la señal luminosa son las irregularidades o asperezas de fabricación en el límite entre el núcleo y el revestimiento. Se pierde potencia en la señal luminosa debido a que la reflexión interna total no es perfecta en el área áspera de la fibra. Cualquier imperfección microscópica en el espesor o simetría de la fibra reducirá la reflexión interna total y el revestimiento absorberá parte de la energía de la luz.

La dispersión de un destello de luz también limita las distancias de transmisión de una fibra. Dispersión es el término técnico para la difusión de los pulsos de luz a medida que viajan a través de la fibra. ¹

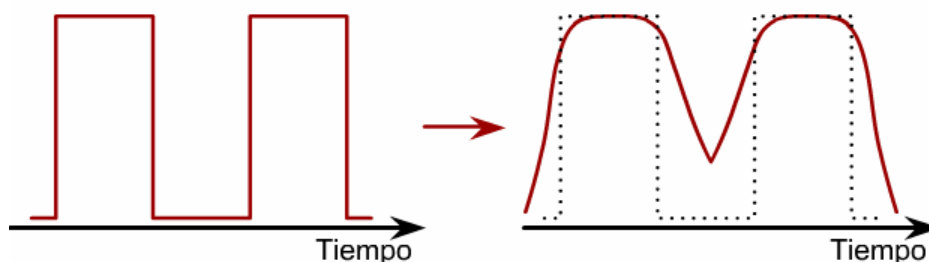


Figura 1

La fibra multimodo de índice graduado está diseñada para compensar las diferentes distancias que los distintos modos de luz deben recorrer en un núcleo de gran diámetro. La fibra monomodo no presenta el problema de trayectos múltiples que una señal luminosa puede recorrer. Sin embargo, la dispersión cromática es una característica de tanto la fibra multimodo como la monomodo. Cuando las longitudes de onda de la luz viajan a través del vidrio a velocidades levemente distintas a las de otras longitudes de onda, se produce la dispersión cromática. Es por eso que un prisma separa las longitudes de onda de la luz. Lo ideal es que la fuente de luz Láser o LED emita luz de una sola frecuencia. Entonces, la dispersión cromática no sería un problema.

Lamentablemente, los láser y, en especial, los LED generan una gama de longitudes de onda de modo que la dispersión cromática limita la distancia hasta que se pueden alcanzar en una fibra. Si se transmite una señal a una distancia demasiado grande, lo que comenzó como un pulso brillante de energía de luz llegará al receptor dispersa, difusa y débil. El receptor no podrá diferenciar un uno de un cero.

3.2.10 Instalación, cuidado y prueba de la fibra óptica

Una de las causas principales de la atenuación excesiva en el cable de fibra óptica es la instalación incorrecta. Si se estira o curva demasiado la fibra, se pueden producir pequeñas fisuras en el núcleo que dispersan los rayos de luz. Al curvar demasiado la fibra se puede cambiar el ángulo de incidencia de los rayos de luz que llegan al límite entre el núcleo y el revestimiento. Entonces, el ángulo de incidencia del rayo será menor que el ángulo crítico para la reflexión interna total. En lugar de reflejarse siguiendo la zona del doblé, parte de los rayos de luz se refractarán en el revestimiento y se perderán. ^{1 2}

Para evitar que la curvatura de la fibra sean demasiado pronunciada, generalmente, se introduce la fibra a un tipo de tubo instalado que se llama de interducto. El interducto es mucho más rígido que la fibra y no se puede curvar de forma pronunciada, de modo que la fibra en el interducto tampoco puede curvarse en

exceso. El interducto protege la fibra, hace que sea mucho más sencillo el tendido y asegura que no se exceda el radio de la curvatura (límite de curva) de la fibra.

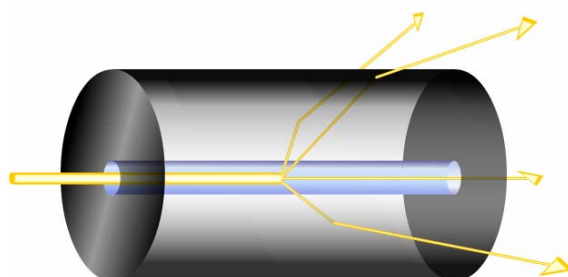


Figura 1

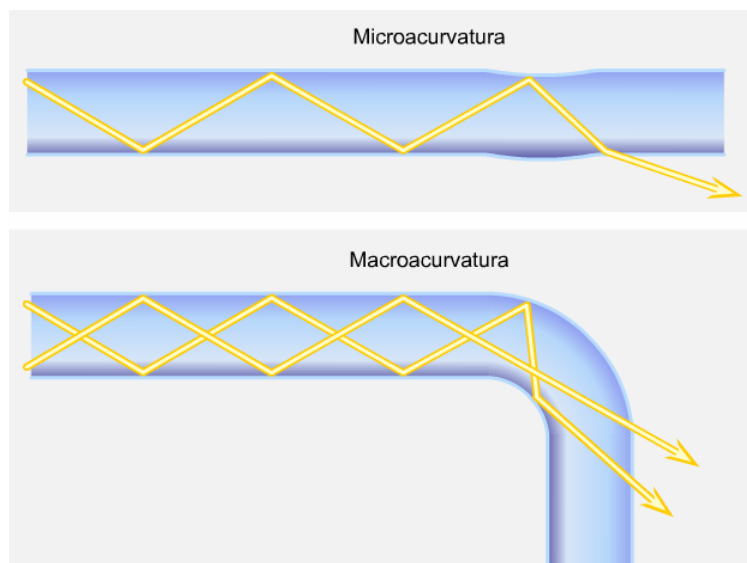


Figura 2

Una vez que se ha tendido la fibra, se debe partir (cortar) y pulir adecuadamente los extremos de la fibra para asegurarse de que estén lisos. ³ Se utiliza un microscopio o un instrumento de prueba con una lupa incorporada para examinar el extremo de la fibra y verificar que tenga la forma y pulido correctos. Entonces, con cuidado, se fija el conector al extremo de la fibra. Los conectores incorrectamente instalados, empalmes no apropiados y el empalme de dos cables de diferentes tamaños de núcleo reducirán drásticamente la fuerza de la señal luminosa. ⁴ ⁵

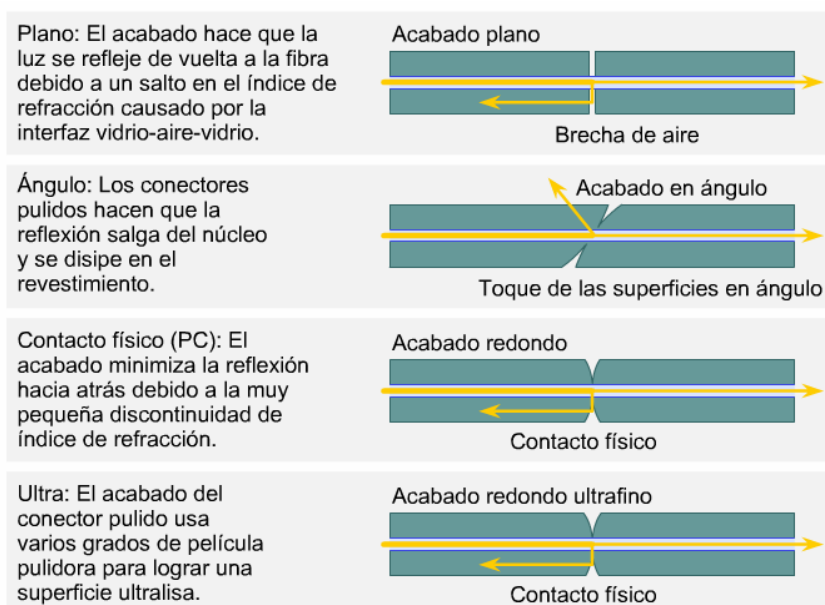


Figura 3

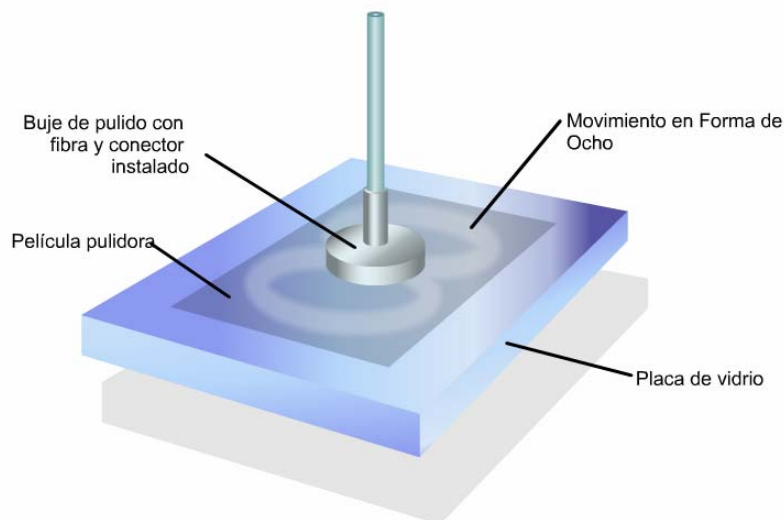


Figura 4

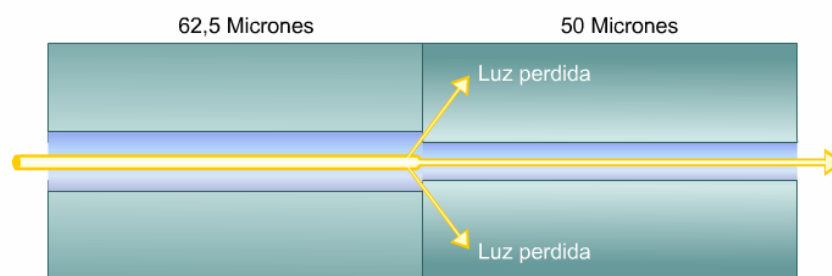


Figura 5

Una vez que el cable de fibra óptica y los conectores han sido instalados, los conectores y los extremos de las fibras deben mantenerse totalmente limpios. Los extremos de las fibras deben cubrirse con cubiertas protectoras para evitar daños. Cuando estas cubiertas son retiradas, antes de conectar la fibra a un puerto en un switch o router, se deben limpiar los extremos de las fibras. Se deben limpiar los extremos de la fibra con paño especial sin pelusa para limpiar lentes, humedecido con alcohol isopropílico puro. Los puertos de fibra de un switch o router también deben mantenerse cubiertos cuando no se encuentran en uso y limpiarse con paño especial para limpiar lentes y alcohol isopropílico antes de realizar la conexión. La suciedad en los extremos de una fibra disminuirá gravemente la cantidad de luz que llega al receptor.

La dispersión, absorción, difusión, incorrecta instalación y los extremos de fibra sucios son factores que disminuyen la fuerza de la señal luminosa y se conocen como ruido de fibra. Antes de usar un cable de fibra óptica, es importante probarlo para asegurarse de que suficiente luz llegue al receptor para que éste pueda detectar los ceros y los unos en la señal.

Al planear un enlace de fibra óptica, es necesario calcular la pérdida tolerable de la potencia de la señal. Esto se conoce como presupuesto de pérdida del enlace óptico. Piense en un presupuesto financiero mensual. Una vez que todos los gastos son sustraídos del ingreso inicial, debe quedar dinero suficiente para todo el mes.

El decibel (dB) es la unidad utilizada para medir la cantidad de pérdida de potencia. Mide el porcentaje de potencia que sale del transmisor y realmente llega al receptor.

Es de suma importancia probar los enlaces de fibra y se deben mantener registros de los resultados de estas pruebas. Se utilizan varios tipos de equipo de prueba para fibra óptica. Dos de los instrumentos más importantes son los Medidores de Pérdida Óptica y los Reflectómetros Ópticos de Dominio de Tiempo (OTDR).

Estos medidores prueban el cable óptico para asegurar que el cable cumpla con los estándares TIA para la fibra. También verifican que la pérdida de potencia del enlace no caiga por debajo del presupuesto de pérdida del enlace óptico. Los OTDR pueden brindar mucha información detallada de diagnóstico sobre el enlace de fibra. Pueden utilizarse para detectar las fallas de un enlace cuando se produce un problema.

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). ¹

- 802.11
- 802.11b
- 802.11a
- 802.11g

Figura 1

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.

802.11g ofrece tasa de transferencia que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b utilizando tecnología de modulación por Multiplexión por División de Frecuencia Ortogonal (OFDM). Cisco ha desarrollado un punto de acceso que permite que los dispositivos 802.11b y 802.11a coexistan en la misma WLAN. El punto de acceso brinda servicios de 'gateway' que permiten que estos dispositivos, que de otra manera serían incompatibles, se comuniquen.

3.3.2 Dispositivos y topologías inalámbricas

Una red inalámbrica puede constar de tan sólo dos dispositivos. ¹- ³Los nodos pueden ser simples estaciones de trabajo de escritorio o computadores de mano. Equipada con NIC inalámbricas, se puede establecer una red 'ad hoc' comparable a una red cableada de par a par. Ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia. Otro problema de este tipo de red es la compatibilidad. Muchas veces, las NIC de diferentes fabricantes no son compatibles.

Para resolver el problema de la compatibilidad, se suele instalar un punto de acceso (AP) para que actúe como hub central para el modo de infraestructura de la WLAN. ⁴El AP se conecta mediante cableado a la LAN cableada a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están

equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda. ⁵Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente. Por lo general, el alcance es de 91,44 a 152,4 metros (300 a 500 pies). Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición. Esta superposición permite pasar de una celda a otra (roaming). ⁶Esto es muy parecido a los servicios que brindan las empresas de teléfonos celulares. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN. Aunque los estándares del IEEE no determinan nada al respecto, es aconsejable una superposición de un 20-30% . Este índice de superposición permitirá el roaming entre las celdas y así la actividad de desconexión y reconexión no tendrá interrupciones.

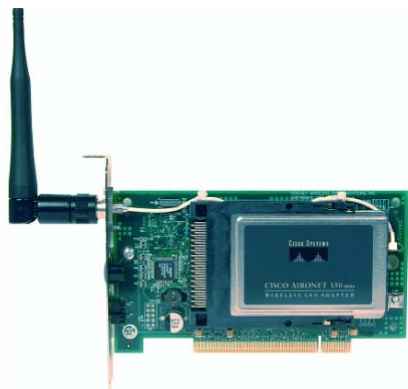


Figura 1



Figura 2



Figura 3



Figura 4

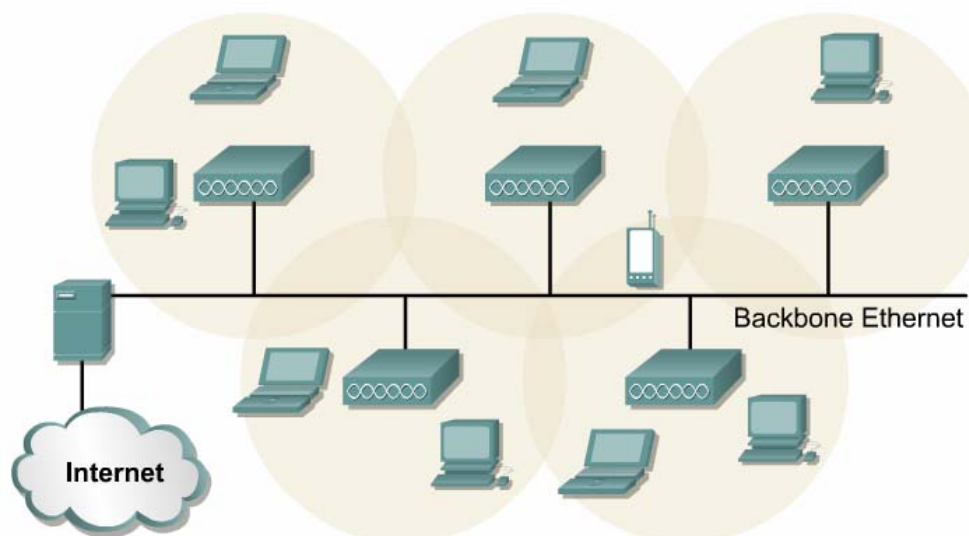


Figura 5

Cuando se activa un cliente dentro de la WLAN, la red comenzará a "escuchar" para ver si hay un dispositivo compatible con el cual "asociarse". Esto se conoce como "escaneo" y puede ser activo o pasivo. El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea

conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo. Se completan los pasos de autenticación y asociación.

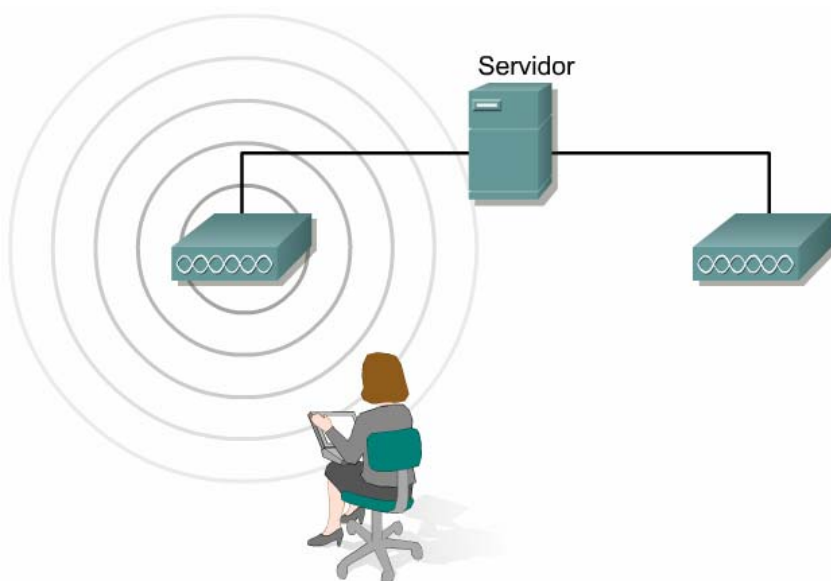


Figura 6

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

3.3.3 Cómo se comunican las LAN inalámbricas

Una vez establecida la conectividad con la WLAN, un nodo pasará las tramas de igual forma que en cualquier otra red 802.x. Las WLAN no usan una trama estándar 802.3. Por lo tanto, el término "Ethernet inalámbrica" puede resultar engañoso. Hay tres clases de tramas: de control, de administración y de datos. 1 Sólo la trama de datos es parecida a 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.

Tramas de administración
• Trama de pedido de asociación
• Trama de respuesta de asociación
• Trama de pedido de sonda
• Trama de respuesta de sonda
• Trama de beacon
• Trama de autenticación
Tramas de control
• Petición para enviar (RTS)
• Preparado para enviar (CTS)
• Acuse de recibo
Tramas de datos

Figura 1

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. ^[2]

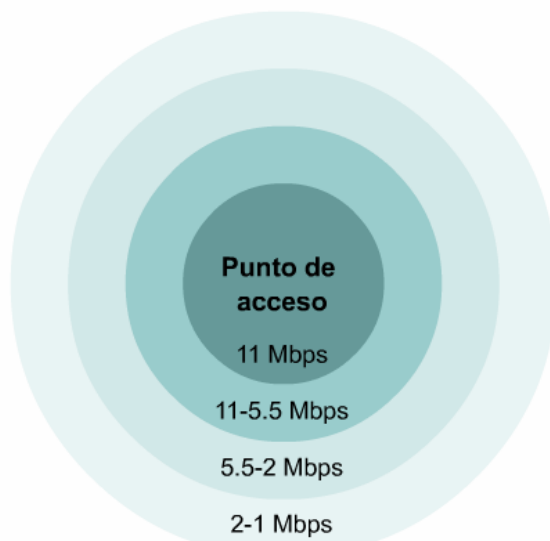


Figura 2

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. ^[1]

- No autenticado y no asociado
- Autenticado y no asociado
- Autenticado y asociado

Figura 1

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.

Tipos de autenticación y asociación

- No autenticado y no asociado
- El nodo está desconectado de la red y no está asociado a un punto de acceso.
- Autenticado y no asociado
- El nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso.
- Autenticado y asociado
- El nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso.

Métodos de Autenticación

IEEE 802.11 presenta dos tipos de procesos de autenticación.

El primer proceso de autenticación es un sistema abierto. Se trata de un estándar de conectividad abierto en el que sólo debe coincidir el SSID. Puede ser utilizado en un entorno seguro y no seguro aunque existe una alta capacidad de los 'husmeadores' de red de bajo nivel para descubrir el SSID de la LAN.

El segundo proceso es una clave compartida. Este proceso requiere el uso de un cifrado del Protocolo de Equivalencia de Comunicaciones Inalámbricas (WEP). WEP es un algoritmo bastante sencillo que utiliza claves de 64 y 128 bits. El AP está configurado con una clave cifrada y los nodos que buscan acceso a la red a través del AP deben tener una clave que coincida. Las claves del WEP asignadas de forma estática brindan un mayor nivel de seguridad que el sistema abierto pero definitivamente no son invulnerables a la piratería informática.

El problema del ingreso no autorizado a las WLAN actualmente está siendo considerado por un gran número de nuevas tecnologías de soluciones de seguridad.

3.3.5 Los espectros de onda de radio y microondas

Los computadores envían señales de datos electrónicamente. Los transmisores de radio convierten estas señales eléctricas en ondas de radio. Las corrientes eléctricas cambiantes en la antena de un transmisor generan ondas de radio. Estas ondas de radio son irradiadas en líneas rectas desde la antena. ¹ Sin embargo, las ondas de radio se atenúan a medida que se alejan de la antena transmisora. En una WLAN, una señal de radio medida a una distancia de sólo 10 metros (30 pies) de la antena transmisora suele tener sólo 1/100mo de su potencia original. Al igual que lo que sucede con la luz, las ondas de radio pueden ser absorbidas por ciertos materiales y reflejadas 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.



Figura 1

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. ²

En un transmisor, las señales eléctricas (datos) que provienen de un computador 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.

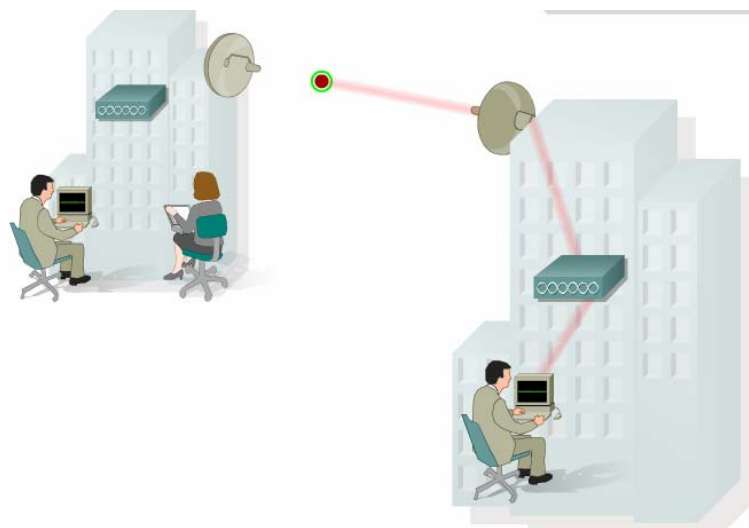


Figura 2

El proceso de alterar una señal portadora que ingresará a la antena del transmisor recibe el nombre de modulación. Existen tres formas básicas en las que se puede modular una señal portadora de radio. Por ejemplo: las estaciones de radio de Amplitud Modulada (AM) modulan la altura (amplitud) de la señal portadora. Las estaciones de Frecuencia Modulada (FM) modulan la frecuencia de la señal portadora según lo determina la señal eléctrica proveniente del micrófono. En las WLAN, se utiliza un tercer tipo de modulación llamado modulación de fase para superponer la señal de los datos a la señal portadora enviada por el transmisor. ³

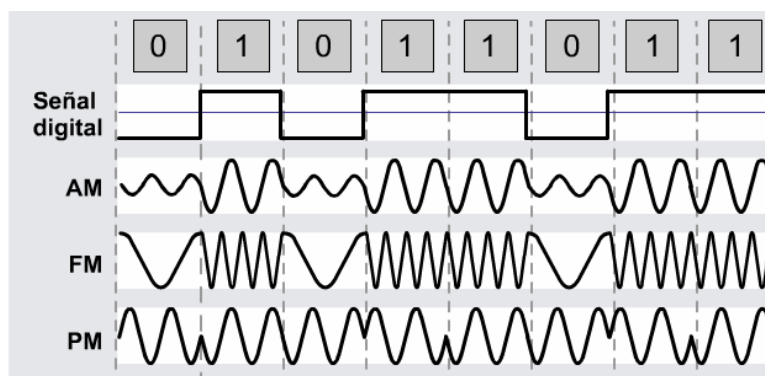


Figura 3

En este tipo de modulación, los bits de datos de una señal eléctrica cambian la fase de la señal portadora. Un receptor demodula la señal portadora que llega desde su antena. El receptor interpreta los cambios de fase de estos la señal portadora y la reconstruye a partir de la señal eléctrica de datos original.

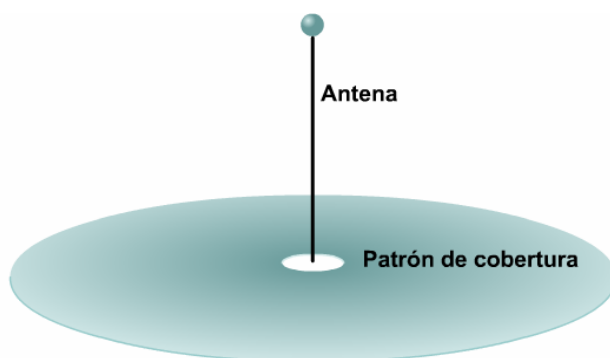
3.3.6 Señales y ruido en una WLAN

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. En realidad, diagnosticar la causa de interferencia en la banda estrecha puede ser una experiencia costosa y que consume tiempo. Identificar la fuente requiere el uso de un analizador de espectro que resulta relativamente costoso, aunque se trate de un modelo económico.

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.

La primera fuente de problemas de señal, y la más obvia, es la estación transmisora y el tipo de antena. Una estación de mayor potencia transmitirá la señal a mayor distancia y una antena parabólica que concentre la señal aumentará el alcance de la transmisión.

En un entorno SOHO, la mayoría de los puntos de acceso utilizan antenas omnidireccionales gemelas que transmiten la señal en todas las direcciones reduciendo así el alcance de la comunicación.

3.3.7 Seguridad de la transmisión inalámbrica

Como ya se ha tratado en este capítulo, la seguridad de las transmisiones inalámbricas puede ser difícil de lograr. Donde existen redes inalámbricas, la seguridad es reducida. Esto ha sido un problema desde los primeros días de las WLAN. En la actualidad, muchos administradores no se ocupan de implementar prácticas de seguridad efectivas.

Están surgiendo varios nuevos protocolos y soluciones de seguridad tales como las Redes Privadas Virtuales (VPN) y el Protocolo de Autenticación Extensible (EAP). En el caso del EAP, el punto de acceso no brinda autenticación al cliente, sino que pasa esta tarea a un dispositivo más sofisticado, posiblemente un servidor dedicado, diseñado para tal fin. Con un servidor integrado, la tecnología VPN crea un túnel sobre un protocolo existente, como por ejemplo el IP. Esta forma una conexión de Capa 3, a diferencia de la conexión de Capa 2 entre el AP y el nodo emisor. ¹



Figura 1

- **Desafío EAP-MD5:** El Protocolo de Autenticación Extensible (EAP) es el tipo de autenticación más antiguo, muy parecido a la protección CHAP con contraseña de una red cableada.
- **LEAP (Cisco):** El Protocolo Liviano de Autenticación Extensible es el tipo más utilizado en los puntos de acceso de las WLAN de Cisco. LEAP brinda seguridad durante el intercambio de credenciales, cifra utilizando claves dinámicas WEP y admite la autenticación mutua.
- **Autenticación del usuario:** Permite que sólo usuarios autenticados se conecten, envíen y reciban datos a través de la red inalámbrica.
- **Cifrado:** Brinda servicios de cifrado que ofrecen protección adicional de los datos contra intrusos.
- **Autenticación de datos:** Asegura la integridad de los datos, autenticando los dispositivos fuente y destino.

La tecnología VPN cierra efectivamente la red inalámbrica ya que una WLAN irrestricta envía tráfico automáticamente entre los nodos que parecen estar en la misma red inalámbrica. Las WLAN a menudo se extienden por afuera del perímetro del hogar o de la oficina donde se las instala y, si no hay seguridad, sin mucho esfuerzo los intrusos pueden infiltrarse en la red. Por otra parte, es poco el esfuerzo necesario de parte del administrador de la red para brindar seguridad de bajo nivel a la WLAN.

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.
- La comprensión de las reglamentaciones y los estándares que se aplican a la tecnología inalámbrica permitirá la interoperabilidad y cumplimiento de todas las redes existentes.
- Los problemas de compatibilidad con las NIC se resuelven instalando un punto de acceso (AP) que actúe como hub central para la WLAN
- Son tres los tipos de tramas que se utilizan en las comunicaciones inalámbricas: de control, de administración y de datos
- Las WLAN utilizan Acceso Múltiple con Detección de Portadora y Prevención de Colisiones (CSMA/CA).
- La autenticación de la WLAN es un proceso que autentica el dispositivo, no el usuario.

Módulo 4: Prueba del cable

Descripción general

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, fibra óptica e inalámbricos, 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.

El objetivo de la primera lección de este módulo es brindar algunas definiciones básicas que servirán para comprender los conceptos sobre pruebas de cables que se presentan en la segunda sección.

La segunda lección de este módulo describe los temas relacionados con la prueba de los medios utilizados para la conectividad de la capa física en las redes de área local (LAN). Para que la LAN funcione correctamente, el medio de la capa física debería cumplir con las especificaciones de los estándares industriales.

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. Este módulo también describe las muchas e importantes pruebas que se realizan.

Los estudiantes que completen este módulo deberán poder:

- Distinguir entre ondas sinusoidales y ondas rectangulares.
- Definir y calcular exponentes y logaritmos.
- Definir y calcular decibelios.
- Definir terminología básica relacionada con tiempo, frecuencia y ruido.
- Distinguir entre ancho de banda digital y ancho de banda analógico.
- Comparar y contrastar niveles de ruido en distintos tipos de cableado.
- Definir y describir los efectos de la falta de concordancia entre atenuación e impedancia.
- Definir diafonía, paradiafonía, telediafonía y paradiafonía de suma de potencia.
- Describir cómo los pares trenzados contribuyen a reducir el ruido.
- Describir las diez pruebas de cable de cobre definidas en TIA/EIA-568-B.
- Describir la diferencia entre un cable de Categoría 5 y un cable de Categoría 6

4.1 Información básica para el estudio de pruebas de cables basadas en frecuencia

4.1.1 Ondas

Una onda es energía que circula de un lugar a otro. Hay muchos tipos de ondas, pero es posible describirlas todas con vocabulario similar.

Es útil pensar en las ondas como disturbios. Un cubo de agua completamente quieto no tiene ondas, porque no hay disturbios. Por el contrario, el océano siempre presenta algún tipo de onda (las olas) detectable debido a los disturbios provocados por el viento y la marea.

Las olas del océano se pueden describir en función de su altura, o amplitud, que se podría medir en metros. También se pueden describir en función de la frecuencia con la que llegan a la orilla, usando período y frecuencia. El período de las olas es el tiempo que transcurre entre cada ola, medida en segundos. La frecuencia es la cantidad de olas que llega a la orilla por segundo, medida en hertz. Un hercio equivale a una ola por segundo, o un ciclo por segundo.

Los profesionales de redes están particularmente interesados en las ondas de voltaje en medios de cobre, las ondas de luz en fibras ópticas, y los campos alternos eléctricos y magnéticos que se denominan ondas electromagnéticas. La amplitud de una señal eléctrica también representa su altura, pero se mide en voltios (V) en lugar de metros (m). El período es la cantidad de tiempo que lleva cumplir un ciclo, medida en segundos. La frecuencia es la cantidad de ciclos completos por segundo, medida en hertz.

Si se genera deliberadamente un disturbio con una duración fija y predecible, éste se llama pulso. Los pulsos son una parte importante de las señales eléctricas porque son la base de la transmisión digital. El patrón de los pulsos representa el valor de los datos que están siendo transmitidos.

4.1.2 Ondas sinoidales y ondas rectangulares

Las ondas sinoidales, son gráficos de funciones matemáticas. ¹Las ondas sinoidales poseen ciertas características. Las ondas sinoidales son periódicas, o sea que repiten el mismo patrón a intervalos regulares. Las ondas sinoidales varían continuamente, o sea que no existen dos puntos adyacentes en el gráfico con el mismo valor.

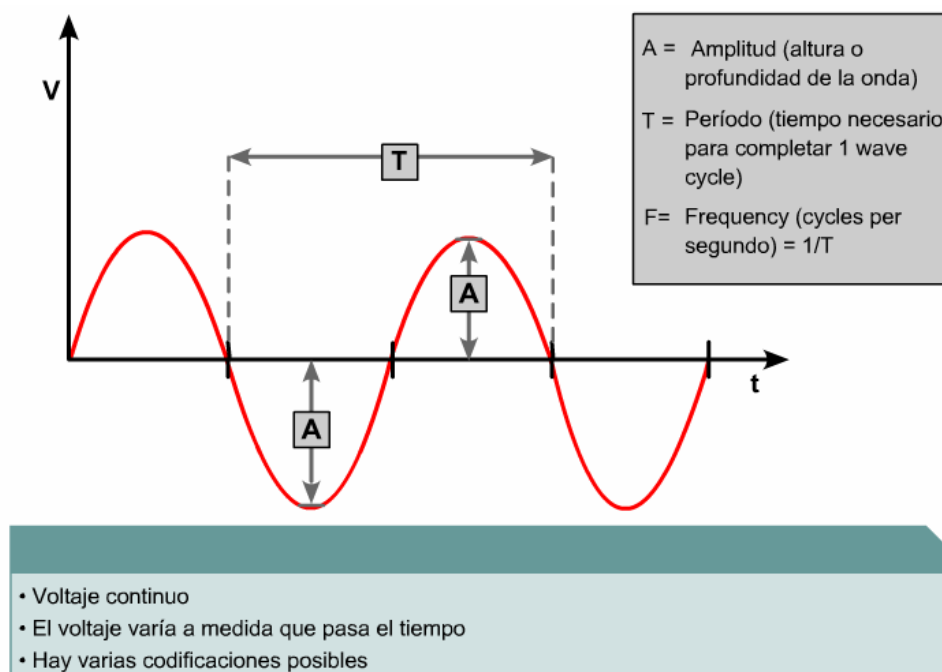


Figura 1

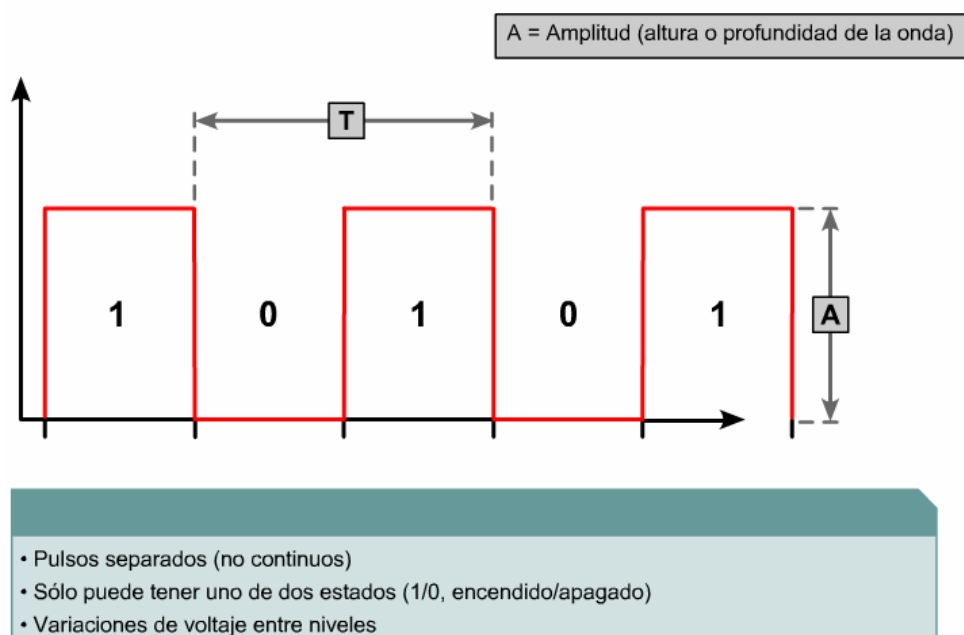


Figura 2

Las ondas sinusoidales 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 sinusoidales varían continuamente, son ejemplos de ondas analógicas.

Las ondas rectangulares, al igual que las ondas sinusoidales, 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.

4.1.3 Exponentes y logaritmos

En de redes, existen tres sistemas numéricos importantes: ¹

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

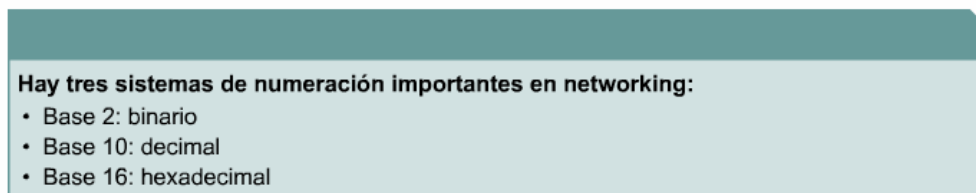


Figura 1

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.

Recuerde que 10×10 se puede escribir como 10^2 . 10^2 significa diez al cuadrado o elevado a la segunda potencia. Escrito de esta manera, se dice que 10 es la base del número y 2 es el exponente del número. $10 \times 10 \times 10$ se puede escribir como 10^3 . 10^3 significa diez al cubo o diez elevado a la tercera potencia. La base sigue siendo 10, pero el exponente ahora es tres. Use las Actividades de Medios a continuación para practicar el cálculo de exponentes. Ingrese "x" y se calculará "y", o bien, ingrese "y" y se calculará "x".

La base de un sistema numérico también se refiere al valor de cada dígito. El dígito menos significativo posee un valor de base⁰, o uno. El siguiente dígito posee un valor de base¹. Esto equivale a 2 para números binarios, 10 para números decimales y 16 para números hexadecimales.

Los números con exponentes se utilizan para representar fácilmente cifras muy grandes o muy pequeñas. Es mucho más fácil y menos propenso a errores representar mil millones numéricamente como 10^9 que como 1000000000. Muchos de los cálculos de las pruebas de cables implican el uso de cifras muy grandes, por eso se prefiere el formato exponencial.

Una forma de trabajar con las cifras muy grandes y muy pequeñas que ocurren en las redes es transformar las cifras conforme a la regla, o función matemática, conocida como logaritmo. Logaritmo se abrevia como "log". Se puede usar cualquier número como base para un sistema de logaritmos. Sin embargo, la base 10 tiene muchas ventajas que no se pueden obtener en los cálculos ordinarios con otras bases. Para cálculos ordinarios se usa casi exclusivamente la base 10. Los logaritmos con 10 como base se conocen como logaritmos comunes. No es posible obtener el logaritmo de un número negativo.

Para calcular el "log" de un número, use una calculadora o la actividad flash. Por ejemplo, $\log(10^9)$ es igual a 9, $\log(10^{-3}) = -3$. También se puede calcular el logaritmo de números que no son potencias de 10, pero no se puede calcular el logaritmo de un número negativo. El estudio de los logaritmos está fuera de los objetivos de este curso. Sin embargo, la terminología se usa a menudo para calcular decibelios y para medir la intensidad de la señal en medios de cobre, ópticos e inalámbricos.

4.1.4 Decibelios

El decibelio (dB) es una unidad de medida importante para la descripción de señales de redes. El decibelio se relaciona con los exponentes y logaritmos descritos en secciones anteriores. Hay dos fórmulas para calcular los decibelios: ¹

Hay dos fórmulas para calcular los decibelios:

- $\text{dB} = 10 \log_{10} (P_{\text{final}}/P_{\text{ref}})$
- $\text{dB} = 20 \log_{10} (V_{\text{final}}/V_{\text{referencia}})$

Figura 1

$$\text{dB} = 10 \log_{10} (P_{\text{final}} / P_{\text{ref}})$$

$$\text{dB} = 20 \log_{10} (V_{\text{final}} / V_{\text{ref}})$$

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

$V_{\text{referencia}}$ 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 $\text{dB} = 10 \log_{10} (P_{\text{final}} / P_{\text{ref}})$, 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.

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. Las ondas de sonido de la voz del que llama ingresan a un micrófono en el teléfono. El micrófono convierte los patrones de energía sonora en patrones de voltaje de energía eléctrica que representan la voz.

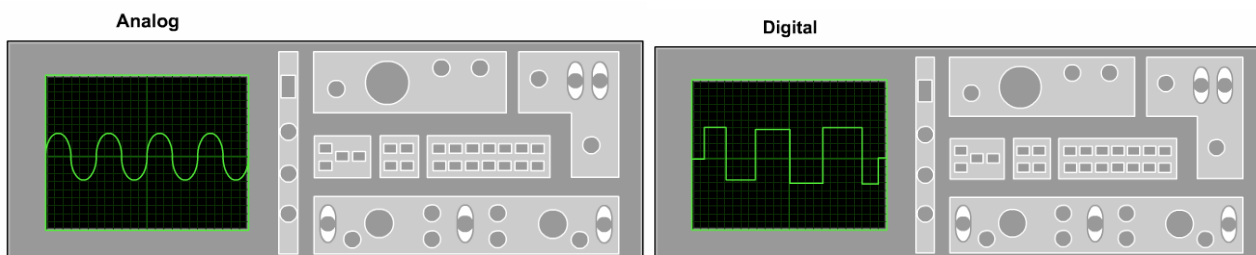


Figura 1

Si los patrones de voltaje se graficaran en función del tiempo, se verían los distintos patrones que representan la voz. ¹Un osciloscopio es un dispositivo electrónico importante que se utiliza para observar

señales eléctricas como, por ejemplo, las ondas de voltaje y pulsos. El eje "x" en el gráfico representa el tiempo y el eje "y" representa el voltaje o la corriente. Generalmente existen dos ejes "y", de modo que se pueden observar y medir dos ondas al mismo tiempo.

El análisis de las señales con un osciloscopio se denomina análisis de dominio temporal, porque el eje "x", o dominio de la función matemática, representa el tiempo. Los ingenieros también utilizan el análisis de dominio de frecuencia para estudiar señales. En el análisis de dominio de frecuencia, el eje "x" representa la frecuencia. Un dispositivo electrónico denominado analizador de espectro genera gráficos para este tipo de análisis.

Las señales electromagnéticas usan diferentes frecuencias para la transmisión, para que las diferentes señales no interfieran entre sí. Las señales de radio de Frecuencia Modulada (FM) usan frecuencias distintas de las señales de televisión o satélite. Cuando los oyentes cambian de estación de radio, están cambiando la frecuencia que recibe la radio.

4.1.6 Señales analógicas y digitales en tiempo y frecuencia

Para entender la complejidad de las señales de redes y de las pruebas de cable, examine cómo las señales analógicas varían en función del tiempo y de la frecuencia. Primero, piense en una onda sinusoidal eléctrica de una sola frecuencia, cuya frecuencia es detectable por el oído humano. Si esta señal se transmite a un orador, es posible oír un tono.

A continuación, imagine la combinación de varias ondas sinusoidales. ¹La onda resultante es más compleja que una onda sinusoidal pura. Se oírían varios tonos. El gráfico de varios tonos muestra varias líneas individuales que corresponden a la frecuencia de cada tono. Finalmente, imagine una señal compleja, como una voz o un instrumento musical. Si hay presentes muchos tonos diferentes, se representaría un espectro continuo de tonos individuales.

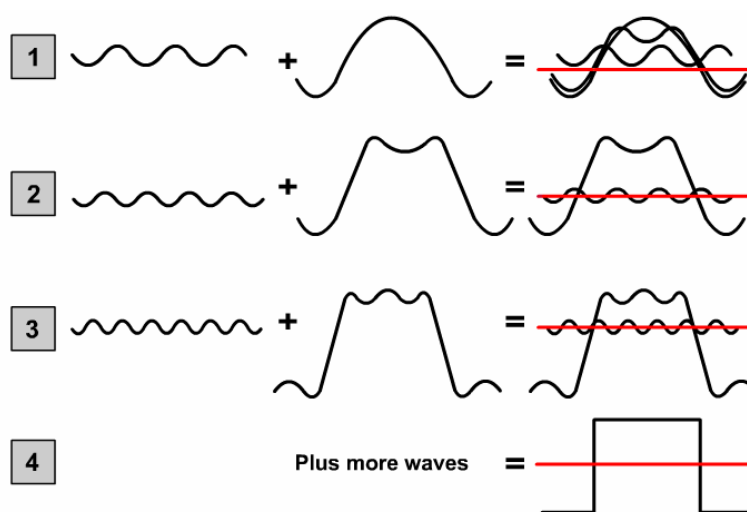


Figura 1

4.1.7 El ruido en tiempo y frecuencia

El ruido es un concepto importante en los sistemas de comunicación, incluyendo las LAN. ¹Cuando se habla de ruido, normalmente se hace referencia a sonidos indeseables; sin embargo, cuando se habla de comunicaciones se entiende por ruido señales indeseables. El ruido puede provenir de fuentes naturales y tecnológicas, y se agrega a las señales de datos en los sistemas de comunicación.

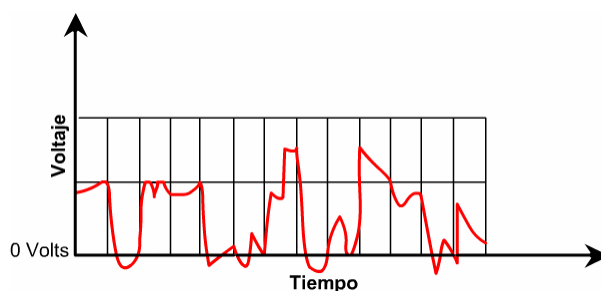


Figura 1

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.

Unidad de ancho de banda	Abrev.	Equivalencia
Bits por segundo	bps	1 kbps = 1.000 bps
Kilobits por segundo	kbps	1 kbps = 1.000 bps
Megabits por segundo	Mbps	1 Mbps = 1.000.000 bps = 1.000 kbps
Gigabits por segundo	Gbps	1 Gbps = 1.000.000.000 bps = 1.000 Mbps

Figura 1

Durante el proceso de prueba de los cables, se usa el ancho de banda analógico para determinar el ancho de banda digital de un cable de cobre. Las formas de onda digitales están compuestas de muchas ondas sinusoidales (ondas análogas). Las frecuencias analógicas se transmiten desde un extremo y se reciben en el extremo opuesto. Luego, ambas señales se comparan y se calcula la atenuación de la señal. En general, los medios capaces de admitir anchos de banda analógicos más altos sin niveles elevados de atenuación, también admiten anchos de banda digitales más altos.

4.2 Señales y ruido

4.2.1 Señales en cables 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. Es importante que tanto el dispositivo transmisor como el receptor hagan referencia al mismo punto de referencia de cero voltios. Cuando es así, se dice que están correctamente conectados a tierra.

Para que una LAN funcione correctamente, el dispositivo receptor debe poder interpretar con precisión los unos y ceros binarios transmitidos como niveles de voltaje. Como la tecnología actual de Ethernet admite

velocidades de miles de millones de bits por segundo, cada bit debe ser reconocido, aun cuando su duración sea muy breve. Esto significa que es necesario retener lo más posible la potencia original de la señal, a medida que la señal recorre el cable y atraviesa los conectores. Anticipándonos a protocolos de Ethernet cada vez más veloces, las nuevas instalaciones de cables se deben hacer con los mejores cables, conectores y dispositivos de interconexión disponibles, tales como bloques de empuje y paneles de conexión.

Existen dos tipos básicos de cables de cobre: blindados y no blindados. En los cables blindados, el material de blindaje protege la señal de datos de las fuentes externas de ruido, así como de ruido generado por señales eléctricas dentro del cable.

El cable coaxial es un tipo de cable blindado. ¹ Se compone de un conductor de cobre sólido recubierto con material aislante, y luego con un blindaje conductor trenzado. En las aplicaciones LAN, el blindaje trenzado está conectado a tierra eléctricamente para proteger el conductor interno del ruido eléctrico externo. El blindaje contribuye además a eliminar la pérdida de la señal, evitando que la señal transmitida se escape del cable. Esto ayuda a que el cable coaxial sea menos sujeto al ruido que los otros tipos de cableado de cobre, pero también lo hace más caro. La necesidad de conectar el blindaje a tierra, así como el tamaño voluminoso del cable coaxial, dificultan su instalación en comparación con otros cables de cobre.

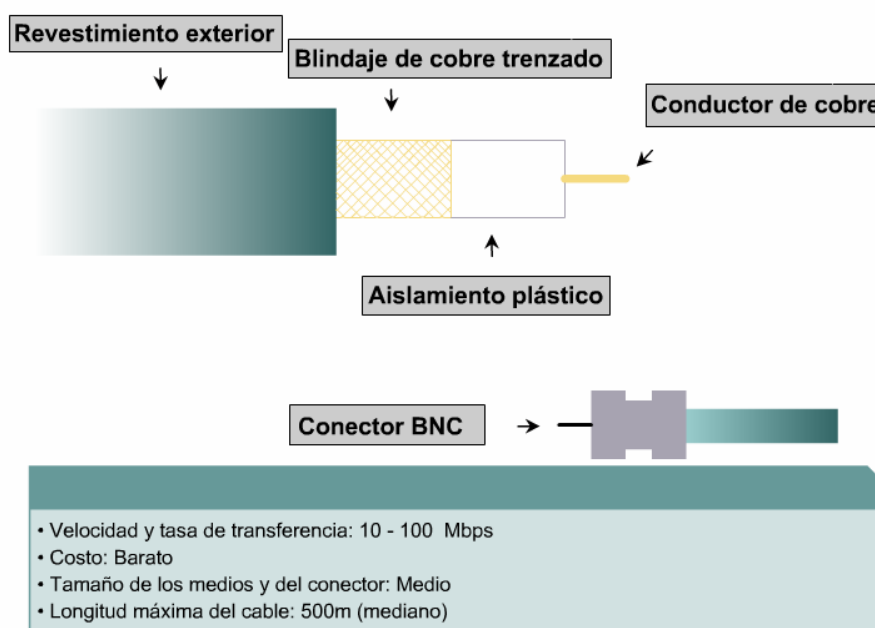


Figura 1

Existen dos tipos de cables de par trenzado: par trenzado blindado (STP) y par trenzado no blindado (UTP).

² ³

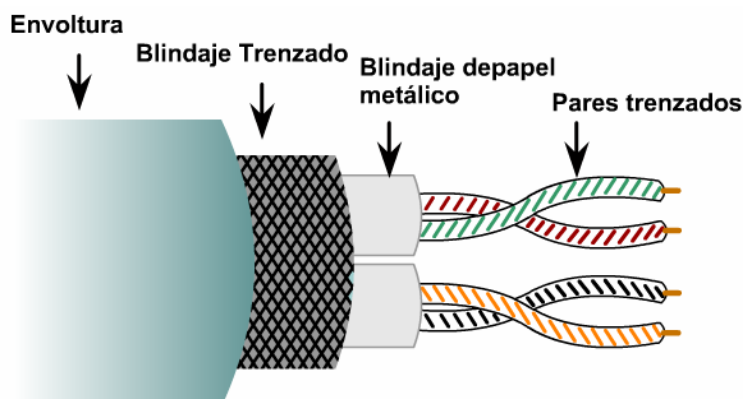


Figura 2

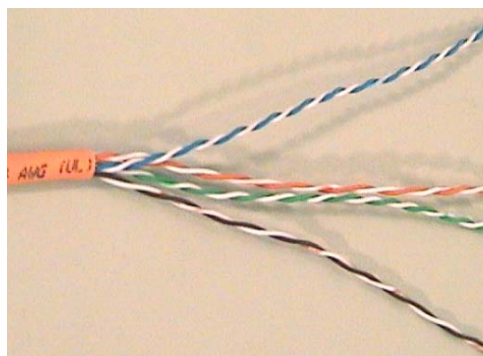


Figura 3

El cable STP contiene un blindaje conductivo externo conectado eléctricamente a tierra para aislar las señales del ruido eléctrico externo. El STP utiliza además blindajes metálicos internos que protegen cada par de cables del ruido generado por los otros pares. Al cable STP a veces se lo llama por error par trenzado apantallado (ScTP). ScTP se refiere generalmente a un cable de par trenzado de Categoría 5 o 5E, mientras que STP se refiere a un cable propietario de IBM que contiene solo dos pares de conductores.

El cable ScTP es más caro, más difícil de instalar, y se usa con menos frecuencia que el UTP. El UTP no tiene blindaje y es más susceptible al ruido externo, pero se usa con más frecuencia por ser económico y más fácil de instalar.

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. ⁴La intensidad de una señal luminosa no disminuye tanto como la intensidad de una señal eléctrica sobre un 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. Por lo tanto, se suele usar fibra óptica entre edificios y entre pisos de un mismo edificio. A medida que disminuyen los costos y aumenta la demanda de velocidad, es posible que la fibra óptica se use cada vez más en los medios LAN.

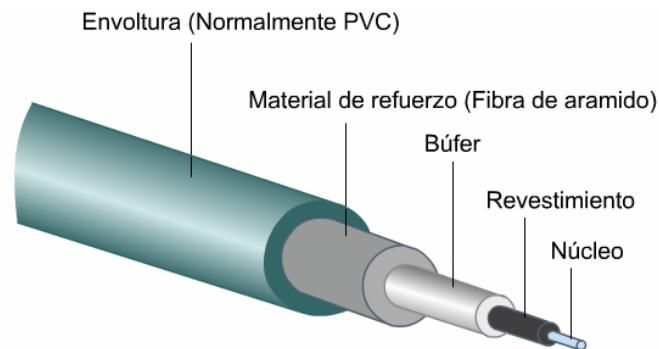
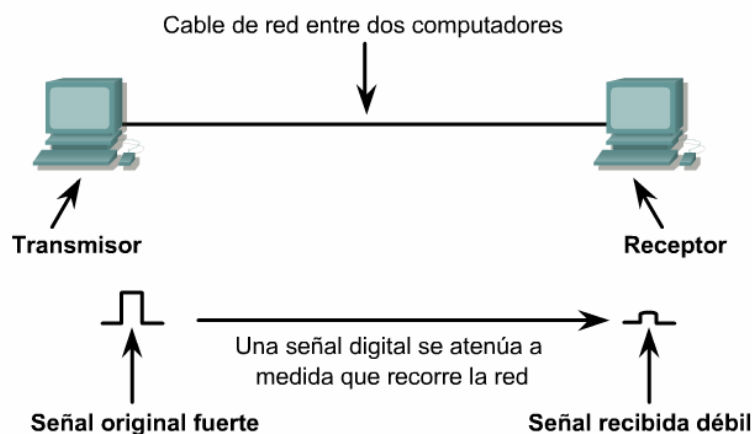


Figura 4

4.2.2 Atenuación y pérdida de inserción en medios de cobre

La atenuación 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.



Son muchos los factores que contribuyen a la atenuación. La resistencia del cable de cobre convierte en calor a parte de la energía eléctrica de la señal. La señal también pierde energía cuando se filtra por el aislamiento del cable y como resultado de la impedancia provocada por conectores defectuosos.

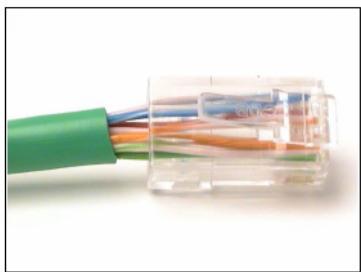
La impedancia mide la resistencia del cable a la corriente alterna (CA) y se mide en ohmios. La impedancia normal, o característica, de un cable Cat5 es de 100 ohmios. Si un conector no está instalado correctamente en Cat5, tendrá un valor de impedancia distinto al del cable. Esto se conoce como discontinuidad en la impedancia o desacoplamiento de impedancias.

La discontinuidad en la impedancia provoca atenuación porque una porción de la señal transmitida se volverá a reflejar en el dispositivo transmisor en lugar de seguir su camino al receptor, como si fuera un eco. Este efecto se complica si ocurren múltiples discontinuidades que hacen que porciones adicionales de la señal restante se vuelvan a reflejar en el transmisor. Cuando el retorno de este reflejo choca con la primera discontinuidad, parte de la señal rebota en dirección de la señal original, creando múltiples efectos de eco. Los ecos chocan con el receptor a distintos intervalos, dificultando la tarea de detectar con precisión los valores de datos de la señal. A esto se lo conoce como fluctuación, y genera errores en los datos.

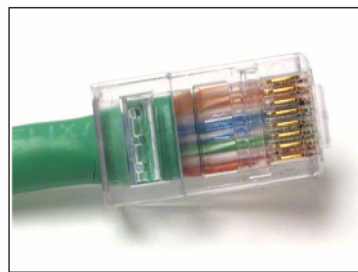
La combinación de los efectos de una señal atenuada con las discontinuidades en la impedancia en un enlace de comunicación se conoce como pérdida de inserción. El correcto funcionamiento de una red depende de una impedancia característica y constante en todos los cables y conectores, sin discontinuidades en la impedancia a lo largo de todo el sistema de cables.

4.2.3 Fuentes de ruido en medios de cobre

El ruido consiste en cualquier energía eléctrica en el cable de transmisión que dificulte que un receptor interprete los datos enviados por el transmisor. En la actualidad, la certificación TIA/EIA-568-B de un cable exige que se hagan pruebas de varios tipos de ruido.



Conector defectuoso: Los hilos están sin trenzar en un trecho demasiado largo.



Conector correcto: Los hilos están sin trenzar sólo en el trecho necesario para unir el conector.

La diafonía es la transmisión de señales de un hilo a otro circundante. Cuando cambia el voltaje en un hilo, se genera energía electromagnética. El hilo transmisor irradia esta energía como una señal de radio de un transmisor. Los hilos adyacentes del cable funcionan como antenas que reciben la energía transmitida, lo que interfiere con los datos transmitidos en esos hilos. Las señales de cables diferentes pero circundantes también pueden causar diafonía. Cuando la diafonía es provocada por una señal de otro cable, se conoce como acoplamiento de diafonía. La diafonía es más destructiva a frecuencias de transmisión elevadas.

Los instrumentos de prueba de cables miden la diafonía aplicando una señal de prueba a un par de hilos. El analizador de cables mide la amplitud de las señales diafónicas no deseadas inducidas sobre los otros pares de hilos del cable.

Los cables de par trenzado están diseñados para aprovechar los efectos de la diafonía para minimizar el ruido. En los cables de par trenzado, se utiliza un par de hilos para transmitir una señal. El par de hilos está trenzado de tal modo que cada hilo experimenta una diafonía similar. Como una señal de ruido en un hilo aparecerá en forma idéntica en el otro hilo, es fácil detectar este ruido y filtrarlo en el receptor.

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: **1**

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

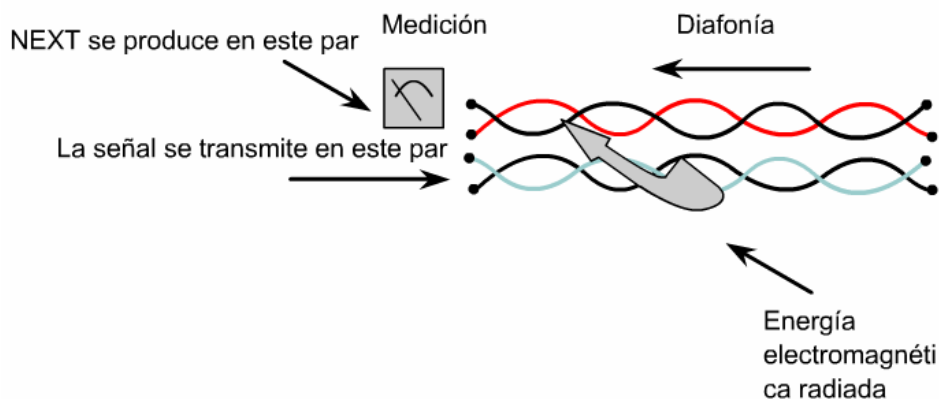


Figura 1

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. Las mediciones resultantes quizás no cumplan con TIA/EIA-568-B, y pasen por alto fallas en el enlace. Para verificar el correcto desempeño de un enlace, NEXT se debe medir desde ambos extremos del enlace con un instrumento de prueba de buena calidad. Este es también un requisito para cumplir con la totalidad de las especificaciones para cables de alta velocidad.

Debido a la atenuación, la diafonía que ocurre a mayor distancia del transmisor genera menos ruido en un cable que la NEXT. A esto se le conoce como telediafonía, o FEXT. El ruido causado por FEXT también regresa a la fuente, pero se va atenuando en el trayecto. Por lo tanto, FEXT no es un problema tan significativo como NEXT.

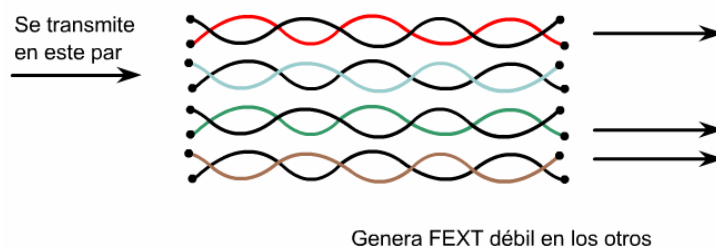


Figura 2

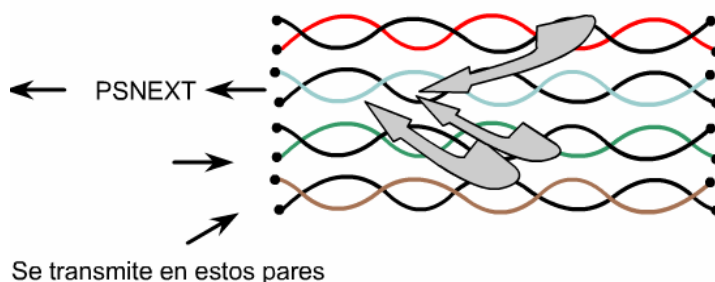


Figura 3

La Paradiafonía de suma de potencia (PSNEXT) mide el efecto acumulativo de NEXT de todos los pares de hilos del cable. PSNEXT se computa para cada par de hilos en base a los efectos de NEXT de los otros tres pares. El efecto combinado de la diafonía proveniente de múltiples fuentes simultáneas de transmisión

puede ser muy perjudicial para la señal. En la actualidad, la certificación TIA/EIA-568-B exige esta prueba de PSNEXT.

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. ¹ 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. ² El mapa de cableado asegura que no existan circuitos abiertos o cortocircuitos en el cable. Un circuito abierto ocurre cuando un hilo no está correctamente unido al conector. Un cortocircuito ocurre cuando dos hilos están conectados entre sí.

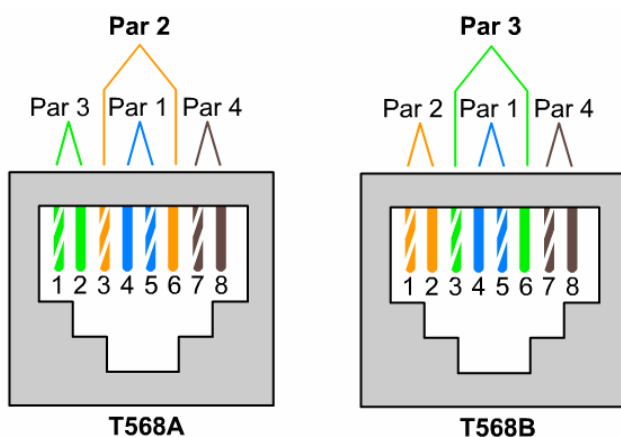


Figura 1

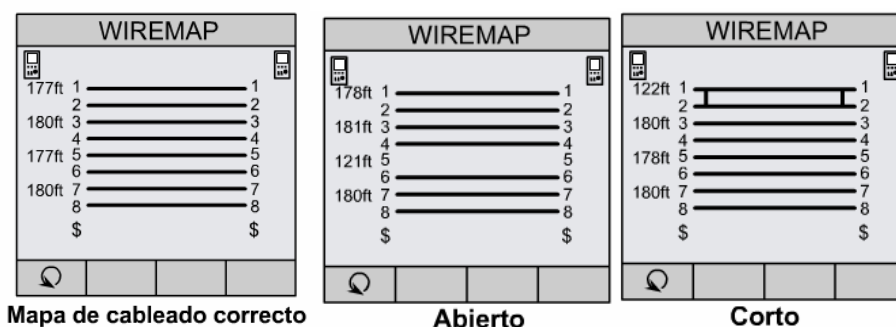


Figura 2

El mapa del cableado verifica además que la totalidad de los ocho cables estén conectados a los pins correspondientes en ambos extremos del cable. Son varias las fallas de cableado que el mapa de cableado puede detectar. 3 La falla de par invertido ocurre cuando un par de hilos está correctamente instalado en un conector, pero invertido en el otro conector. Si el hilo blanco/naranja se termina en el pin 1 y el hilo naranja se termina en el pin 2 en uno de los extremos de un cable, pero de forma invertida en el otro extremo, entonces el cable tiene una falla de par invertido. Este ejemplo se ilustra en el gráfico.

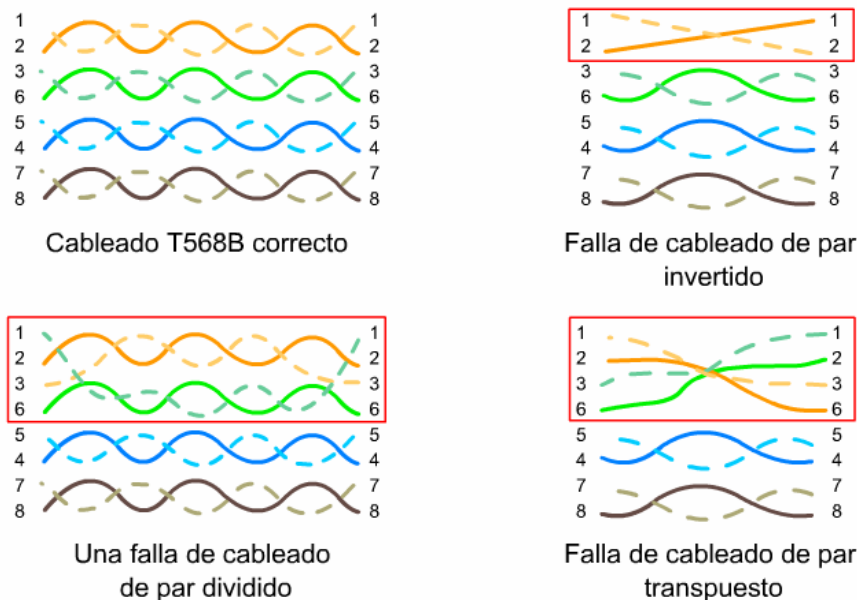


Figura 3

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
- Una analizador de cable mide NEXT aplicando una señal de prueba a un par de cables
- La prueba de telediafonía de igual nivel (ELFEXT) mide FEXT
- La telediafonía de igual nivel de suma de potencia (PSELFEXT) es el efecto combinado de ELFEXT de todos los pares de hilos de todos los pares de hilos

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 amplitud 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.

4.2.7 Parámetros basados en tiempo

El retardo de propagación es una medición simple del tiempo que tarda una señal en recorrer el cable que se está probando. El retardo en un par de hilos depende de su longitud, trenzado y propiedades eléctricas. Los retardos se miden con una precisión de centésimas de nanosegundos. Un nanosegundo es una mil millonésima parte de un segundo, o 0,000000001 segundo. El estándar TIA/EIA-568.B establece un límite para el retardo de propagación para las diversas categorías de UTP.

Las mediciones de retardo de propagación son la base para las mediciones de longitud de cable. El TIA/EIA-568-B.1 especifica que la longitud física del enlace se calcula usando el par de hilos con el menor retardo eléctrico. Los analizadores de cables miden la longitud del hilo en base al retardo eléctrico según la medición de una prueba de Reflectometría en el dominio del tiempo (TDR), y no por la longitud física del revestimiento del cable. Ya que los hilos adentro del cable están trenzados, las señales en realidad recorren una distancia mayor que la longitud del cable. Cuando un analizador de cables realiza una medición TDR, envía una señal de pulso por un par de hilos y mide el tiempo requerido para que el pulso regrese por el mismo par de hilos.

- La demora de propagación es una medición simple del tiempo que tarda una señal en recorrer el cable que se prueba.
- Las demoras se miden con una precisión de centésimas de nanosegundos.
- El estándar TIA/EIA-568-B establece un límite para la demora de propagación para las diversas categorías de UTP.
- La diferencia de retardo entre pares se denomina desajuste por retardo "delay skew".

La prueba TDR se utiliza no sólo para determinar la longitud, sino también para identificar la distancia hasta las fallas de cableado, tales como cortocircuitos y circuitos abiertos. Cuando el pulso encuentra un circuito abierto, un cortocircuito o una conexión deficiente, la totalidad o una parte de la energía del pulso se vuelve a reflejar al analizador de cables. Esto puede ser usado para calcular la distancia aproximada a la falla. La distancia aproximada es útil a la hora de localizar un punto de conexión defectuoso en el recorrido de un cable, como un jack de pared.

Los retardos de propagación de los distintos pares de hilos en un solo cable pueden presentar leves diferencias debido a diferencias en la cantidad de trenzas y propiedades eléctricas de cada par de cables. La diferencia de retardos entre pares se denomina sesgo de retardo. El sesgo de retardo es un parámetro crítico en redes de alta velocidad en las que los datos se transmiten simultáneamente a través de múltiples pares de hilos, tales como Ethernet 1000BASE-T. Si el sesgo de retardo entre los pares es demasiado grande, los bits llegan en momentos diferentes y los datos no se vuelven a ensamblar correctamente. A pesar de que un enlace de cable no es lo que más se ajusta a este tipo de transmisión de datos, la prueba de sesgo de retardo ayuda a garantizar que el enlace admitirá futuras actualizaciones a redes de alta velocidad.

Todos los enlaces de cable en una LAN deben pasar todas las pruebas antes mencionadas, según lo especificado por el estándar TIA/EIA-568.B para ser considerados dentro de los estándares. 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. Las pruebas de cables se deben realizar en el momento de instalar el cable, y a partir de ahí de forma periódica para garantizar que el cableado de la LAN cumpla con los estándares industriales. Se deben utilizar correctamente instrumentos de prueba para cables de buena calidad para garantizar la precisión de dichas pruebas. Además, se deben documentar cuidadosamente los resultados de las pruebas.

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.

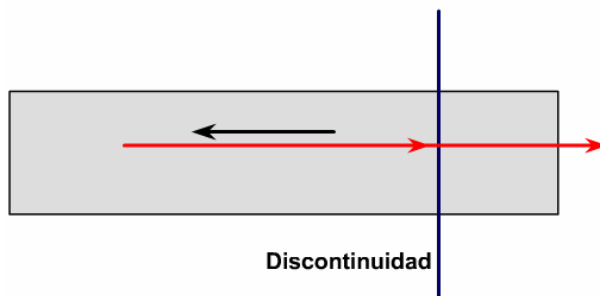


Figura 1

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.

En un enlace de fibra óptica, se debe calcular la cantidad aceptable de pérdida de potencia de señal que puede ocurrir sin que resulte inferior a los requisitos del receptor. A este cálculo se le conoce como presupuesto de pérdida del enlace óptico. Un instrumento para probar fibra, conocido como fuente de luz y medidor de potencia, verifica si el presupuesto de pérdida del enlace óptico ha sido excedido. Si la fibra falla la prueba, se puede usar otro instrumento para probar cables para indicar donde ocurren las discontinuidades ópticas a lo largo de la longitud del enlace de cable. Un TDR óptico conocido como OTDR es capaz de localizar estas discontinuidades. Por lo general, el problema tiene que ver con conectores mal unidos. El OTDR indicará la ubicación de las conexiones defectuosas que se deberán reemplazar. Una vez corregidas las fallas, se debe volver a probar el cable.

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.

Un analizador de cables de buena calidad, similar a la serie Fluke DSP-4000 o Fluke OMNIScanner2 puede realizar todas las mediciones de prueba requeridas para las certificaciones Cat 5, Cat 5e y Cat 6, tanto para enlaces permanentes como en el canal. La figura 1 muestra el Analizador de Cable Fluke DSP-4100 con un adaptador Canal/Tráfico DSP-LIA013 para Cat 5e.



Figura 1

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 sinusoidales son funciones periódicas de variación continua. Las señales analógicas son parecidas a las ondas sinusoidales.
- 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, $10^3 = 10 \times 10 \times 10 = 1000$.
- 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, $\log_{10} 1000 = 3$ porque $10^3 = 1000$.
- 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.

Módulo 5: Cableado de las LAN y las WAN

Descripción general

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. Este módulo presenta información sobre los elementos de las LAN de Ethernet y los dispositivos de LAN más comunes.

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. Este módulo presenta información sobre varios tipos de conexiones WAN.

- Los estudiantes que completen este módulo deberán poder:
- Identificar las características de las redes Ethernet
- Identificar los cables de conexión directa, de conexión cruzada y transpuesto.
- Describir las funciones, ventajas y desventajas de los repetidores, hubs, puentes, switches, y componentes de una red inalámbrica.
- Describir las funciones de las redes de par a par.
- Describir las funciones, ventajas, y desventajas de las redes cliente-servidor.
- Describir y marcar la diferencia entre las conexiones WAN seriales, de Red Digital de Servicios Integrados (RDSI), de Línea Digital del Suscriptor (DSL), y de cable módem.
- Identificar los puertos seriales, cables y conectores del router.
- Identificar y describir la ubicación del equipo usado en las distintas configuraciones WAN.

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. ¹

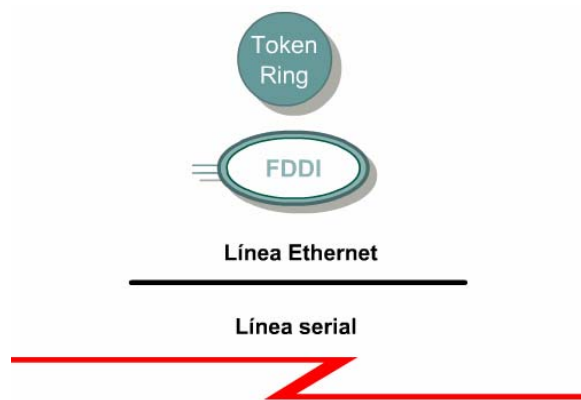


Figura 1

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 2 muestra un subconjunto de implementaciones de la capa física que se pueden implantar para su uso con Ethernet.

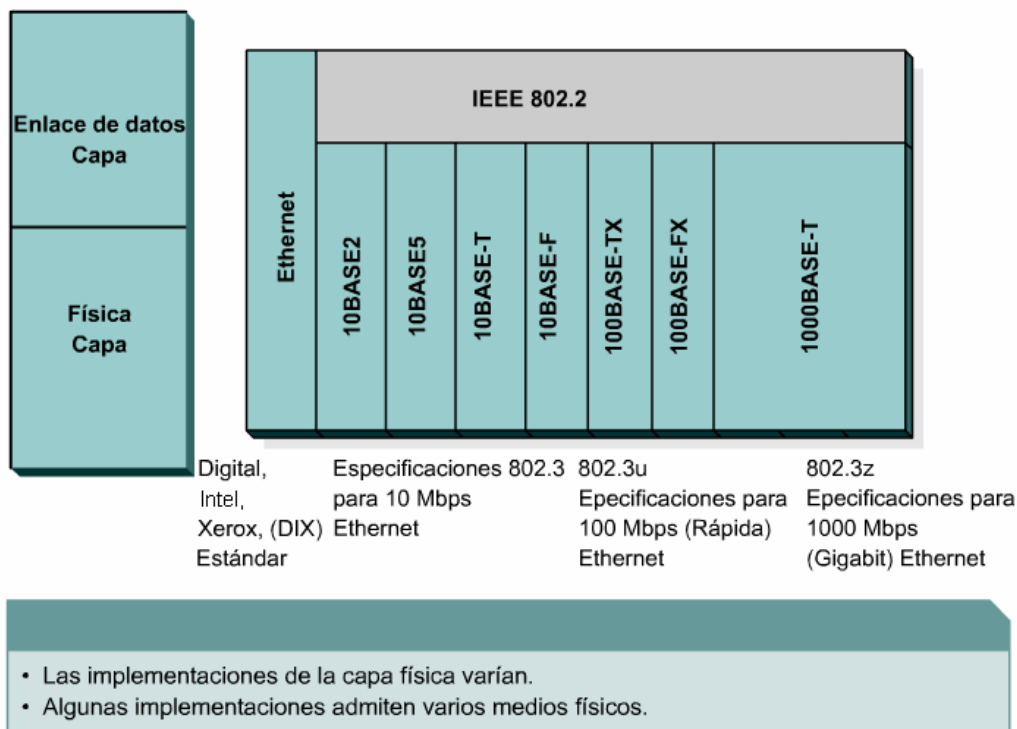


Figura 2

5.1.2 Ethernet en el campus

Ethernet es la tecnología LAN de uso más frecuente. Un grupo formado por las empresas Digital, Intel y Xerox, conocido como DIX, fue el primero en implementar Ethernet. DIX creó e implementó la primera especificación LAN Ethernet, la cual se utilizó como base para la especificación 802.3 del Instituto de Ingenieros Eléctrica y Electrónica (IEEE), publicada en 1980. Más tarde, el IEEE extendió la especificación 802.3 a tres nuevas comisiones conocidas como 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet transmitido en fibra óptica) y 802.3ab (Gigabit Ethernet en UTP).

Los requisitos de la red pueden forzar a la actualización a topologías de Ethernet más rápidas. La mayoría de las redes de Ethernet admiten velocidades de 10 Mbps y 100 Mbps.

La nueva generación de productos para multimedia, imagen y base de datos puede fácilmente abrumar a redes que funcionan a las velocidades tradicionales de Ethernet de 10 y 100 Mbps. Los administradores de red pueden considerar proveer Gigabit Ethernet desde el backbone hasta los usuarios finales. Los costos de instalación de un nuevo cableado y de adaptadores pueden hacer que esto resulte casi imposible. Por el momento, Gigabit Ethernet en el escritorio no constituye una instalación estándar.

Por lo general, las tecnologías Ethernet se pueden utilizar en redes de 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.

	Implementación de Ethernet 10BASE-T	Implementación de Fast Ethernet	Implementación de Gigabit Ethernet
Nivel de usuario final (dispositivo del usuario final al dispositivo de grupo de trabajo)	Proporciona conectividad para aplicaciones de volumen bajo a mediano.	Ofrece a las estaciones de trabajo de PC de alto rendimiento acceso de 100 Mbps al servidor.	No se usa normalmente a ese nivel.
Nivel de grupo de trabajo (dispositivo de grupo de trabajo al backbone)	No se usa normalmente a ese nivel.	Ofrece conectividad entre el usuario final y los grupos de trabajo. Ofrece conectividad desde el grupo de trabajo al backbone. Ofrece conectividad desde el bloque del servidor a la capa de backbone.	Ofrece conectividad de alto rendimiento al bloque del servidor de la empresa.
Nivel de backbone	No se usa normalmente a ese nivel.	Ofrece conectividad desde el bloque del servidor del grupo de trabajo al backbone.	Ofrece conectividad de backbone de alta velocidad y dispositivos de red.

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).

5.1.4 Medios de conexión

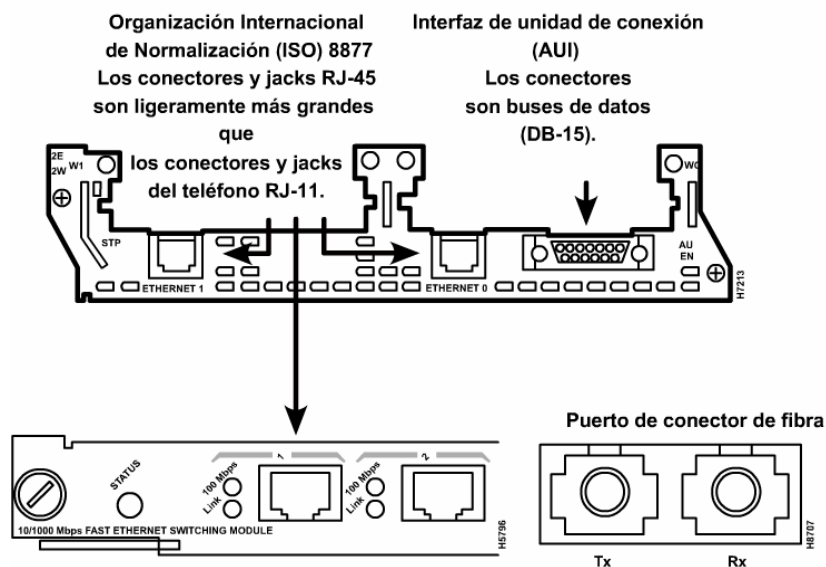


Figura 1

La Figura 1 muestra los diferentes tipos de conexión utilizados en cada implementación de la capa física. El jack y el conector de jack registrado (RJ-45) son los más comunes. En la próxima sección se discuten los conectores RJ-45 con más detalle.

En algunos casos el tipo de conector de la tarjeta de interfaz de red (NIC) no se ajusta al medio al que se tiene que conectar. Como se ve en la Figura 1, puede existir una interfaz para el conector interfaz de unidad de conexión (AUI) de 15 pins. El conector AUI permite que medios diferentes se conecten cuando se usan con el transceptor apropiado. Un transceptor es un adaptador que convierte un tipo de conexión a otra. Por ejemplo, un transceptor convierte un conector AUI en uno RJ-45, coaxial, o de fibra óptica. En Ethernet 10BASE5, o Thicknet, se utiliza un cable corto para conectar el AUI a un transceptor en el cable principal.

5.1.5 Implementación del UTP

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado. El conector transparente RJ-45 muestra ocho hilos de distintos colores. Cuatro de estos hilos conducen el voltaje y se consideran "tip" (punta) (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman "ring" (anillo) (R1 a R4). Tip y ring son términos que surgieron a comienzos de la era de la telefonía. Hoy, estos términos se refieren al hilo positivo y negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente.

El conector RJ-45 es el componente macho, engarzado al extremo del cable. Como se ve en la Figura 1 cuando observa el conector macho de frente, las ubicaciones de los pins están numeradas desde 8, a la izquierda, hasta 1, a la derecha.

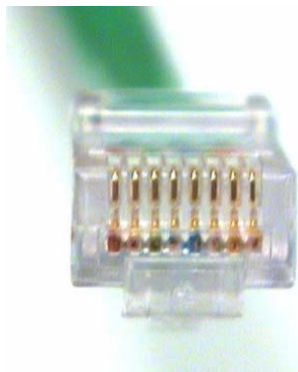


Figura 1



Figura 2

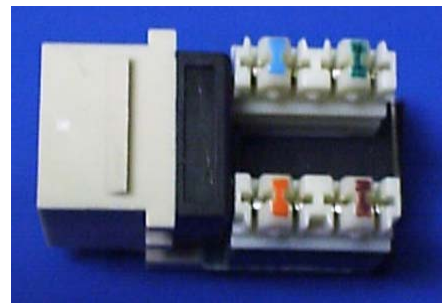


Figura 3

Como se ve en la Figura 2, el jack es el componente femenino en un dispositivo de red, toma de pared o panel de conexión. La Figura 3 muestra las conexiones a presión en la parte posterior del jack donde se conecta el cable Ethernet UTP.

Para que la electricidad fluya entre el conector y el jack, el orden de los hilos debe seguir el código de colores T568A, o T568B recomendado en los estándares EIA/TIA-568-B.1, como se ve en la Figura 4. Identifique la categoría de cableado EIA/TIA correcta que debe usar un dispositivo de conexión, refiriéndose a la documentación de dicho dispositivo, o ubicando alguna identificación en el mismo cerca del jack. Si no se dispone de la documentación o de alguna identificación, use categoría 5E o mayor, dado que las categorías superiores pueden usarse en lugar de las inferiores. Así podrá determinar si va a usar cable de conexión directa (straight-through) o de conexión cruzada (crossover).

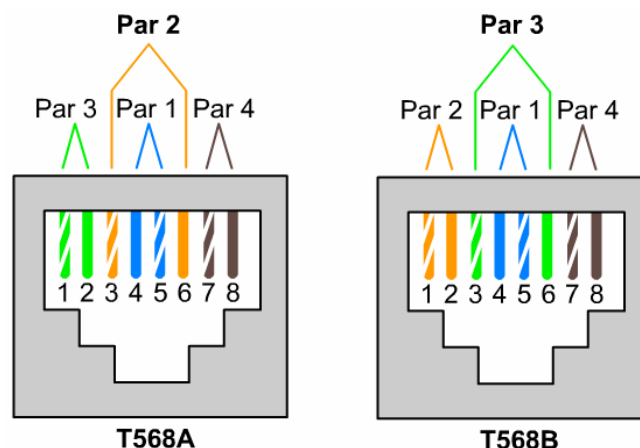


Figura 4

Si los dos conectores de un cable RJ-45 se colocan uno al lado del otro, con la misma orientación, podrán verse en cada uno los hilos de color. Si el orden de los hilos de color es el mismo en cada extremo, entonces el cable es de conexión directa, como se observa en la Figura 5.



Figura 5

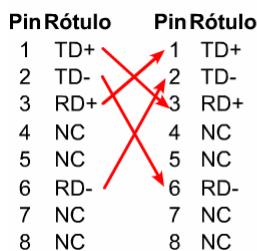
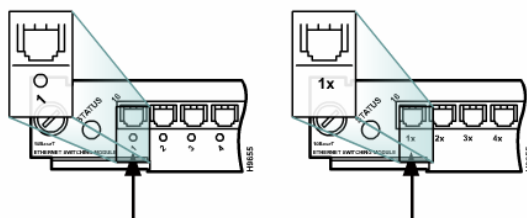


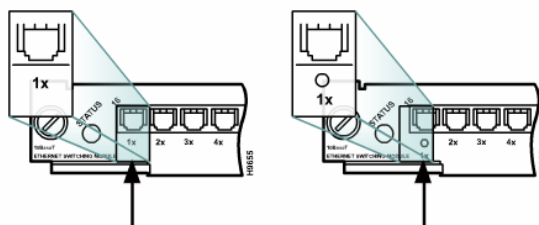
Figura 6

En un cable de conexión cruzada, los conectores RJ-45 de ambos extremos muestran que algunos hilos de un extremo del cable están cruzados a un pin diferente en el otro extremo del cable. La Figura 6 muestra que los pins 1 y 2 de un conector se conectan respectivamente a los pins 3 y 6 de otro.

La Figura 7 da las pautas de qué tipo de cable se debe utilizar cuando se interconecten dispositivos de Cisco.



Se usa un cable de conexión directa sólo cuando un puerto se encuentra designado con una "x".



Se usa un cable de conexión cruzada cuando AMBOS puertos están designados con una "x" o cuando ninguno de los puertos está designado con una "x".

Figura 7

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

La Figura 8 ilustra cómo una red determinada puede requerir una variedad de tipos de cable. La categoría de cable UTP requerida depende del tipo de Ethernet que se elija.

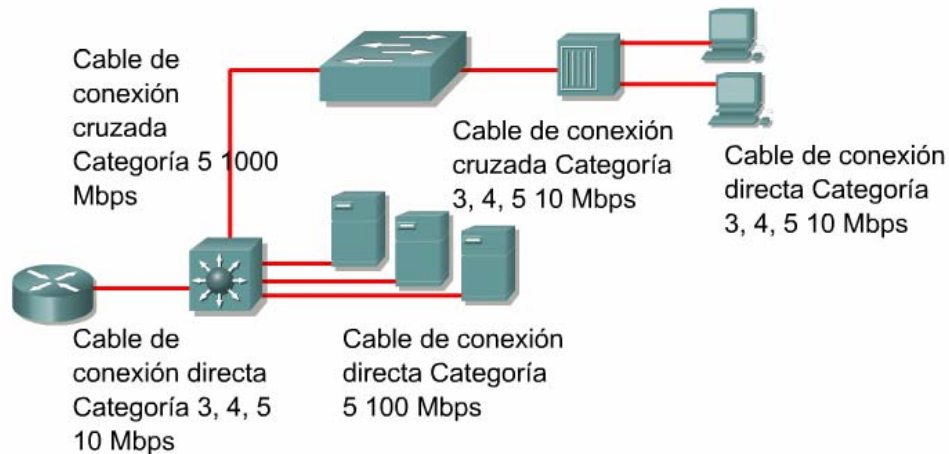


Figura 8

5.1.6 Repetidores

El término repetidor proviene de los inicios de las comunicaciones de larga distancia. El término describe una situación en la que una persona en una colina repite la señal que acababa de recibir de otra persona ubicada en una colina anterior. El proceso se repetía hasta que el mensaje llegaba a destino. El telégrafo, el teléfono, las microondas, y las comunicaciones por fibra óptica usan repetidores para fortalecer la señal enviada a través de largas distancias.

Un repetidor recibe una señal, la regenera, y la transmite. El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. En Ethernet e IEEE 802.3 se implementa la "regla 5-4-3", en referencia al número de repetidores y segmentos en un Backbone de acceso compartido con topología de árbol. La "regla 5-4-3 divide la red en dos tipos de segmentos físicos: Segmentos Poblados (de usuarios), y Segmentos no Poblados (enlaces). En los segmentos poblados se conectan los sistemas de los usuarios. Los segmentos no poblados se usan para conectar los repetidores de la red entre sí. La regla manda que entre cualquiera dos nodos de una red, puede existir un máximo de cinco segmentos, conectados por cuatro repetidores o concentradores, y solamente tres de los cinco segmentos pueden tener usuarios conectados a los mismos. El protocolo Ethernet requiere que una señal enviada en la LAN alcance cualquier parte de la red dentro de una longitud de tiempo especificada. La "regla 5-4-3" asegura que esto pase. Cada repetidor a través del cual pasa la señal añade una pequeña cantidad de tiempo al proceso, por lo que la regla está diseñada para minimizar el tiempo de transmisión de la señal. Demasiada latencia en la LAN incrementa la cantidad de colisiones tardías, haciendo la LAN menos eficiente.

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:

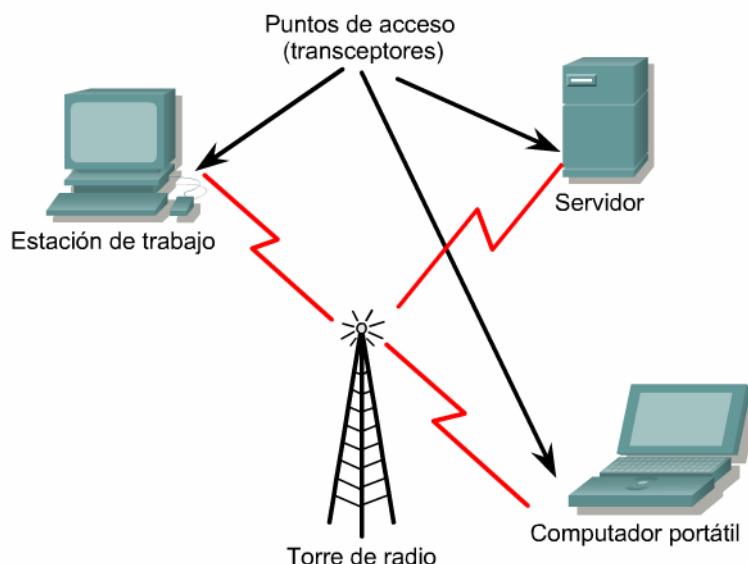
- **Pasivo:** Un hub pasivo sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un hub pasivo se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.
- **Activo:** Se debe conectar un 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 computador a otro sin una conexión de cable permanente. El único cableado permanente es el necesario para conectar los puntos de acceso de la red. Las estaciones de trabajo dentro del ámbito de la red inalámbrica se pueden trasladar con facilidad sin tener que conectar y reconectar al cableado de la red. Una aplicación común de la comunicación inalámbrica de datos es la que corresponde a los usuarios móviles. Algunos ejemplos de usuarios móviles incluyen las personas que trabajan a distancia, aviones, satélites, las sondas espaciales remotas, naves espaciales y estaciones espaciales.



En el centro de la comunicación inalámbrica están los dispositivos llamados transmisores y receptores. El transmisor convierte los datos fuente en ondas electromagnéticas (EM) que pasan al receptor. El receptor entonces transforma de nuevo estas ondas electromagnéticas en datos para el destinatario. Para una comunicación de dos vías, cada dispositivo requiere de un transmisor y un receptor. Muchos de los fabricantes de dispositivos para networking construyen el transmisor y el receptor en una sola unidad llamada transceptor o tarjeta de red inalámbrica. Todos los dispositivos en las LAN inalámbrica (WLAN) deben tener instalada la tarjeta apropiada de red inalámbrica.

Las dos tecnologías inalámbricas más comunmente usadas para networking son IR y RF. La tecnología de IR tiene sus puntos débiles. Las estaciones de trabajo y los dispositivos digitales deben estar en la línea de vista del transmisor para operar. Las redes basadas en infrarrojo se acomodan a entornos donde todos los dispositivos digitales que requieren conectividad de red se encuentran en una habitación. La tecnología IR de networking se puede instalar rápidamente, pero las personas que cruzan la habitación, o el aire húmedo pueden debilitar u obstruir las señales de datos. Sin embargo, se están desarrollando nuevas tecnologías que pueden funcionar fuera de la vista.

La tecnología de radiofrecuencia permite que los dispositivos se encuentren en habitaciones o incluso en edificios diferentes. El rango limitado de señales de radio restringe el uso de esta clase de red. La tecnología de RF puede utilizar una o varias frecuencias. Una radiofrecuencia única está sujeta a interferencias externas y a obstrucciones geográficas. Además, una sola frecuencia es fácil de monitorear, lo que hace que la transmisión de datos no sea segura. La técnica del espectro disperso evita el problema de la transmisión insegura de datos porque usa múltiples frecuencias para aumentar la inmunidad al ruido y hace que sea más difícil que intrusos intercepten la transmisión de los datos.

En la actualidad se utilizan dos enfoques para implementar el espectro disperso para transmisiones de WLAN. Uno es el Espectro Disperso por Salto de Frecuencia (FHSS) y el otro es el Espectro Disperso de Secuencia Directa (DSSS). Los detalles técnicos del funcionamiento de estas tecnologías exceden el alcance de este curso.

5.1.9 Puentes

A veces, es necesario dividir una LAN grande en segmentos más pequeños que sean más fáciles de manejar. ¹ Esto disminuye la cantidad de tráfico en una sola LAN y puede extender el área geográfica más allá de lo que una sola LAN puede admitir. Los dispositivos que se usan para conectar segmentos de redes son los puentes, switches, routers y gateways. 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.

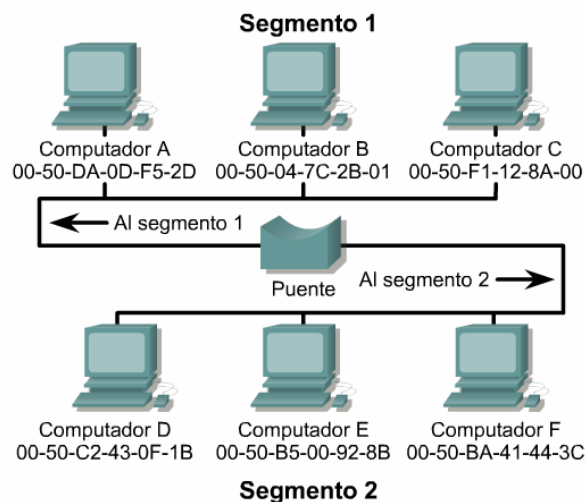


Figura 1

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. Al igual que los puentes, los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red. ¹

Aunque hay algunas similitudes entre los dos, un switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino. Un switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los switches Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los switches mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

Interfaz	Dirección MAC
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444

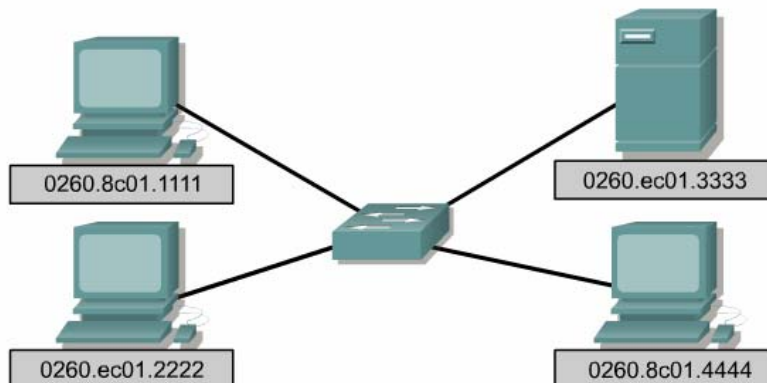


Figura 1

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento con un mínimo de intrusión en la red ya existente.

Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. La conmutación de las tramas de datos es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida. El segundo es el mantenimiento de operaciones de conmutación cuando los switch crean y mantienen tablas de conmutación y buscan loops.

Los switches operan a velocidades mucho más altas que los puentes y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales.

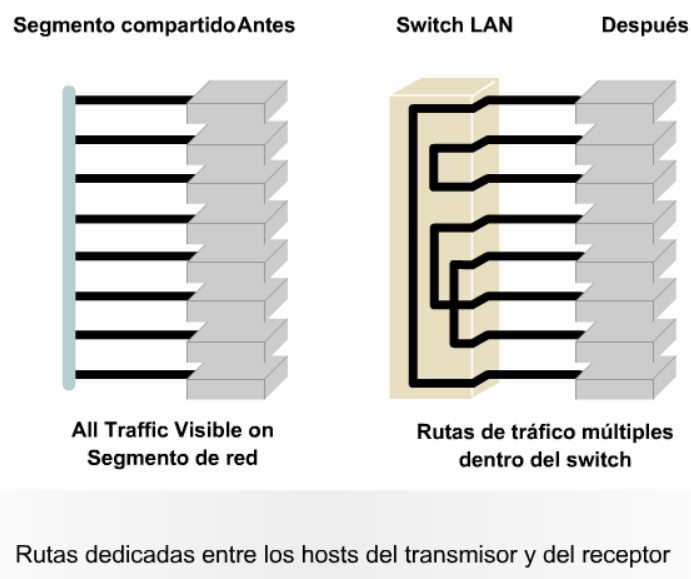


Figura 2

Un switch Ethernet ofrece muchas ventajas. Un beneficio es que un switch para Ethernet permite que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales y segmentos de red dedicados en un entorno virtualmente sin colisiones. ²Esto aumenta al máximo el ancho de banda disponible en el medio

compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar.

5.1.11 Conectividad del host

La función de una NIC es conectar un dispositivo host al medio de red. Una NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard o dispositivo periférico de un computador. La NIC también se conoce como adaptador de red. En los computadores portátiles o de mano, una NIC tiene el tamaño de una tarjeta de crédito.

Las NIC se consideran dispositivos Capa 2 porque cada NIC lleva un identificador exclusivo codificado, denominado dirección MAC. Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Posteriormente se suministrarán más detalles acerca de la dirección MAC. Tal como su nombre lo indica, la tarjeta de interfaz de red controla el acceso del host al medio.

En algunos casos, el tipo de conector de la NIC no concuerda con el tipo de medios con los que debe conectarse. Un buen ejemplo de ello es el router Cisco 2500. En el router, se ve un conector AUI. Ese conector AUI necesita conectarse a un cable Ethernet UTP Categoría 5. Para hacer esto, se usa un transmisor/receptor, también conocido como transceptor. El transceptor convierte un tipo de señal o conector en otro. Por ejemplo, un transceptor puede conectar una interfaz AUI de 15 pins a un jack RJ-45. Se considera un dispositivo de Capa 1, dado que sólo analiza los bits y ninguna otra información acerca de la dirección o de protocolos de niveles más altos.

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, muchos computadores se interconectan para brindar servicios a sus usuarios. Para lograrlo, los computadores en red toman diferentes roles o funciones entre sí. ¹Algunos tipos de aplicaciones requieren que los computadores funcionen como socios en partes iguales. Otro tipo de aplicaciones distribuyen sus tareas de modo que las funciones de un computador sirvan a una cantidad de otros de manera desigual. En cualquiera de los casos, dos computadores por lo general se comunican entre sí usando protocolos petición/respuesta. Un computador realiza una petición de servicio, y el segundo computador lo recibe y responde. El que realiza la petición asume el papel de cliente, y el que responde el de servidor.

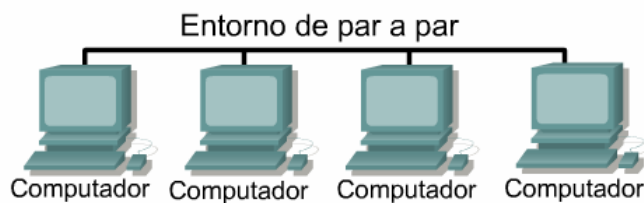


Figura 1

En una red de par a par, los computadores en red actúan como socios en partes iguales, o pares. Como pares, cada computador puede tomar la función de cliente o de servidor. ¹En algún momento, el computador A pedirá un archivo al computador B, el cual responderá entregándole el archivo al computador A. El computador A funciona como cliente, mientras que el B funciona como servidor. Más tarde, los computadores A y B cambiarán de papel.

En una red de par a par, los usuarios individuales controlan sus propios recursos. Los usuarios pueden decidir compartir ciertos archivos con otros usuarios. ² ³ 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. Cuando un computador actúa como servidor, es posible que el usuario de ese equipo note que el rendimiento es menor, ya que el equipo cumple las peticiones realizadas por otros sistemas.

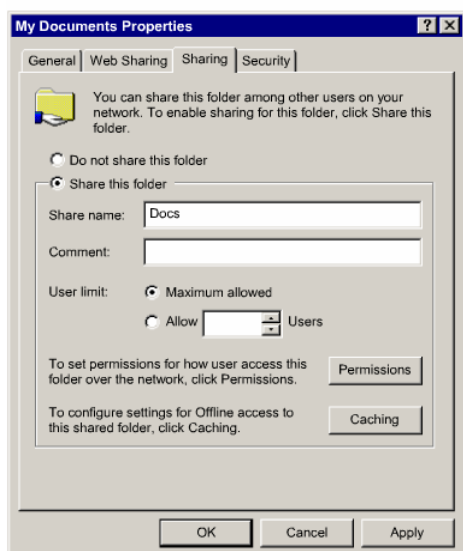


Figura 2

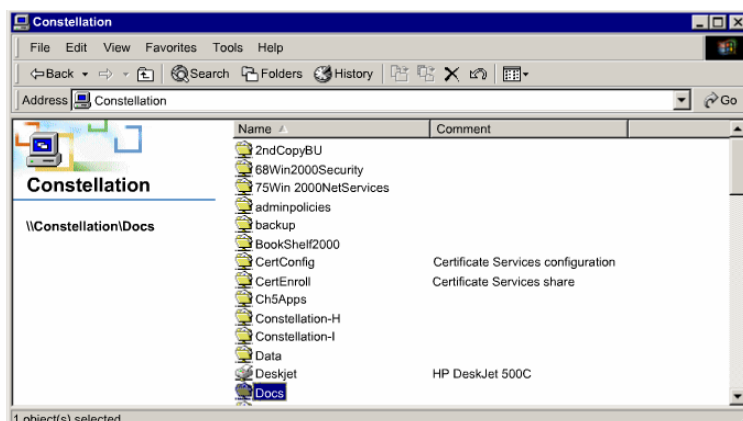


Figura 3

Las redes de par a par son relativamente fáciles de instalar y operar. No se necesita más equipo que un sistema operativo adecuado en cada computador. Como los usuarios controlan sus propios recursos, no se necesitan administradores dedicados.

A medida que la red crece, las relaciones de par a par se hacen cada vez más difíciles de coordinar. Una red de par a par funciona bien con 10 computadores o menos. Ya que las redes de par a par no se adaptan bien a mayores tamaños, su eficiencia disminuye a medida que el número de computadores en la red aumenta. Además, los usuarios individuales controlan el acceso a los recursos de sus computadores, lo que implica que la seguridad se hace difícil de mantener. El modelo cliente/servidor de networking se puede usar para superar las limitaciones de la red de par a par.

5.1.13 Cliente/servidor

En una disposición cliente/servidor, los servicios de red se ubican en un computador dedicado denominado servidor. El servidor responde a las peticiones de los clientes. ¹El servidor es un computador central que se encuentra disponible de forma continua para responder a las peticiones de los clientes, ya sea de un archivo, impresión, aplicación u otros servicios. La mayoría de los sistemas operativos adoptan la forma de relación cliente/servidor. En general, los computadores de escritorio funcionan como clientes y uno o más computadores con potencia de procesamiento adicional, memoria y software especializado funcionan como servidores. ²

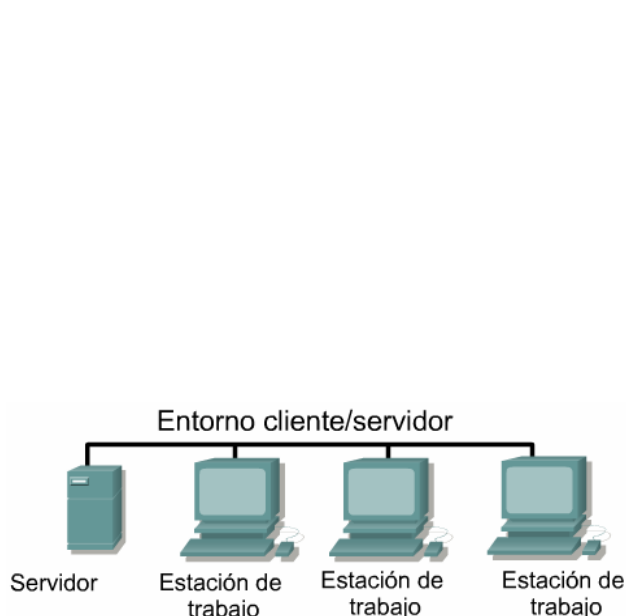


Figura 1

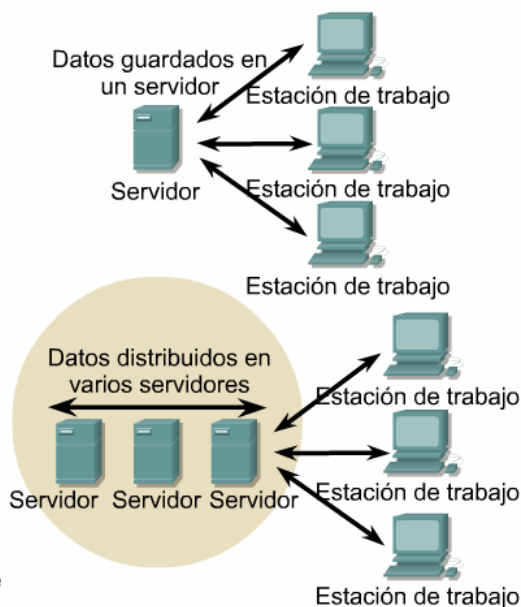


Figura 2

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.

Ventajas de la Red de par a par	Ventajas de la Red cliente/servidor
Su implementación es menos costosa.	Ofrece mejor seguridad.
No requiere software de administración de red especializado	Es más fácil de administrar cuando la red es grande porque la administración se encuentra centralizada.
No requiere un administrador de red dedicado.	Todos los datos pueden copiarse en una ubicación central.

Figura 3

Desventajas de la Red de par a par	Desventajas de Red cliente/servidor
No se amplía bien y en las redes grandes la administración se vuelve inmanejable.	Necesita costoso software administrativo y operacional de red especializado
Es necesario capacitar a cada uno de los usuarios para realizar tareas administrativas.	Necesita hardware más potente y costoso para la máquina del servidor.
Es menos segura.	Requer um administrador profissional
Todas las máquinas comparten los recursos, lo que perjudica el rendimiento.	Tiene un solo punto de falla. Los datos del usuario no están disponibles si el servidor está desactivado.

Figura 4

Las Figuras 3 y 4 resumen las ventajas y desventajas comparativas entre los sistemas de par a par y cliente-servidor.

5.2 Cableado WAN

5.2.1 Capa física de las WAN

La implementación de la capa física varía según la distancia que haya entre el equipo y los servicios, la velocidad, y el tipo de servicio en sí. 1 Las conexiones seriales se usan para admitir los servicios WAN tales como líneas dedicadas arrendadas que usan el protocolo punto a punto (PPP) o de Frame Relay La velocidad de estas conexiones va desde los 2400 bits por segundo (bps) hasta el servicio T1 a 1544 megabits por segundo (Mbps) y el servicio E1 a 2048 megabits por segundo (Mbps).

Cisco HDLC	PPP	Frame Relay	ISDN BRI	Módem DSL	Módem por cable
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 Interfaz serial de alta velocidad (HSSI)			RJ-45 Nota: Las salidas de pin de BRI RDSI se diferencian de las salidas de pin para Ethernet	RJ-11 Nota: Funciona a través de la línea telefónica	F Nota: Funciona a través de la línea de TV por cable

- La implementación de la capa física varía. - Las especificaciones de cable definen la velocidad del enlace

Figura 1

RDSI ofrece conexiones conmutadas por demanda o servicios de respaldo conmutados. La interfaz de acceso básico (BRI) RDSI está compuesta de dos canales principales de 64 kbps (canales B) para datos, un canal delta (canal D) de 16 kbps que se usa para señalar y para otras tareas de administración del enlace. PPP se utiliza por lo general para transportar datos en los canales B.

Con la creciente demanda de servicios residenciales de banda ancha de alta velocidad, las conexiones de DSL y cable módem se están haciendo más populares. Por ejemplo, un servicio DSL residencial puede alcanzar velocidades T1/E1 con la línea telefónica existente. Los servicios de cable utilizan la línea de cable coaxial del televisor. Una línea de cable coaxial provee una conectividad de alta velocidad que iguala o excede aquella de DSL. En un módulo posterior se presentará una explicación detallada de los servicios de DSL y cable módem.

5.2.2 Conexiones seriales de WAN

Para las comunicaciones de larga distancia, las WAN utilizan transmisiones seriales. Este es un proceso por el cual los bits de datos se envían por un solo canal. Este proceso brinda comunicaciones de larga distancia confiables y el uso de un rango específico de frecuencias ópticas o electromagnéticas.

Las frecuencias se miden en términos de ciclos por segundo y se expresan en Hercios (Hz). Las señales que se transmiten a través de las líneas telefónicas de grado de voz utilizan 4 kilohercios (KHz). El tamaño del rango de frecuencia se denomina ancho de banda. En el networking, el ancho de banda es la medida de bits por segundo que se transmite. ¹

Datos (bps)	Distancia (Metros) EIA/TIA-232	Distancia (Metros) EIA/TIA-449
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1 (1.544 Mbps)	—	15

Figura 1

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. ²

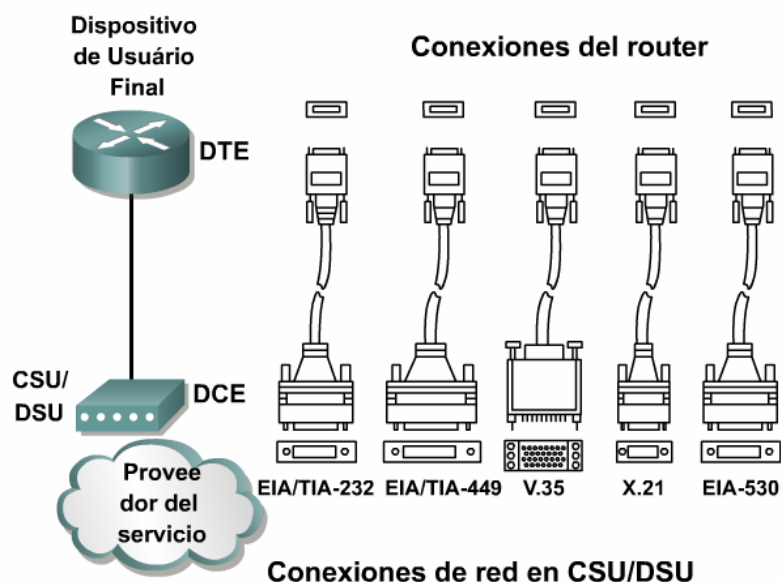


Figura 2

Si la conexión se hace directamente con el proveedor de servicio, o con un dispositivo que provee señal de temporización tal como la unidad de servicio de canal/datos (CSU/DSU), el router será un equipo terminal de datos (DTE) y usará cable serial DTE. Por lo general, este es el caso. Sin embargo, hay situaciones en las que se requiere que el router local brinde la temporización y entonces utilizará un cable para equipo de comunicación de datos (DCE). En las prácticas de laboratorio incluidas en el currículo, uno de los routers conectados necesitará brindar la función de temporización. Por lo tanto, la conexión estará formada por un cable DCE y DTE.

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.

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. ¹En general, esta es la forma de conectar los routers. Sin embargo, hay casos en que los routers tendrán que actuar como DCE. Al armar un escenario de routers conectados espalda contra espalda en un ámbito de prueba, uno de los routers debe ser DTE y el otro DCE. ²

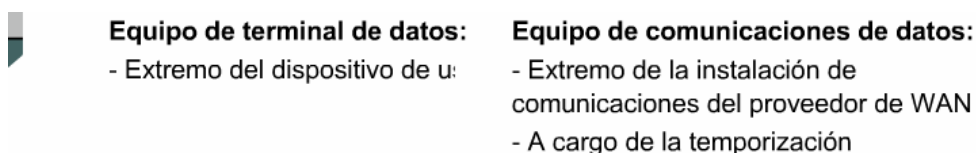


Figura 1

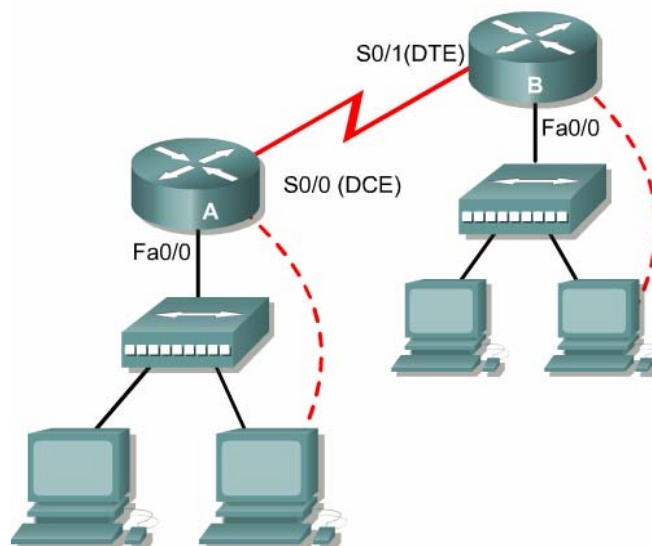


Figura 2

Al cablear routers para obtener conectividad serial, los routers tendrán puertos fijos o modulares. El tipo de puerto que se utilice afectará la sintaxis que se use posteriormente para configurar cada interfaz.

Las interfaces de los routers que tienen puertos seriales fijos están rotuladas según tipo y número de puerto.

3

Router Cisco 2503-Vista posterior

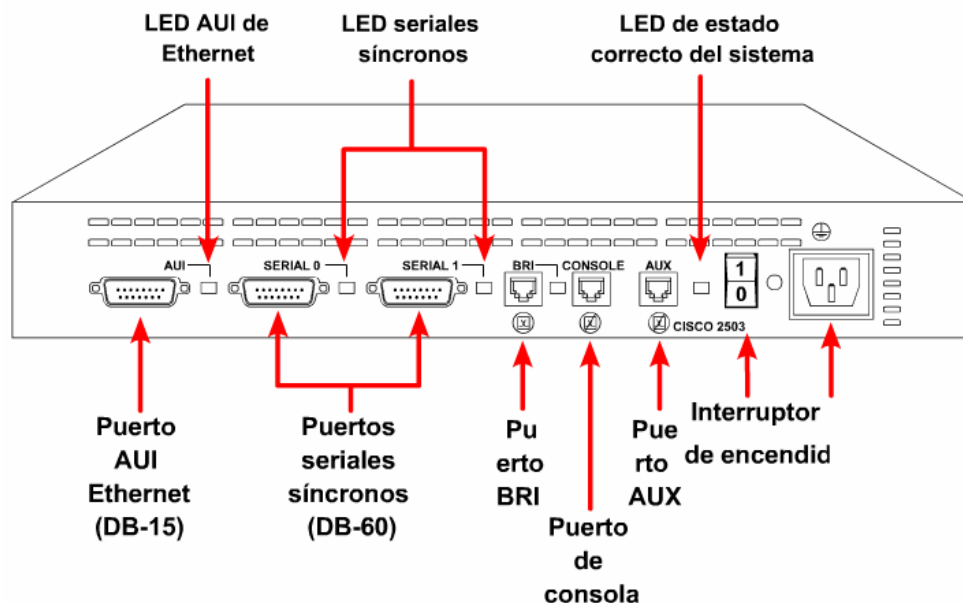


Figura 3

Las interfaces de los routers que tienen puertos seriales modulares se rotulan según el tipo de puerto, ranura y número de puerto. 4 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.

Los puertos seriales de WAN pueden ser modulares.

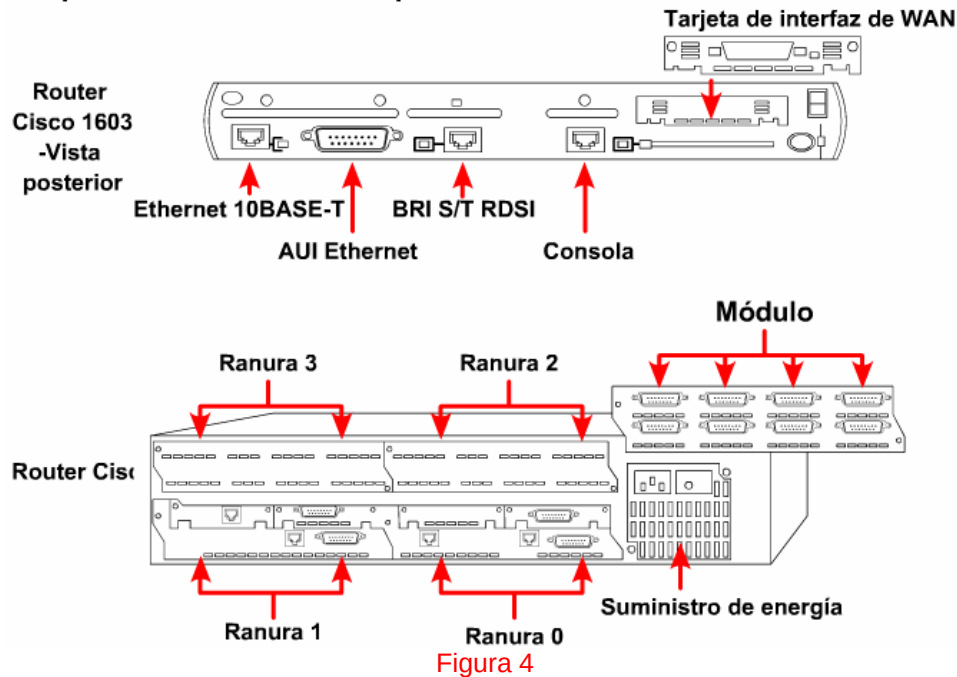


Figura 4

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.

Un NT1 es un dispositivo intermedio ubicado entre el router y el switch del proveedor de servicios RDSI. Se utiliza NT1 para conectar el cableado de cuatro hilos del abonado con el loop local de dos hilos convencional. En América del norte, el cliente por lo general provee el NT1, mientras que en el resto del mundo el proveedor de servicios se encarga del dispositivo NT1.

Puede ser necesario colocar un NT1 externo si el dispositivo no está integrado al router. Revisar los rótulos de las interfaces de router es por lo general la manera más fácil de determinar si el router cuenta con un NT1 integrado. Una interfaz BRI con un NT1 integrado tiene el rótulo BRI U mientras que la interfaz BRI sin un NT1 integrado tiene el rótulo BRI S/T. Debido a que los routers pueden tener muchos tipos de interfaz RDSI, es necesario determinar qué tipo de interfaz se necesita al comprar el router. Se puede determinar el tipo de interfaz BRI al mirar el rótulo del puerto. ¹Para interconectar el puerto BRI RDSI al dispositivo del proveedor de servicios, utilice un cable de conexión directa UTP de Categoría 5.

Determinar si se necesita una interfaz BRI S/T o U.

Los routers tienen uno o ambos tipos de puerto.

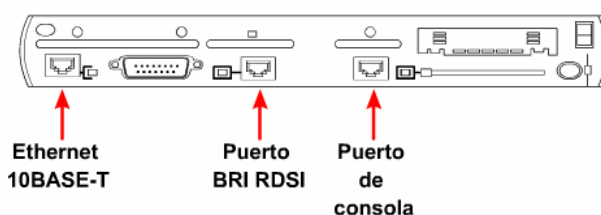
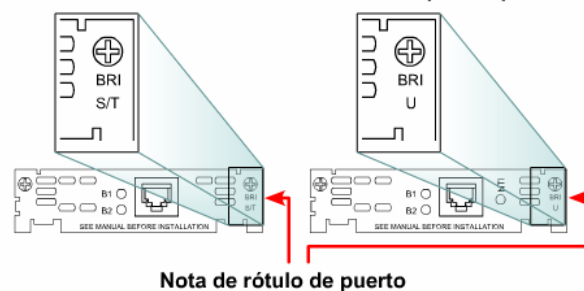


Figura 1

PRECAUCIÓN:

Es importante que inserte el cable que va desde un puerto BRI RDSI a un jack RDSI o switch RDSI solamente. BRI RDSI utiliza voltajes que pueden dañar seriamente los dispositivos que no son de RDSI.

5.2.5 Conexiones DSL y routers

El router ADSL Cisco 827 posee una interfaz de línea de suscripción digital asimétrica (ADSL). ¹Para 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.

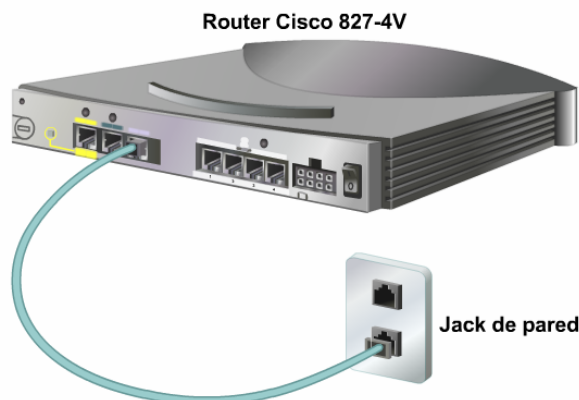


Figura 1

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 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.

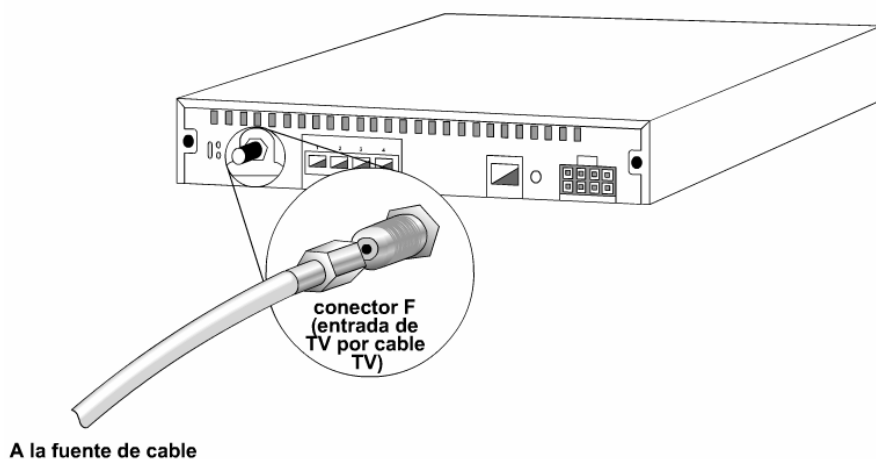


Figura 1

Siga los siguientes pasos para conectar el router de acceso al cable uBR905 de Cisco al sistema de cable:

- Verifique que el router no esté conectado a la alimentación eléctrica.
- Ubique el cable coaxial de RF que sale de la toma de pared para cable coaxial (de TV).
- Instale el divisor de señal/ acoplador direccional, si fuera necesario, para separar las señales para uso del televisor y del computador. Si fuera necesario, también instale un filtro de paso alto para evitar las interferencias entre las señales de TV y del computador.

- Conecte el cable coaxial al conector F del router. 1 Ajuste el conector con los dedos, luego apriétalo dándole un 1/6 de vuelta con una llave.
- Asegúrese de que todos los otros conectores del cable coaxial, todos los divisores intermedios, acopladores, o conexiones a tierra, estén bien ajustados desde la distribución hasta el router uBR905 de Cisco.

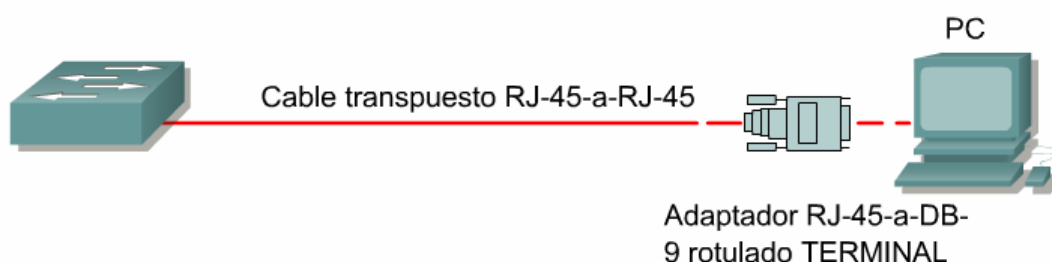
PRECAUCIÓN:

No ajuste el conector excesivamente. Si lo ajusta excesivamente lo puede romper. No utilice una llave de torsión porque se corre el riesgo de ajustar el conector más de 1/6 de vuelta, que es lo que se recomienda una vez que se haya ajustado con los dedos.

5.2.7 Configuración de las conexiones de la consola

Para configurar inicialmente un dispositivo Cisco, se debe conectar directamente una conexión para administración al dispositivo. Para los equipos Cisco esta conexión para administración recibe el nombre de puerto de consola. Este puerto de consola permite monitorear y configurar un hub, switch o router Cisco.

Dispositivo con consola



- Los PC requieren un adaptador de RJ-45 a DB-9 o RJ-45 a DB-25.
- Las configuraciones de puerto COM son 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, sin control de flujo.
- Esto proporciona acceso de consola fuera de banda.
- El puerto de switch AUX se puede usar para una consola conectada por módem.

Figura 1

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

Resumen

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

- La tarjeta de interfaz de red (NIC) proporciona las capacidades de comunicación de red hacia y desde un PC.
- Use un cable de conexión cruzada para conectar dos dispositivos similares, tales como los switch, routers, PC y hubs.
- Use un cable de conexión directa para conectar diferentes tipos de dispositivos tales como las conexiones entre un switch y un router, un switch y un PC o un hub y un router.
- Existen dos tipos principales de LAN, de par a par y de cliente/servidor.
- Las WAN utilizan transmisión serial de datos. Los tipos de conexión de WAN incluyen: RDSI, DSL y cable módem.
- Un router es, en general, el DTE y necesita un cable serial para conectarse a un dispositivo DCE como un CSU/DSU.
- El BRI RDSI tiene dos tipos de interfaces: las S/T y las U. Para interconectar el puerto BRI RDSI al dispositivo del proveedor de servicios, se utiliza un cable de conexión directa UTP de Categoría 5 con conectores RJ-45.
- Un cable telefónico y un conector RJ-11 se usan para conectar un router para obtener servicio DSL.
- El cable coaxial y el conector BNC se usan para conectar el router en un sistema de cable.
- El cable transpuesto se usa para conectar una terminal y un puerto de consola de un dispositivo de internetworking.

Módulo 6: Principios básicos de Ethernet

Descripción general

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 es 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.

Los estudiantes que completen este módulo deberán poder:

- Describir los principios básicos de la tecnología de Ethernet.
- Explicar las reglas de denominación de la tecnología de Ethernet.
- Definir cómo interactúan Ethernet y el modelo OSI.
- Describir el proceso de entramado de Ethernet y la estructura de la trama.
- Nombrar las denominaciones de los campos de Ethernet y su propósito.
- Identificar las características del CSMA/CD.
- Describir los aspectos claves de la temporización de Ethernet, espacio entre tramas y tiempo de postergación después de una colisión.
- Definir los errores y las colisiones de Ethernet.
- Explicar el concepto de auto-negociación en relación con la velocidad y el duplex.

6.1 Principios básicos de Ethernet

6.1.1 Introducción a Ethernet

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

El éxito de Ethernet se debe a los siguientes factores:

- Sencillez y facilidad de mantenimiento.
- Capacidad para incorporar nuevas tecnologías.
- Confiabilidad
- Bajo costo de instalación y de actualización.

Con la llegada de Gigabit Ethernet, lo que comenzó como una tecnología LAN ahora se extiende a distancias que hacen de Ethernet un estándar de red de área metropolitana (MAN) y red de área amplia (WAN).

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

La primera LAN del mundo fue la versión original de Ethernet. Robert Metcalfe y sus compañeros de Xerox la diseñaron hace más de treinta años. El primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Company, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto. Los primeros productos que se desarrollaron utilizando el estándar de Ethernet se vendieron a principios de la década de 1980. Ethernet transmitía a una velocidad de hasta 10 Mbps en cable coaxial

grueso a una distancia de hasta 2 kilómetros (Km). Este tipo de cable coaxial se conocía como thicknet (red con cable grueso) y tenía el ancho aproximado de un dedo pequeño.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el modelo OSI de la Organización Internacional de Estándares (ISO). Por eso, el estándar IEEE 802.3 debía cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

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

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

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

El estándar original de Ethernet ha sufrido una cantidad de enmiendas con el fin de administrar nuevos medios y mayores velocidades de transmisión. Estas enmiendas sirven de estándar para las tecnologías emergentes y para mantener la compatibilidad entre las variaciones de Ethernet.

6.1.2 Reglas del IEEE para la denominación de Ethernet

Ethernet no es una tecnología para networking, sino una familia de tecnologías para networking que incluye Legacy, Fast Ethernet y Gigabit Ethernet. Las velocidades de Ethernet pueden ser de 10, 100, 1000 ó 10000 Mbps. El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet.

Cuando es necesario expandir Ethernet para agregar un nuevo medio o capacidad, el IEEE publica un nuevo suplemento del estándar 802.3. Los nuevos suplementos reciben una designación de una o dos letras, como por ejemplo: 802.3u. También se asigna una descripción abreviada (identificador) al suplemento. ¹

Velocidad	Método de señalización	Medio
10	BASE	2
100	BROAD	5
1000		-T
10G		-TX
		-SX
		-LX

Figura 1

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. El IEEE no puede forzar a los fabricantes de equipamiento para networking a cumplir con todas las particularidades de ningún estándar. El IEEE espera que se logre lo siguiente:

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

6.1.3 Ethernet y el modelo OSI

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física. ¹

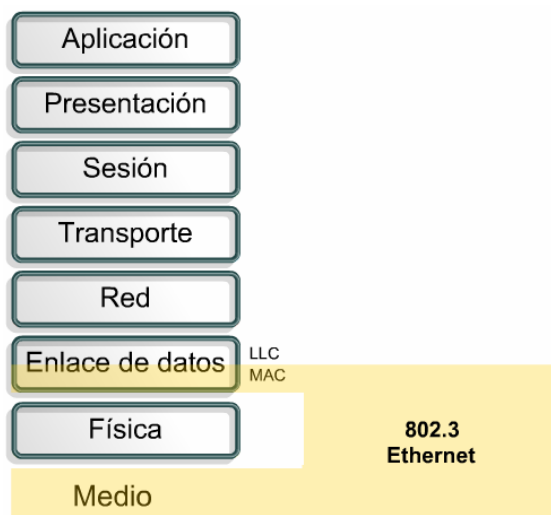


Figura 1

Para mover datos entre una estación Ethernet y otra, a menudo, estos pasan a través de un repetidor. Todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor. ² Un dominio de colisión es entonces un recurso compartido. Los problemas que se originan en una parte del dominio de colisión generalmente tienen impacto en todo el dominio.

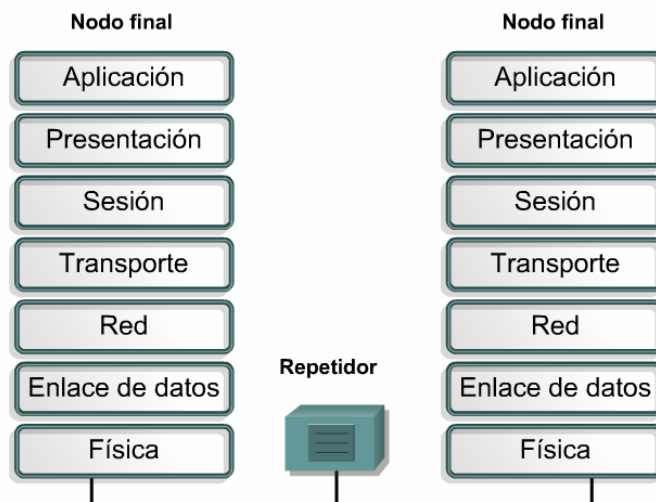


Figura 2

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 dominio de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes.

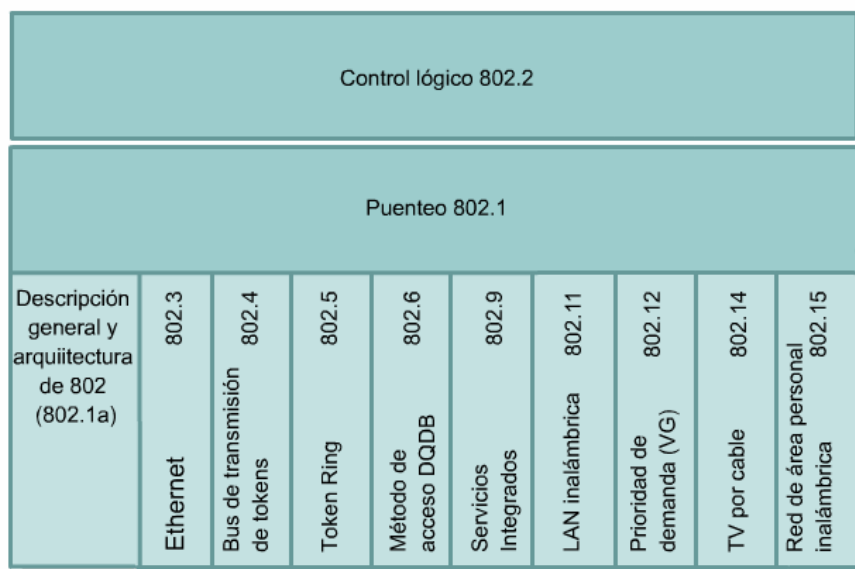


Figura 3

La Figura 3 relaciona una variedad de tecnologías Ethernet con la mitad inferior de la Capa 2 y con toda la Capa 1 del modelo OSI. Ethernet en la Capa 1 incluye las interfaces con los medios, señales, corrientes de bits que se transportan en los medios, componentes que transmiten la señal a los medios y las distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones. La Capa 2 se ocupa de estas limitaciones.

4

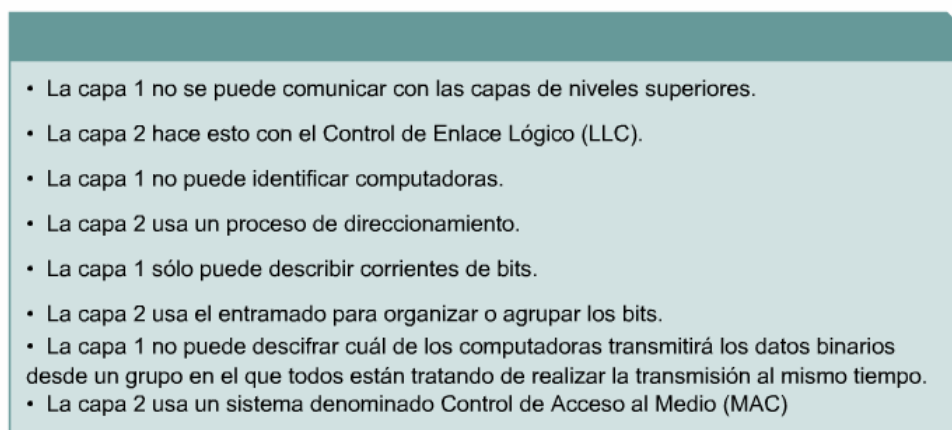


Figura 4

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

La Figura 5 relaciona una variedad de tecnologías Ethernet con la mitad inferior de la Capa 2 y con toda la Capa 1 del modelo OSI. Aunque hay otras variedades de Ethernet, las que se muestran son las de uso más difundido.

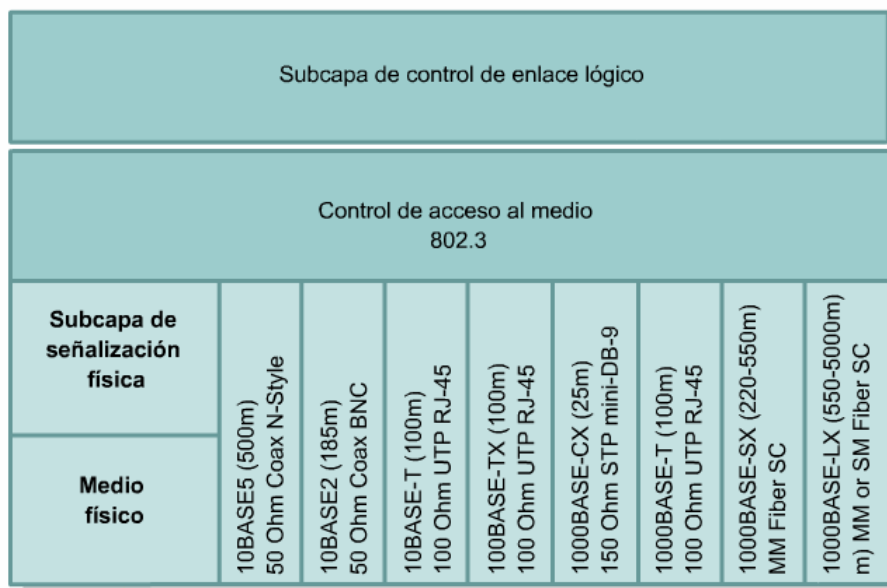


Figura 5

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 computadores y las interfaces de manera exclusiva. 1 Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales. Los primeros seis dígitos hexadecimales, que IEEE administra, identifican al fabricante o al vendedor. Esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI). Los seis dígitos hexadecimales restantes representan el número de serie de la interfaz u otro valor administrado por el proveedor mismo del equipo. 2 Las direcciones MAC a veces se denominan direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la NIC.



Figura 1

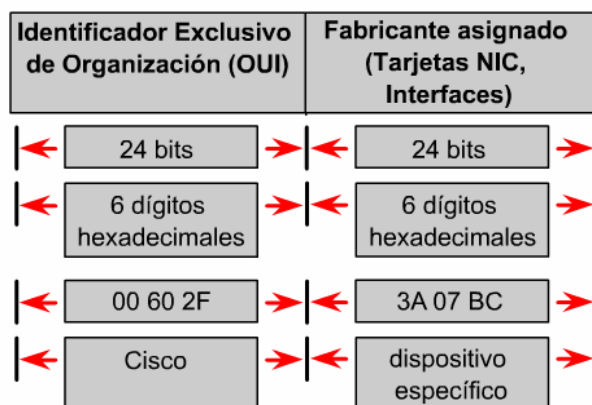


Figura 2

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

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

En una red Ethernet, cuando un dispositivo envía datos, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC destino. El dispositivo origen adjunta un encabezado con la dirección MAC del destino y envía los datos a la red. A medida que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección destino física que transporta la trama de datos. Si no hay concordancia, la NIC descarta la trama de datos. Cuando los datos llegan al nodo destino, la NIC hace una copia y pasa la trama hacia las capas superiores del modelo OSI. En una red Ethernet, todos los nodos deben examinar el encabezado MAC aunque los nodos que están comunicando estén lado a lado.

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

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

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

Se podría utilizar un gráfico de voltaje en función de tiempo para visualizar los bits. Sin embargo, cuando se trabaja con grandes unidades de datos e información de control y direccionamiento, los gráficos de voltaje en función de tiempo pueden volverse excesivamente grandes y confusos. Otro tipo de diagrama que se puede utilizar es el diagrama de *formato de trama*, que se basa en los gráficos de voltaje en función de tiempo. Estos diagramas se leen de izquierda a derecha, como un gráfico de osciloscopio. Los diagramas de formato de trama muestran distintas agrupaciones de bits (campos), que ejecutan otras funciones. ¹

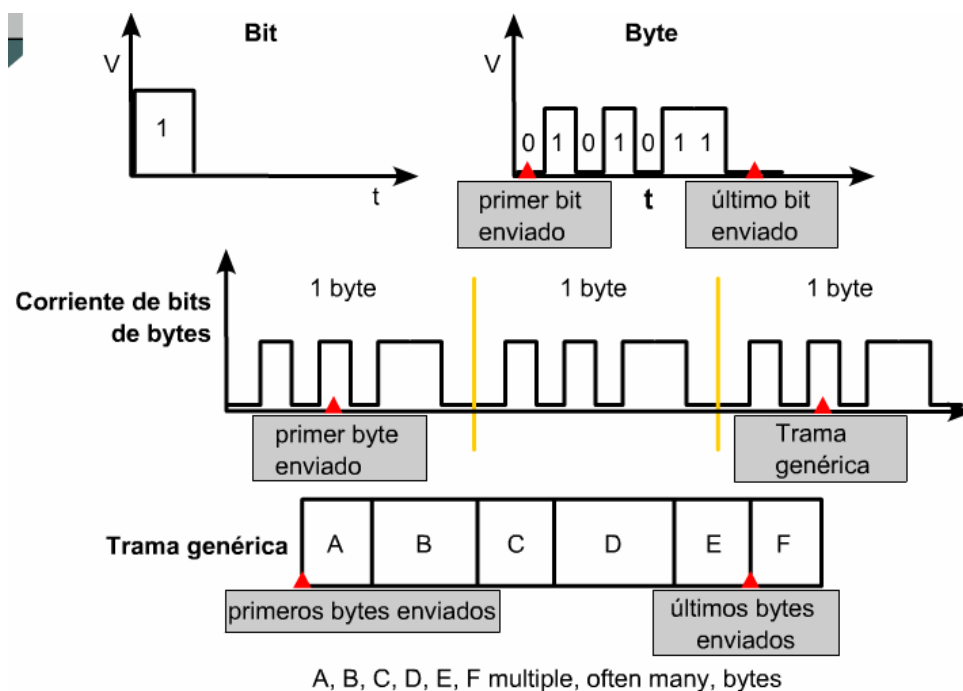


Figura 1

Hay varios tipos distintos de tramas que se describen en diversos estándares. Una trama genérica tiene secciones denominadas campos, y cada campo está formado por bytes. ² Los nombres de los campos son los siguientes:

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

Nombres de campos				
A	B	C	D	E
Campo de inicio de trama	Campo de dirección	Campo de tipo/longitud	Campo de datos	Campo FCS

Figura 2

Cuando los computadores se conectan a un medio físico, debe existir alguna forma de informar a los otros computadores cuando están próximos a enviar un trama. Las diversas tecnologías tienen distintas formas para hacerlo, pero todas las tramas, de cualquier tecnología, tienen una secuencia de señalización de inicio de bytes.

Todas las tramas contienen información de denominación como, por ejemplo, el nombre del computador origen (dirección MAC) y el nombre del computador destino (dirección MAC).

La mayoría de las tramas tienen algunos campos especializados. En algunas tecnologías, el campo "longitud" especifica la longitud exacta de una trama en bytes. Algunas tienen un campo "tipo", que especifica el protocolo de Capa 3 que realiza la petición de envío.

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

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

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

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

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 de la trama de Ethernet

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet desde 10 Mbps hasta 10000 Mbps. ¹ 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.

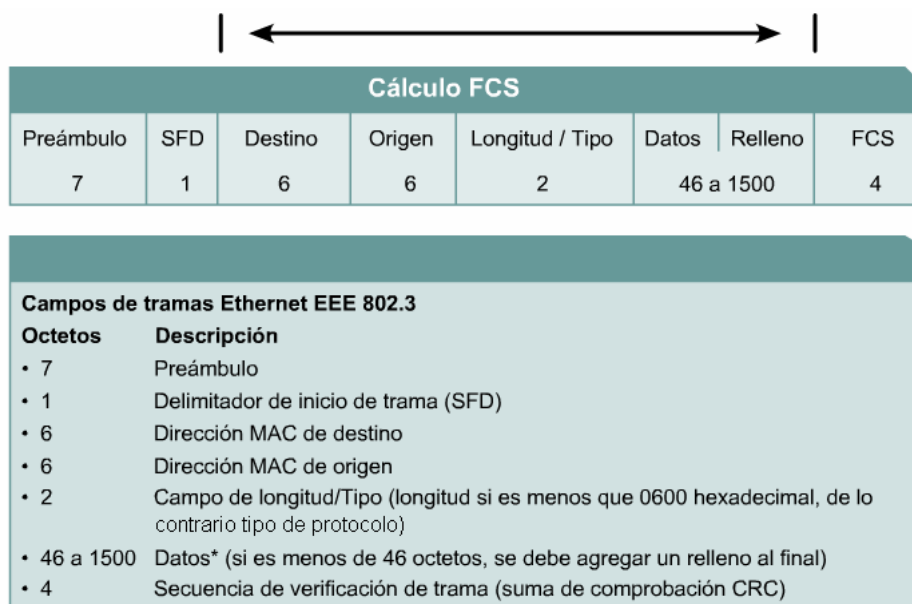


Figura 1

En la versión de Ethernet desarrollada por DIX antes de la adopción de la versión IEEE 802.3 de Ethernet, el Preámbulo y el Delimitador de Inicio de Trama (SFD) se combinaron en un solo campo, aunque el patrón binario era idéntico. El campo que se denomina Longitud/Tipo aparecía como sólo Longitud en las primeras versiones de IEEE y sólo como Tipo en la versión de DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que el uso que ambos le daban al campo era común en toda la industria. ²

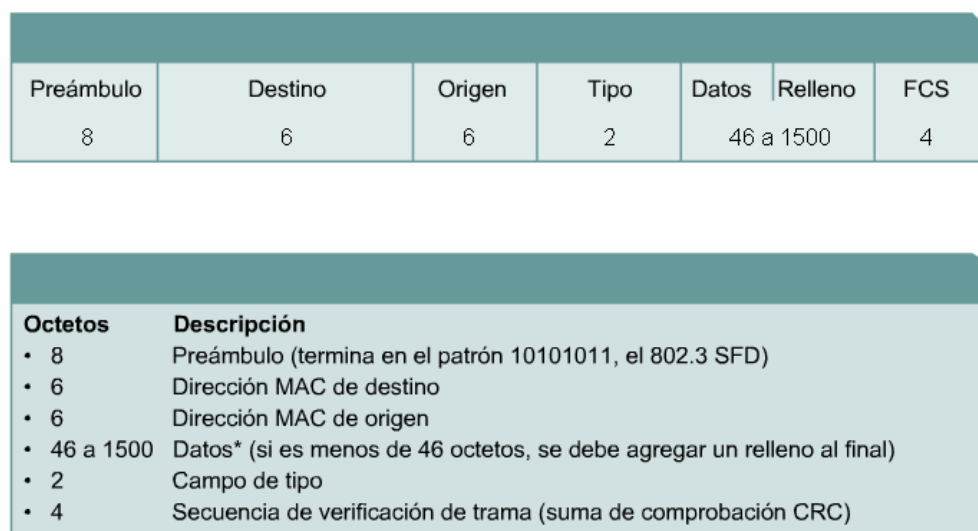


Figura 2

El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. El nodo receptor debe determinar cuál de los protocolos de capa superior está presente en una trama entrante examinando el campo Longitud/Tipo. Si el valor de los dos octetos es igual o mayor que el de 0x600 (hexadecimal), 1536 (decimal), entonces el contenido del campo de Data es codificado de acuerdo al protocolo indicado. ³

- Estándar presentado por DIX.
- Usado por las redes TCP/IP
- Usa el campo de Tipo para determinar el protocolo de la capa superior.
- Ejemplos de tipo:
 - 0x0806 = ARP
 - 0x0800 = IPv4

Figura 3

6.1.7 Campos de la trama de Ethernet

Algunos de los campos que se permiten o requieren en la Trama 802.3 de Ethernet son: ¹

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

IEEE 802.3						
7	1	6	6	2	64 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección origen	Longitud/Tipo	Encabezado y datos de 802.2	Secuencia de verificación de trama

Ethernet					
8	6	6	2	64 a 1500	4
Preámbulo	Dirección de destino	Dirección origen	Tipo	Datos	Secuencia de verificación de trama

Figura 1

El Preámbulo es un patrón alternado de unos y ceros que se utiliza para la sincronización de los tiempos en implementaciones de 10 Mbps y menores de Ethernet. Las versiones más veloces de Ethernet son síncronas y esta información de temporización es redundante pero se retiene por cuestiones de compatibilidad. ²

10101010 10101010 10101010 10101010 10101010 10101010 10101010

Figura 2

Un Delimitador de Inicio de Trama es un campo de un octeto que marca el final de la información de temporización y contiene la secuencia de bits 10101011.

El campo de dirección destino contiene la dirección destino MAC. La dirección destino puede ser unicast, multicast o de broadcast.

El campo de dirección de origen contiene la dirección MAC de origen. La dirección origen generalmente es la dirección unicast del nodo de transmisión de Ethernet. Sin embargo, existe un número creciente de protocolos virtuales en uso que utilizan y a veces comparten una dirección MAC origen específica para identificar la entidad virtual.

El campo Longitud/Tipo admite dos usos diferentes. Si el valor es menor a 1536 decimal, 0x600 (hexadecimal), entonces el valor indica la longitud. La interpretación de la longitud se utiliza cuando la Capa LLC proporciona la identificación del protocolo. El valor del tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento de Ethernet. La longitud indica la cantidad de bytes de datos que sigue este campo.

Los Campos de datos y de relleno, de ser necesario, pueden tener cualquier longitud, mientras que la trama no exceda el tamaño máximo permitido de trama. La unidad máxima de transmisión (MTU) para Ethernet es de 1500 octetos, de modo que los datos no deben superar dicho tamaño. El contenido de este campo no está especificado. Se inserta un relleno no especificado inmediatamente después de los datos del usuario cuando no hay suficientes datos de usuario para que la trama cumpla con la longitud mínima especificada. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud.

Una FCS contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. 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 computadores de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la Capa 2 del modelo OSI. Tanto MAC como LLC son subcapas de la Capa 2. Hay dos categorías amplias de Control de acceso al medio: determinística (por turnos) y la no determinística (el que primero llega, primero se sirve).

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

Los protocolos MAC no determinísticos utilizan el enfoque de "el primero que llega, el primero que se sirve". 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: ¹

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

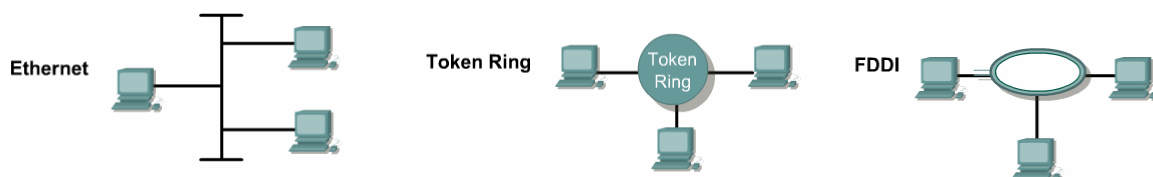


Figura 1

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: 1

- 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

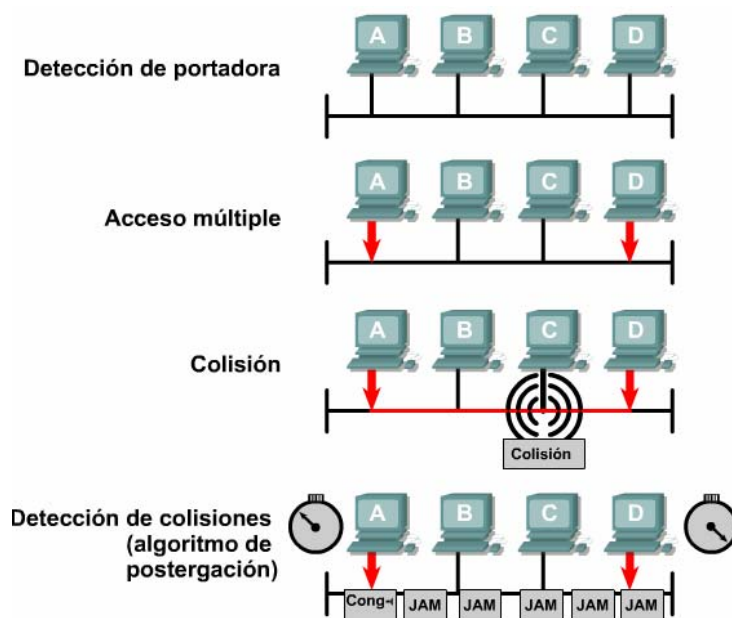


Figura 1

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. 2

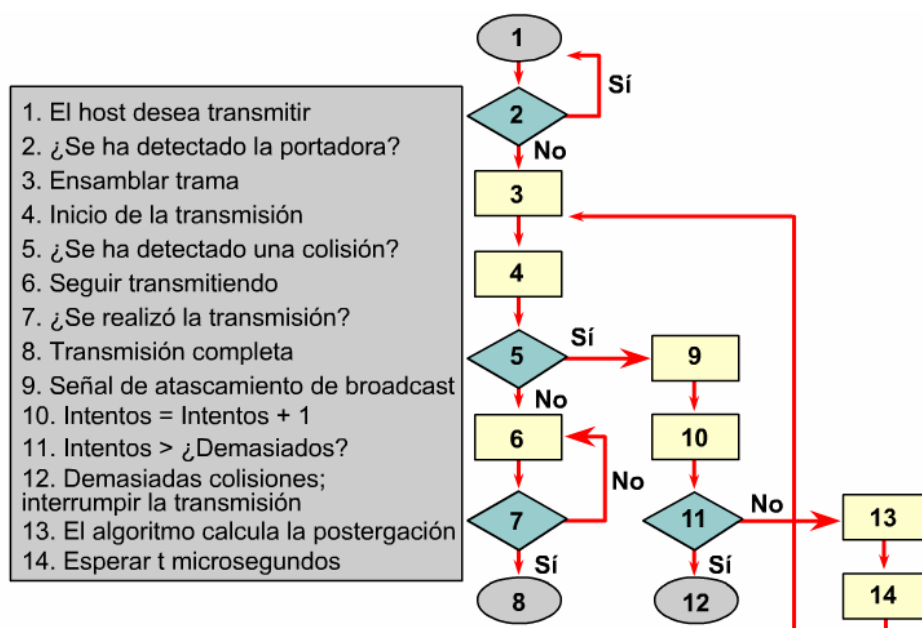


Figura 2

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

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

6.2.3 Temporización de Ethernet

Las reglas y especificaciones básicas para el adecuado funcionamiento de Ethernet no son particularmente complicadas aunque algunas de las implementaciones más veloces de la capa física así se están volviendo. A pesar de su sencillez básica, cuando se produce un problema en Ethernet, a menudo resulta difícil determinar el origen. Debido a la arquitectura común en bus de Ethernet, también descrita como punto único de falla distribuido, el alcance del problema a menudo abarca a todos los dispositivos del dominio de colisión. En los casos en que se utilizan repetidores, esto puede incluir dispositivos separados hasta por cuatro segmentos.

Cualquier estación de una red Ethernet que desee transmitir un mensaje, primero "escucha" para asegurar que ninguna otra estación se encuentre transmitiendo. Si el cable está en silencio, la estación comienza a transmitir de inmediato. La señal eléctrica tarda un tiempo en transportarse por el cable (retardo) y cada repetidor subsiguiente introduce una pequeña cantidad de latencia en el envío de la trama desde un puerto al siguiente. Debido al retardo y a la latencia, es posible que más de una estación comience a transmitir a la vez o casi al mismo tiempo. Esto produce una colisión.

Si la estación conectada opera en full duplex entonces la estación puede enviar y recibir de forma simultánea y no se deberían producir colisiones. Las operaciones en full-duplex también cambian las consideraciones de temporización y eliminan el concepto de la ranura temporal. La operación en full-duplex permite diseños de arquitectura de redes más grandes ya que se elimina la restricción en la temporización para la detección de colisiones.

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

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

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

Las versiones de 10 Mbps y más lentas de Ethernet son asíncronas. Asíncrona significa que cada estación receptora utiliza los ocho octetos de la información de temporización para sincronizar el circuito receptor con los datos entrantes y luego los descarta. Las implementaciones de 100 Mbps y de mayor velocidad de Ethernet son síncronas. Síncrona significa que la información de temporización no es necesaria, sin embargo, por razones de compatibilidad, el Preámbulo y la SFD (Delimitador de Inicio de Trama) están presentes.

Para todas las velocidades de transmisión de Ethernet de 1000 Mbps o menos, el estándar describe la razón por la cual una transmisión no puede ser menor que la ranura temporal. 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. ¹

Velocidad de Ethernet	Período de bit
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

Figura 1

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. ¹

Velocidad	Espacio entre las tramas	Tiempo requerido
10 Mbps	96 tiempos de bit	9.6 μ s
100 Mbps	96 tiempos de bit	0.96 μ s
1 Gbps	96 tiempos de bit	0.096 μ s
10 Gbps	96 tiempos de bit	0.0096 μ s

Figura 1

Una vez enviada la trama, todas las estaciones de Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir, de manera legal, la siguiente trama. En versiones de Ethernet más veloces, el espacio sigue siendo el mismo, 96 tiempos de bit, pero el tiempo que se requiere para dicho intervalo se vuelve proporcionalmente más corto. Este intervalo se conoce como separación. El propósito del intervalo es permitir que las estaciones lentas tengan tiempo para procesar la trama anterior y prepararse para la siguiente trama.

Se espera que un repetidor regenere los 64 bits completos de información de temporización, que es el preámbulo y la SFD, al inicio de cualquier trama. Esto a pesar de la pérdida potencial de algunos de los bits iniciales del preámbulo, debido a una sincronización lenta. Debido a esta reintroducción forzada de los bits de temporización, cierta reducción menor de la separación entre las tramas no sólo es posible sino que también esperada. Algunos chipsets de Ethernet son sensibles a un acortamiento del espacio entre las tramas y comienzan a dejar de ver las tramas a medida que se reduce la separación. Con el aumento del poder de procesamiento en el escritorio, resultaría muy sencillo para un computador personal saturar un segmento de Ethernet con tráfico y comenzar a transmitir nuevamente antes de que se cumpla el tiempo de retardo del espacio entre las tramas.

Una vez producida la colisión y que todas las estaciones permitan que el cable quede inactivo (cada una espera que se cumpla el intervalo completo entre las tramas), entonces, las estaciones que sufrieron la colisión deben esperar un período adicional y cada vez potencialmente mayor antes de intentar la retransmisión de la trama que sufrió la colisión. El período de espera está intencionalmente diseñado para que sea aleatorio de modo que dos estaciones no demoren la misma cantidad de tiempo antes de efectuar la retransmisión, lo que causaría colisiones adicionales. Esto se logra en parte al aumentar el intervalo a partir del cual se selecciona el tiempo de retransmisión aleatorio cada vez que se efectúa un intento de retransmisión. El período de espera se mide en incrementos de la ranura temporal del parámetro.

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

6.2.5 Manejo de los errores

El estado de error más común en redes Ethernet son las colisiones. ¹Las colisiones son el mecanismo para resolver la contención del acceso a la red. Unas pocas colisiones proporcionan una forma simple y sin problemas, que usa pocos recursos, para que los nodos de la red arbitren la contención para el recurso de red. Cuando la contención de la red se vuelve demasiado grave, las colisiones se convierten en un impedimento significativo para la operación útil de la red.

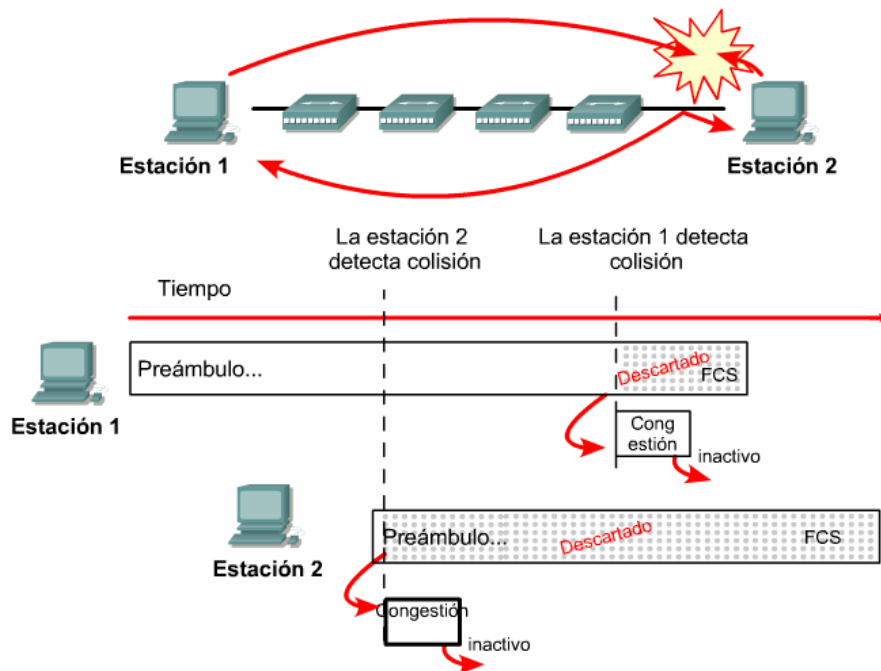


Figura 1

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 ¹ 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. Finalmente, cuando los fragmentos de la colisión llegaron a la Estación 1, ésta cortó la transmisión en curso y sustituyó con la señal de congestión de 32 bits el resto de la trama que estaba transmitiendo. Luego de enviar la señal de congestión de 32 bits, la Estación 1 dejó de transmitir.

Una señal de congestión puede estar compuesta por cualquier dato binario siempre que no forme una checksum apropiada para la porción de la trama ya transmitida. El patrón de datos que se observa con mayor frecuencia para una señal de congestión es simplemente un patrón de uno, cero, uno, cero que se repite, al igual que el Preámbulo. Cuando se observa con un analizador de protocolos, este patrón aparece como una secuencia repetida de A ó 5 hexadecimales. Los mensajes corrompidos, transmitidos de forma parcial, generalmente se conocen como fragmentos de colisión o runts. Las colisiones normales tienen menos de 64 octetos de largo y, por lo tanto, reprueban tanto la prueba de longitud mínima como la prueba de la checksum de FCS.

6.2.6 Tipos de colisiones

Por lo general, las colisiones se producen cuando dos o más estaciones de Ethernet transmiten al mismo tiempo dentro de un dominio de colisión. Una colisión simple es una colisión que se detecta al tratar de transmitir una trama, pero en el siguiente intento es posible transmitir la trama con éxito. Las colisiones múltiples indican que la misma trama colisionó una y otra vez antes de ser transmitida con éxito. Los resultados de las colisiones, los fragmentos de colisión, son tramas parciales o corrompidas de menos de 64 octetos y que tienen una FCS inválida. Los tres tipos de colisiones son: 1

- Locales
- Remotas
- Tardías

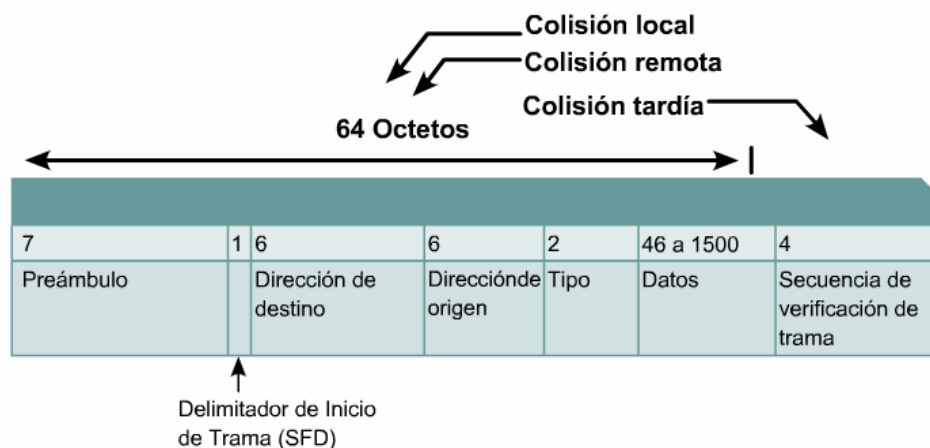
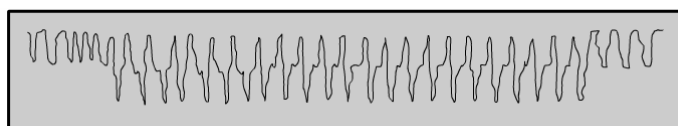


Figura 1

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 2 contiene 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.



Colisión en mitad de trama 10BASE2 / 10BASE5 capturada por un osciloscopio de almacenamiento digital.

Figura 2

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.

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

6.2.7 Errores de Ethernet

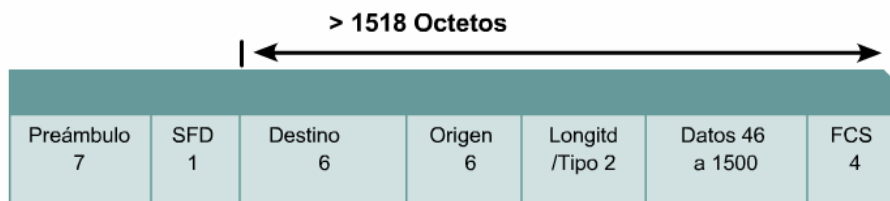
El conocimiento de los errores típicos es invaluable para entender tanto la operación como la detección de fallas de las redes Ethernet.

Las siguientes son las fuentes de error de Ethernet.

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

Mientras las colisiones locales o remotas se consideran parte normal de la operación de Ethernet, las colisiones tardías son un error. La presencia de errores en una red siempre sugiere la necesidad de una mayor investigación. La gravedad del problema indica la urgencia de la detección de la falla relativa a los errores detectados. Algunos errores detectados en varios minutos u horas suele ser una prioridad baja. Miles detectados en pocos minutos sugieren que se requiere atención urgente.

El estándar 802.3, en varios lugares, define al jabber como una transmisión de al menos 20.000 a 50.000 tiempos de bit de duración. Sin embargo, la mayoría de las herramientas de diagnóstico informan de la presencia de jabber siempre que se detecta una transmisión que excede el tamaño máximo legal de la trama, que es considerablemente menor a 20.000 a 50.000 tiempos de bit. La mayoría de las referencias al jabber, realmente se deben llamar tramas largas. ¹

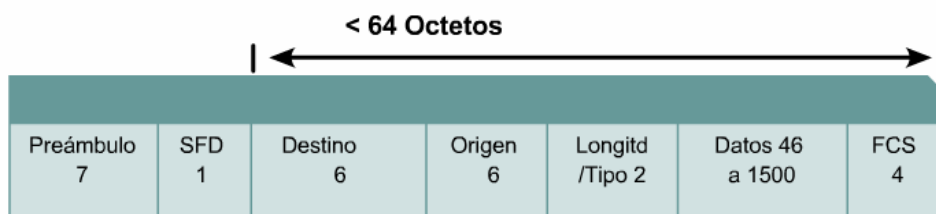


Las jabbers y las tramas largas superan ambas el tamaño máximo permitido de trama. La jabber es bastante más grande.

Figura 1

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 "runt". Por lo general, la presencia de tramas cortas no significa que la red esté fallando. ²



Las tramas cortas están formadas correctamente en todos los aspectos salvo uno y tienen sumas de comprobación FCS válidas, pero tienen un tamaño de trama menor que el mínimo (64 octetos).

Figura 2

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 más allá

Una trama recibida que tiene una Secuencia de verificación de trama incorrecta, también conocido como error de CRC o de checksum, difiere de la transmisión original en al menos un bit. En una trama con error de FCS, es probable que la información del encabezado sea correcta, pero la checksum que calcula la estación receptora no concuerda con la checksum que adjunta la estación transmisora al extremo de la trama. Por lo tanto, se descarta la trama.

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

Un mensaje que no termina en un límite de octeto se conoce como error de alineamiento. En lugar del número correcto de bits binarios que forman agrupaciones completas de octetos, hay bits adicionales que sobran (menos de ocho). Una trama así se trunca en el límite del octeto más cercano, y si la checksum de FCS falla, entonces, se informa un error de alineamiento. Esto es causado a menudo por controladores de software dañados, o una colisión, y con frecuencia viene acompañado por una falla de la checksum de FCS. Una trama con un valor válido en el campo "longitud" pero que no concuerda con el número real de octetos contabilizados en el campo de datos de la trama recibida recibe el nombre de error de rango. Este error también aparece cuando el valor del campo de longitud es menor que el tamaño mínimo legal sin relleno para el campo de datos. Un error, similar, Fuera de rango, se informa cuando el valor del campo "longitud" indica que el tamaño de los datos es demasiado grande para ser legal.

Fluke Networks ha acuñado el término fantasma para referirse a la energía (ruido) que se detecta en el cable y que parece ser una trama, pero que carece de un SFD válido. Para ser considerada fantasma, la trama debe tener una longitud de al menos 72 octetos, incluyendo el preámbulo. De lo contrario, se clasifica como colisión remota. Debido a la naturaleza peculiar de los fantasmas, cabe notar que los resultados de las pruebas dependen en gran medida del lugar donde se efectuó la medición del segmento.

Las mallas a tierra y otros problemas de cableado son normalmente la causa de los fantasmas. La mayoría de las herramientas de monitoreo de la red no reconocen la existencia de fantasmas por la misma razón que no reconocen las colisiones de los preámbulos. Las herramientas confían completamente en lo que el chipset les dice. Los analizadores de protocolo basados en software, muchos analizadores de protocolos basados en hardware, las herramientas de diagnóstico manuales así como la mayoría de las sondas de monitoreo remoto (RMON) no informan de estos eventos.

6.2.9 Auto-negociación de Ethernet

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

La 10BASE-T requirió que cada estación transmitiera un pulso de enlace aproximadamente cada 16 milisegundos, siempre que la estación no estuviera transmitiendo un mensaje. La Auto-Negociación adoptó esta señal y la red denominó Pulso de enlace normal (NLP). Cuando se envía una serie de NLP en un grupo con el propósito de Auto-Negociación, el grupo recibe el nombre de ráfaga de Pulso de enlace rápido (FLP). Cada ráfaga de FLP se envía a los mismos intervalos que un NLP y tiene como objetivo permitir que los antiguos dispositivos de 10BASE-T operen normalmente en caso de que reciban una ráfaga de FLP. ¹

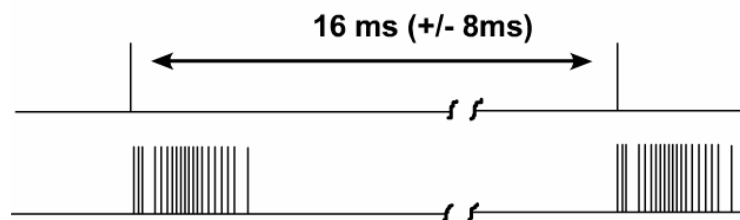
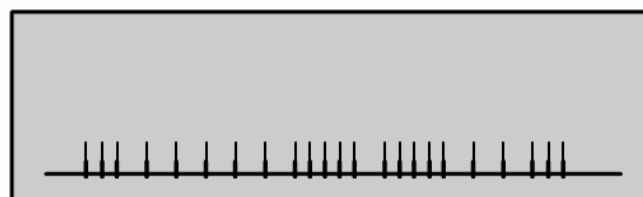


Figura 1

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. ²



La ráfaga FLP se compone de múltiples pulsos de enlace NLP.

Figura 2

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

Muchos proveedores implementan hardware de forma tal que va intentando los distintos estados posibles de forma cíclica. Transmite ráfagas de FLP para Auto-Negociar por unos momentos, luego se configura para la Fast Ethernet, intenta enlazarse por unos instantes y luego sólo escucha. Algunos proveedores no ofrecen ningún intento para enlazarse hasta que la interfaz primero escucha una ráfaga de FLP o algún otro esquema de señalización.

Son dos las modalidades de duplex, half y full. Para los medios compartidos, el modo half-duplex es obligatorio. Todas las implementaciones en cable coaxial son half-duplex por naturaleza y no pueden operar en full duplex. Las implementaciones en UTP y fibra pueden operar en half duplex. Las implementaciones de 10 Gbps se especifican sólo para full duplex.

En half duplex, sólo una estación puede transmitir a la vez. En las implementaciones en coaxial, una transmisión desde una segunda estación hará que las señales se superpongan y se corrompan. Como el UTP y la fibra, por lo general, transmiten por pares distintos, las señales no tienen oportunidad de superponerse o dañarse. Ethernet ha establecido las reglas de arbitraje para resolver los conflictos que surgen cuando más de una estación intenta transmitir al mismo tiempo. Se permite que dos estaciones de un enlace full-duplex punto a punto transmitan en cualquier momento, independientemente de si la otra estación está transmitiendo.

La Auto-Negociación evita la mayoría de las situaciones donde una estación de un enlace punto a punto transmite de acuerdo a las reglas de half-duplex y la otra de acuerdo a las reglas de full-duplex.

- 
- 1000BASE-T full duplex
 - 1000BASE-T half duplex
 - 100BASE-TX full duplex
 - 100BASE-TX half duplex
 - 10BASE-T full duplex
 - 10BASE-T half duplex

Figura 1

En el caso en que los socios del enlace sean capaces de compartir más de una tecnología en común, consulte la lista de la Figura 1. Esta lista se utiliza para determinar la tecnología se debe elegir entre las configuraciones ofrecidas.

Las implementaciones de Ethernet en fibra óptica no se incluyen en esta lista de resolución de prioridades porque la electrónica y la óptica de la interfaz no permiten una fácil configuración entre las implementaciones. Se supone que la configuración de la interfaz es fija. Si las dos interfaces pueden Auto-Negociar, entonces, ya utilizan la misma implementación de Ethernet. Sin embargo, todavía quedan varias opciones de configuración que tiene que determinarse, tales como el ajuste del duplex o cuál es la estación que actuará como Master a los fines de sincronización.

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

Módulo 7: Tecnologías Ethernet

Descripción general

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: Este módulo presenta los datos específicos de los tipos más importantes de Ethernet. El objetivo no es transmitir todos los hechos acerca de cada tipo de Ethernet sino desarrollar el sentido de lo que es común a todas las formas de Ethernet.

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). Los estándares para Gigabit Ethernet sólo tardaron tres años en salir. Una versión de Ethernet aún más rápida, Ethernet de 10 Gigabits (10 Gigabit Ethernet) se halla fácilmente en el mercado e inclusive, versiones más rápidas están en desarrollo.

En estas versiones más rápidas de Ethernet, el direccionamiento MAC, CSMA/CD y el formato de trama no han sufrido cambios respecto de versiones anteriores de Ethernet. Sin embargo, otros aspectos de la subcapa MAC, la capa física y el medio han cambiado. Las tarjetas de interfaz de red (NIC) con base de cobre capaces de operar a 10/100/1000 están ahora entre las más comunes. Los switches y los routers con puertos de Gigabit se están convirtiendo en el estándar para los armarios de cableado. El uso de la fibra óptica que admite Gigabit Ethernet se considera un estándar para el cableado backbone en la mayoría de las instalaciones nuevas.

Los estudiantes que completen este módulo deberán poder:

- Describir las similitudes y diferencias entre las Ethernet 10BASE5, 10BASE2 y 10BASE-T.
- Definir la codificación de Manchester.
- Nombrar los factores que afectan los límites de temporización de Ethernet.
- Nombrar los parámetros de cableado 10BASE-T.
- Describir las características y tipos principales de Ethernet de 100 Mbps.
- Describir la evolución de Ethernet.
- Explicar los métodos MAC, los formatos de trama y el proceso de transmisión de Gigabit Ethernet.
- Describir los usos de los medios y la codificación específicos en Gigabit Ethernet.
- Identificar las salidas de pin y el cableado, típicos de las distintas implementaciones de Gigabit Ethernet.
- Describir las similitudes y diferencias entre Gigabit Ethernet y Ethernet de 10 Gigabits.
- Describir las consideraciones arquitectónicas básicas de Gigabit Ethernet y Ethernet de 10 Gigabits.

7.1 Ethernet de 10-Mbps y 100-Mbps

7.1.1 Ethernet de 10-Mbps

		Subcapa de control de enlace lógico Control de acceso al medio 802.3								
Capa de señalización física	Medio físico	Coaxial N-Style 10BASE5 (500m) de 50 Ohmios	BNC coaxial 10BASE2 (185m) de 50 Ohmios	UTP RJ-45 10BASE-T (100m) de 100 Ohmios	UTP RJ-45 100BASE-TX (100m) de 100 Ohmios	SC de fibra 100BASE-FX (228-412m) MM	UTP RJ-45 1000BASE-T (100m) de 100 Ohmios	SC de fibra 1000BASE-SX (220-550m) MM	SC de fibra 1000BASE-LX (550-5000m) MM	SC de fibra 10GBASE- (varios) MM o SM

Figura 1

Las Ethernet de 10BASE5, 10BASE2 y 10BASE-T se consideran implementaciones antiguas de Ethernet. ¹ 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.

En la figura ² se muestran los parámetros de operación para Ethernet de 10 Mbps. 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 microsegundos = 1 diez millonésima parte de un segundo. Esto significa que en una red Ethernet de 10 Mbps, 1 bit en la subcapa MAC requiere de 100 nseg para ser transmitido.

Parámetro	Valor
Período de bit	100 nanosegundos (ns)
Ranura temporal	512 veces un bit, (64 octetos)
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)

Figura 2

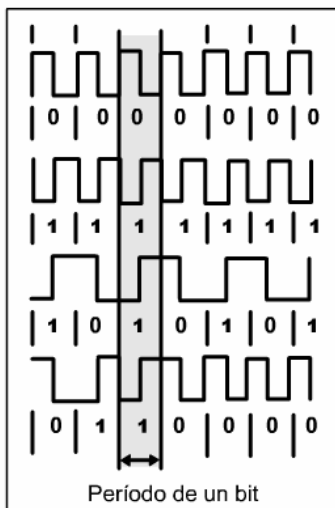
Para todas las velocidades de transmisión Ethernet igual o por debajo de 1000 Mbps, la transmisión no debe ser menor al margen de tiempo "Slot time". El margen de tiempo es apenas mayor al tiempo, que en teoría, le tomaría a una transmisión desde un extremo de la red llegar hasta el otro extremo ubicado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

El proceso de transmisión anterior de Ethernet es idéntico hasta la parte inferior de la capa física OSI. Los datos de la trama de Capa 2 se convierten de números hexadecimales a números binarios. A medida que la trama pasa de la subcapa MAC a la capa física, se llevan a cabo procesos adicionales antes de que los bits se trasladen desde la capa física al medio. Un proceso de importancia es la señal de error de calidad de señal (Signal Quality Error, SQE). La SQE es una transmisión del transceptor de respuesta al controlador para indicarle sobre la funcionalidad de los circuitos de detección de colisiones. La SQE es conocida como "latido de corazón". La señal SQE fue diseñada para corregir el problema en versiones anteriores de Ethernet, en las cuales el host desconocía si el transceptor estaba conectado. El SQE siempre se utiliza en half-duplex. Es posible utilizar el SQE en una operación en full-duplex pero no es necesario. El SQE está activo en las siguientes instancias:

- Dentro de los 4 a los 8 microsegundos después de una transmisión normal para indicar que se transmitió con éxito la trama saliente.
- Siempre que haya colisión en el medio.
- Siempre que haya una señal inadecuada en el medio, o las reflexiones causadas por un corto en el cable.
- Siempre que se haya interrumpido una transmisión.

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 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. ³ 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. 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.



Ejemplo de codificación de Manchester. El eje Y es el voltaje; el eje X es el tiempo.

Figura 3

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

- La longitud del cable y su retardo de propagación.
- El retardo de los repetidores.
- El retardo de los transceptores.
- El acortamiento del intervalo entre las tramas.
- Los retardos dentro de la estación.

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

7.1.2 10BASE5

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 1 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.

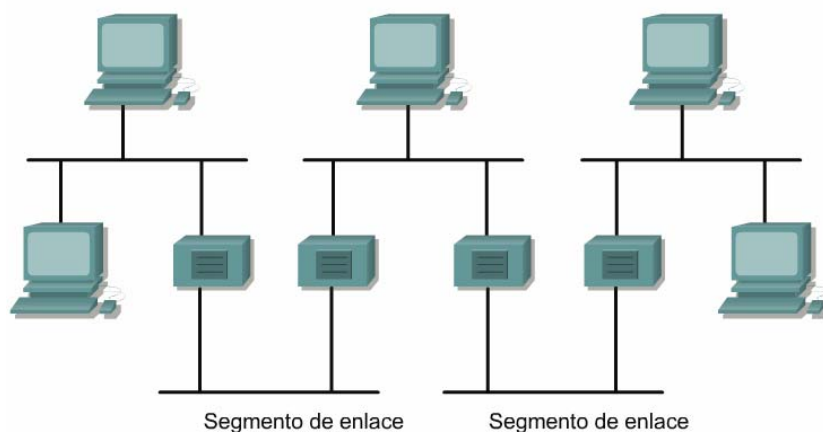


Figura 1

7.1.3 10BASE2

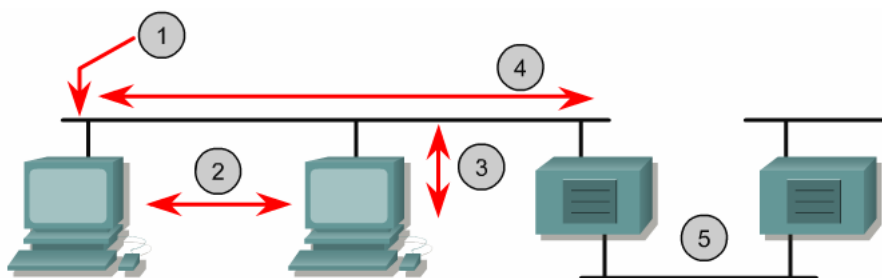
La tecnología 10BASE2 se introdujo en 1985. La instalación fue más sencilla debido a su menor tamaño y peso, y por su mayor flexibilidad. Todavía existen en redes de este tipo, como 10BASE5, la cual no es recomendable para la instalación de redes hoy en día. Tiene un costo bajo y carece de la necesidad de hubs. Además, las NIC son difíciles de conseguir para este medio.

10BASE2 usa la codificación Manchester también. Los computadores en la LAN se conectaban entre sí con una serie de tendidos de cable coaxial sin interrupciones. Se usaban conectores BNC para unir estos tendidos a un conector en forma de T en la NIC.

10BASE2 tiene un conductor central trenzado. Cada uno de los cinco segmentos máximos de cable coaxial delgado puede tener hasta 185 metros de longitud y cada estación se conecta directamente al conector BNC con forma de "T" del cable coaxial.

Sólo una estación puede transmitir a la vez, de lo contrario, se produce una colisión. 10BASE2 también usa half-duplex. La máxima velocidad de transmisión de 10BASE2 es de 10 Mbps.

Puede haber hasta 30 estaciones en cada segmento individual de 10BASE2. De los cinco segmentos consecutivos en serie que se encuentran entre dos estaciones lejanas, sólo tres pueden tener estaciones conectadas. ¹



1. La terminación de cada extremo del cable coaxial debe ser de 50 Ohmios.
2. La distancia mínima entre conectores es de 0,5 metros.
3. Cada estación debe conectarse dentro de los cuatro centímetros del cable coaxial delgado.
4. Máxima longitud del segmento es 185 metros.
5. Los segmentos de enlaces entre repetidores deben tener en total sólo dos conexiones, los propios repetidores.

Figura 1

7.1.4 10BASE-T

10BASE-T fue introducido en 1990. 10BASE-T utilizaba cable de cobre (UTP) de par trenzado, no blindado de Categoría 3 que era más económico y más fácil de usar que el cable coaxial. 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 1 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.

Número de 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 negativa)
7	No se utiliza
8	No se utiliza

Figura 1

Half duplex o full duplex es la elección de configuración. 10BASE-T transporta 10 Mbps de tráfico en modo half-duplex y 20 Mbps en modo full-duplex.

7.1.5 Cableado y arquitectura de 10BASE-T

Los enlaces de 10BASE-T generalmente consisten en una conexión entre la estación y un hub o switch. Los hubs son repetidores multipuertos y cuentan en el número límite de repetidores entre las estaciones lejanas. Los hubs no dividen los segmentos de la red en distintos dominios de colisión. Como los hubs o repetidores solamente extienden la longitud de una red dentro de un solo dominio de colisión, existe un límite respecto de cuántos hubs pueden ser utilizados en dicho segmento. Los puentes y los switches dividen un segmento en dominios de colisión individuales, dejando que las limitaciones de los medios determinen la distancia entre los switches. 10BASE-T limita la distancia entre los switches a 100 m (328 pies).

Aunque los hubs pueden estar enlazados, es recomendable evitar esta disposición. Esto contribuye a evitar que se exceda el límite de retardo máximo entre las estaciones lejanas. Cuando se requiera del uso de múltiples hubs, es recomendable organizarlos de forma jerárquica, para así crear una estructura en forma de árbol. Mejorará el rendimiento si pocos repetidores separan las estaciones.

La Figura 1 muestra un ejemplo de arquitectura. Son aceptables todas las distancias entre las estaciones. Sin embargo, la distancia total desde un extremo de la red hasta el otro lleva la arquitectura al límite. El aspecto más importante a considerar es cómo mantener el retardo entre las estaciones lejanas al mínimo, independientemente de la arquitectura y los tipos de medios utilizados. Un retardo máximo más corto brinda un mejor rendimiento general.

Los enlaces de 10BASE-T pueden tener distancias sin repetición de hasta 100 m. Aunque esta pueda parecer una distancia larga, por lo general se ve maximizada al cablear un edificio real. Los hubs pueden solucionar el problema de la distancia pero permiten que se propaguen las colisiones. La introducción difundida de los switches ha hecho que la limitación de la distancia resulte menos importante. Siempre que

las estaciones de trabajo se encuentren dentro de unos 100 m de distancia del switch, esta distancia de 100m comienza nuevamente a partir del switch.

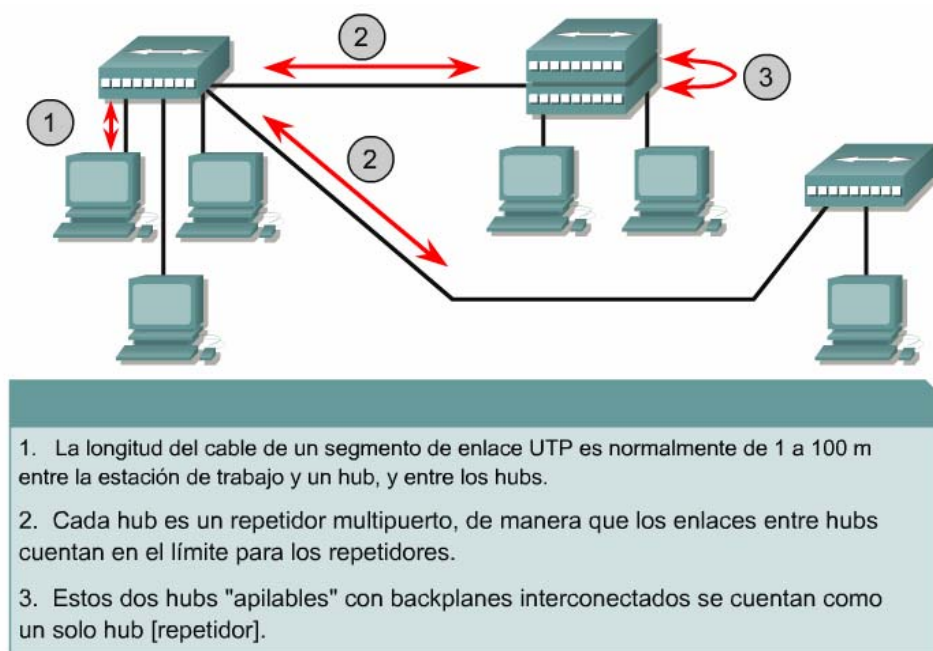


Figura 1

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. ¹

Parámetro	Valor
Período de bit	10 nanosegundos (ns)
Ranura temporal	512 veces un bit, (64 octetos)
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)

Figura 1

Trama de Ethernet							
Preámbulo	SFD	Destino	Origen	Longitud Tipo	Datos	Relleno	FCS
7	1	6	6	2	46 a 1500		4

Figura 2

El formato de trama de 100-Mbps es el mismo que el de la trama de 10-Mbps. ²

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.

7.1.7 100BASE-TX

En 1995, 100BASE-TX con un cable UTP Cat 5 fue el estándar que se convirtió en un éxito comercial. Ethernet coaxial original utilizaba transmisión en half-duplex de modo que sólo un dispositivo podía transmitir a la vez. Sin embargo, en 1997, Ethernet se expandió para incluir capacidad de full duplex permitiendo que más de un PC transmitiera al mismo tiempo en una red. Cada vez más, los switches reemplazaban los hubs. Estos switches tenían la capacidad de transmitir en full duplex y de manejar rápidamente las tramas de Ethernet.

100BASE-TX usa codificación 4B/5B, que luego es mezclada y convertida a 3 niveles de transmisión multinivel o MLT-3. ¹En el ejemplo, la ventana resaltada muestra cuatro ejemplos de forma de onda. La forma de la onda superior no presenta transición en el centro de la ventana de temporización. La ausencia de una transición indica que el binario 0 está presente. La segunda forma de onda presenta una transición en el centro de la ventana de temporización. La transición representa el binario 1. La tercera forma de onda muestra una secuencia binaria alternada. La ausencia de una transición binaria indica un binario 0 y la presencia de una transición indica un binario 1. Bordes ascendentes o descendentes indican unos. Cambios de señal muy pronunciados indican unos. Toda línea horizontal detectable en la señal indica un 0.

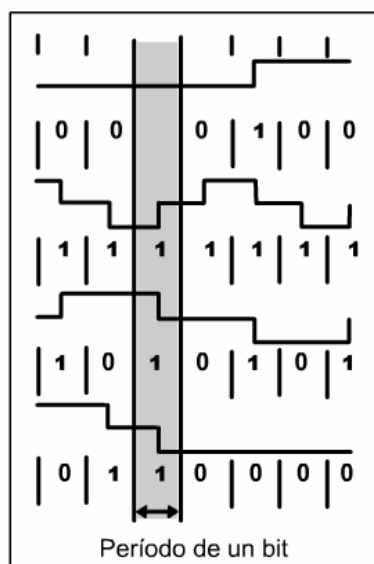


Figura 1

La Figura ²muestra la disposición de la salida de los pins para una conexión 100BASE-TX. Tenga en cuenta que existen dos diferentes rutas de transmisión-recepción. Esto es igual que en la configuración de 10BASE-T.

Número de p	Señal
1	TD+ (Transmitir datos, señal diferencial positiva)
2	TD- (Transmitir datos, señal diferencial negativa)
3	RD+ (Recibir datos, señal diferencial positiva)
4	No se utiliza
5	No se utiliza
6	RD- (Recibir datos, señal diferencial negativa)
7	No se utiliza
8	No se utiliza

Figura 2

100BASE-TX transporta 100 Mbps de tráfico en modo half-duplex. En modo full-duplex, 100BASE-TX puede intercambiar 200 Mbps de tráfico. El concepto de full duplex se hace cada vez más importante a medida que aumentan las velocidades de Ethernet.

7.1.8 100BASE-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 1 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.

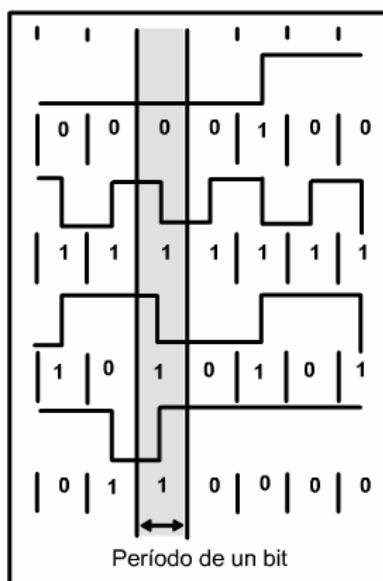


Figura 1

La Figura 2 resume un enlace y las salidas de pins para 100BASE-FX. El par de fibra con conectores ST o SC es el que se utiliza más comúnmente.

Fibra	Señal
1	Tx (transmisores LED y láser)
2	Rx (detectores de fotodiodos de alta velocidad)

Figura 2

La transmisión a 200 Mbps es posible debido a las rutas individuales de Transmisión (Tx) y Recepción (Rx) de fibra óptica de 100BASE-FX.

7.1.9 Arquitectura de la Fast Ethernet

Los enlaces de Fast Ethernet generalmente consisten en una conexión entre la estación y el hub o switch. Los hubs se consideran repetidores multipuerto y los switches, puentes multipuerto. Estos están sujetos a la limitación de 100 m de distancia de los medios UTP.

Un repetidor Clase 1 puede introducir hasta 140 tiempos de bit de latencia. Todo repetidor que cambie entre una implementación de Ethernet y otra es un repetidor Clase 1. Un repetidor Clase II está restringido a menores retardos, 92 tiempos de bit, debido a que inmediatamente repite la señal entrante al resto de los puertos sin proceso de translación. Para lograr menor latencia, los repetidores Clase II deben conectarse a tipos de segmentos que usen la misma técnica de señalización.

Tal como sucede con las versiones de 10 Mbps, es posible modificar algunas de las reglas de arquitectura para las versiones de 100 Mbps. Sin embargo, no se permite casi ningún retardo adicional. La modificación de las reglas de arquitectura para 100BASE-TX no es recomendable. El cable para 100BASE-TX entre repetidores Clase II no puede superar los 5 metros. Con frecuencia se encuentran enlaces en Fast Ethernet que operan en half duplex. Sin embargo, no se recomienda el half duplex porque el esquema de señalización en sí es full duplex.

La Figura 1 muestra las distancias de cable de la configuración arquitectónica. Los enlaces de 100BASE-TX pueden tener distancias sin repetición de hasta 100 m. El amplio uso de switches ha hecho que las limitaciones de distancia sean menos importantes. Como la mayoría de Fast Ethernet está conmutada, estos representan los límites prácticos entre los dispositivos.

Arquitectura	100BASE-TX	100BASE-FX	100BASE-TX y FX
Estación a estación, Estación a Switch, Switch a Switch (half o full duplex)	100 m	412 m	N/A
Un Repetidor Clase I (half duplex)	200 m	272 m	100 m (TX) 160.8 m (FX)
Un Repetidor Clase II (half duplex)	200 m	320 m	100 m (TX) 208 m (FX)
Dos Repetidores Clase II (half duplex)	205 m	228 m	105 m (TX) 211.2 m (FX)

Figura 1

7.2 Ethernet Gigabit y 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. 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.

Subcapa de control de enlace lógico Control de acceso al medio 802.3	
Capa de señalización física	Medio físico
Coaxial N-Style 10BASE5 (500m) de 50 Ohmios	Coaxial N-Style 10BASE5 (500m) de 50 Ohmios
BNC coaxial 10BASE2 (185m) de 50 Ohmios	BNC coaxial 10BASE2 (185m) de 50 Ohmios
UTP RJ-45 10BASE-T (100m) de 100 Ohmios	UTP RJ-45 10BASE-T (100m) de 100 Ohmios
UTP RJ-45 100BASE-TX (100m) de 100 Ohmios	UTP RJ-45 100BASE-TX (100m) de 100 Ohmios
SC de fibra 100BASE-FX (228-412m) MM	SC de fibra 100BASE-FX (228-412m) MM
UTP RJ-45 1000BASE-T (100m) de 100 Ohmios	UTP RJ-45 1000BASE-T (100m) de 100 Ohmios
SC de fibra 1000BASE-SX (220-550m) MM	SC de fibra 1000BASE-SX (220-550m) MM
SC de fibra 10GBASE- (varios) MM o SM	SC de fibra 10GBASE- (varios) MM o SM
SC de fibra 1000BASE-LX (550-5000m) MM	SC de fibra 1000BASE-LX (550-5000m) MM

Figura 1

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización, como muestra la Figura 2. Utilizan un tiempo de bit de 1 nanosegundo (0,000000001 segundos) o 1 mil millonésima parte de un segundo. La trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Según su implementación, Gigabit Ethernet puede hacer uso de distintos procesos para convertir las tramas a bits en el cable. La Figura 3 muestra los formatos de trama para Ethernet.

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

* El valor listado es el espaciado intertrama oficial

Figura 2

Trama de Ethernet							
Preámbulo	SFD	Destino	Origen	Longitud Tipo	Datos	Relleno	FCS
7	1	6	6	2	46 a 1500		4

Figura 3

Las diferencias entre Ethernet estándar, Fast Ethernet y Gigabit Ethernet se encuentran en la capa física. Debido a las mayores velocidades de estos estándares recientes, la menor duración de los tiempos de bit requiere una consideración especial. Como los bits ingresan al medio por menor tiempo y con mayor frecuencia, es fundamental la temporización. Esta transmisión a alta velocidad requiere de frecuencias cercanas a las limitaciones de ancho de banda para los medios de cobre. Esto hace que los bits sean más susceptibles al ruido en los medios de cobre.

Estos problemas requieren que Gigabit Ethernet utilice dos distintos pasos de codificación. La transmisión de datos se realiza de manera más eficiente utilizando códigos para representar el corriente binario de bits. Los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores características de la Relación entre Señal y Ruido.

En la capa física, los patrones de bits a partir de la capa MAC se convierten en símbolos. Los símbolos también pueden ser información de control tal como trama de inicio, trama de fin, condiciones de inactividad del medio. La trama se codifica en símbolos de control y símbolos de datos para aumentar la tasa de transferencia de la red.

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

7.2.2 1000BASE-T

Al instalar Fast Ethernet para aumentar el ancho de banda de las estaciones de trabajo, se comenzaron a crear cuellos de botella corriente arriba en la red. 1000BASE-T (IEEE 802.3ab) se desarrolló para proporcionar ancho de banda adicional a fin de ayudar a aliviar estos cuellos de botella. Proporcionó mayor desempeño a dispositivos tales como backbones dentro de los edificios, enlaces entre los switches, servidores centrales y otras aplicaciones de armarios para cableado así como conexiones para estaciones de trabajo de nivel superior. Fast Ethernet se diseñó para funcionar en los cables de cobre Cat 5 existentes y esto requirió que dicho cable aprobara la verificación de la Cat 5e. La mayoría de los cables Cat 5 instalados pueden aprobar la certificación 5e si están correctamente terminados. Uno de los atributos más importantes del estándar para 1000BASE-T es que es interoperable con 10BASE-T y 100BASE-TX.

Como el cable Cat 5e puede transportar, de forma confiable, hasta 125 Mbps de tráfico, obtener 1000 Mbps (Gigabit) de ancho de banda fue un desafío de diseño. El primer paso para lograr una 1000BASE-T es utilizar los cuatro pares de hilos en lugar de los dos pares tradicionales utilizados para 10BASE-T y 100BASE-TX. Esto se logra mediante un sistema de circuitos complejo que permite las transmisiones full duplex en el mismo par de hilos. Esto proporciona 250 Mbps por par. Con los cuatro pares de hilos,

proporciona los 1000 Mbps esperados. Como la información viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor.

La codificación de 1000BASE-T con la codificación de línea 4D-PAM5 se utiliza en UTP de Cat 5e o superior.. Esto significa que la transmisión y recepción de los datos se produce en ambas direcciones en el mismo hilo a la vez. Como es de esperar, esto provoca una colisión permanente en los pares de hilos. Estas colisiones generan patrones de voltaje complejos. Mediante los complejos circuitos integrados que usan técnicas tales como la cancelación de eco, la Corrección del Error de Envío Capa 1 (FEC) y una prudente selección de los niveles de voltaje, el sistema logra una tasa de transferencia de 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. ¹Con 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.

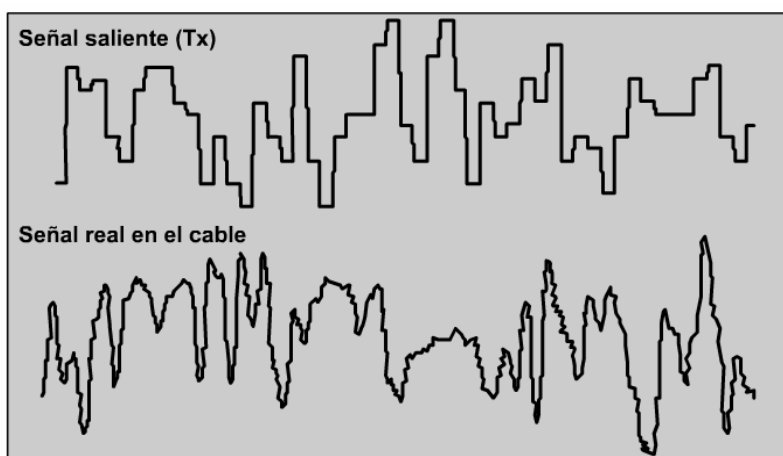


Figura 1

Los datos que provienen de la estación transmisora se dividen cuidadosamente en cuatro corrientes paralelas; luego se codifican, se transmiten y se detectan en paralelo y finalmente se reensamblan en una sola corriente de bits recibida. La Figura 2 representa la conexión full duplex simultánea en los cuatro pares de hilos. 1000BASE-T admite tanto las operaciones en half-duplex como las en full-duplex. El uso de 1000BASE-T en full-duplex está ampliamente difundido.

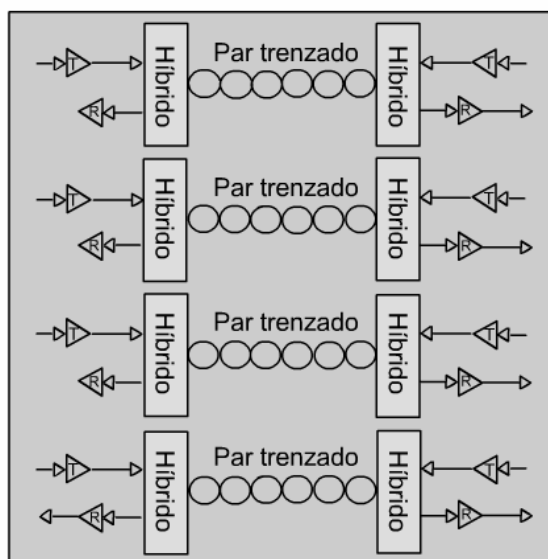


Figura 2

7.2.3 1000BASE-SX y LX

El estándar IEEE 802.3 recomienda Gigabit Ethernet en fibra como la tecnología de backbone de preferencia. ¹

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

Figura 1

La temporización, el formato de trama y la transmisión son comunes a todas las versiones de 1000 Mbps. En la capa física, se definen dos esquemas de codificación de la señal. 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.

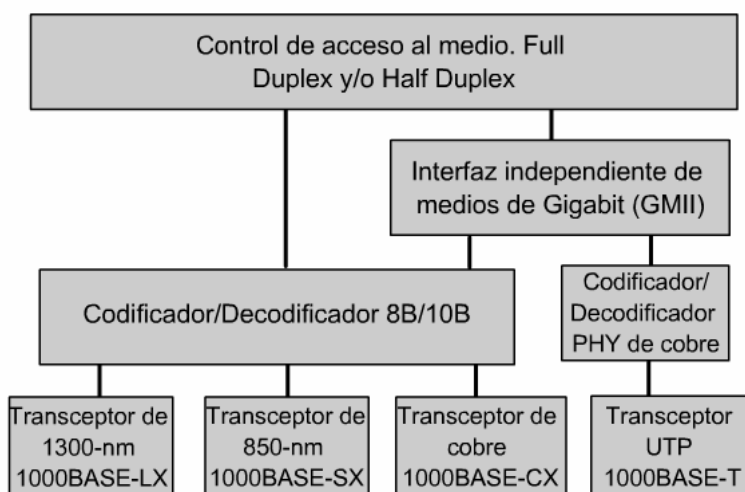


Figura 2

1000BASE-X utiliza una codificación 8B/10B convertida en la codificación de línea sin retorno a cero (NRZ). La codificación NRZ depende del nivel de la señal encontrado en la ventana de temporización para determinar el valor binario para ese período de bits. A diferencia de la mayoría de los otros esquemas de codificación descritos, este sistema de codificación va dirigido por los niveles en lugar de por los bordes. Es decir, determinar si un bit es un cero o un uno depende del nivel de la señal en vez del momento cuando la señal cambia de nivel.

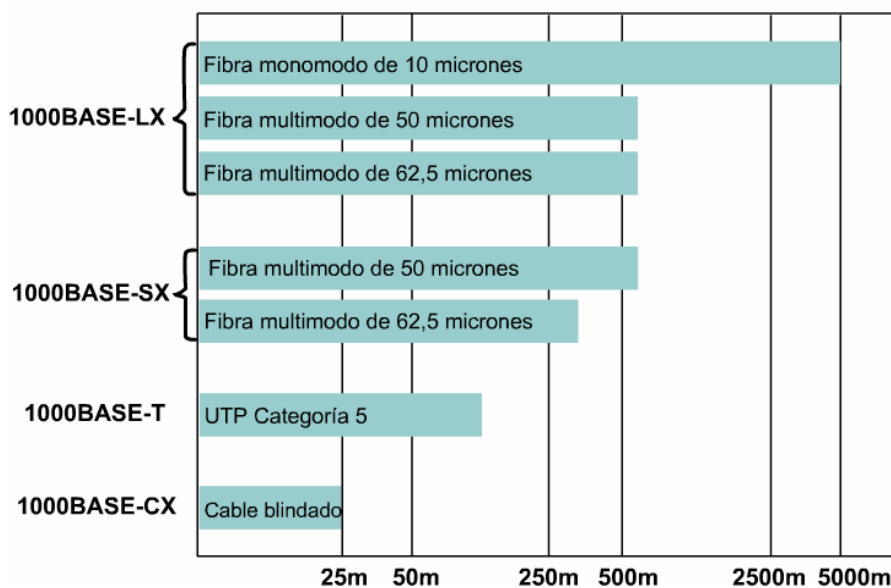


Figura 3

Las señales NRZ son entonces pulsadas hacia la fibra utilizando fuentes de luz de onda corta o de onda larga. La onda corta utiliza un láser de 850 nm o una fuente LED en fibra óptica multimodo (1000BASE-SX). Es la más económica de las opciones pero cubre distancias más cortas. La fuente láser de 1310 nm de onda larga utiliza fibra óptica monomodo o multimodo (1000BASE-LX). Las fuentes de láser utilizadas con fibra monomodo pueden cubrir distancias de hasta 5000 metros. Debido al tiempo necesario para encender y apagar por completo el LED o el láser cada vez, la luz se pulsa utilizando alta y baja energía. La baja energía representa un cero lógico y la alta energía, un uno lógico.

El método de Control de Acceso a los Medios considera el enlace como si fuera de punto a punto. Como se utilizan distintas fibras para transmitir (Tx) y recibir (Rx) la conexión de por sí es de full duplex. Gigabit Ethernet permite un sólo repetidor entre dos estaciones. La Figura 3 es un cuadro de comparación de medios de Ethernet 1000BASE

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 Figuras 1 y 2 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 máxima
Fibra multimodo 62,5µm	160	220 m
Fibra multimodo 62,5µm	200	275 m
Fibra multimodo 50µm	400	500 m
Fibra multimodo 50µm	500	500 m

Figura 1

Medio	Ancho de banda modal	Distancia máxima
Fibra multimodo 62,5µm	500	550 m
Fibra multimodo 50µm	400	550 m
Fibra multimodo 50µm	500	550 m
Fibra multimodo 10µm	N/A	5000 m

Figura 2

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

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

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

7.2.5 10-Gigabit Ethernet

Se adaptó el IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. Las similitudes básicas entre 802.3ae y 802.3, Ethernet original son notables. Esta Ethernet de 10-Gigabit (10GbE) está evolucionando no sólo para las LAN sino también para las MAN y las WAN.

Con un formato de trama y otras especificaciones de Capa 2 de Ethernet compatibles con estándares anteriores, 10GbE puede proporcionar mayores necesidades de ancho de banda que son interoperables con la infraestructura de red existente.

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

Parámetro	Valor
Período de bit	0.1 nsec
Ranura temporal	no es aplicable *
Espacio entre las tramas	96 bits **
Límite de intento de colisión	no es aplicable *
Límite de postergación de colisión	no es aplicable *
Tamaño de atascamiento de colisiones	no es aplicable *
Tamaño de trama máximo sin rotular	1518 octetos
Tamaño de trama mínimo	512 bits (64 octetos)
Límite de ráfaga	no es aplicable *
Relación de Ampliación de Espacio entre Tramas	104 bits ***

* 10-Gbps Ethernet no permite la operación half duplex, de manera que los parámetros que se relacionan con tiempos de bit y manejo de colisiones no se aplican.

** El valor mencionado es el espacio entre tramas oficial.

*** La Relación de Ampliación de Espacio entre Tramas se aplica exclusivamente a las definiciones 10GBASE-W.

En resumen, ¿cómo se compara 10GbE con otras variedades de Ethernet?

- El formato de trama es el mismo, permitiendo así la interoperabilidad entre todos los tipos de tecnologías antiguas, fast, gigabit y 10 Gigabit, sin retramado o conversiones de protocolo.
- El tiempo de bit es ahora de 0,1 nanosegundos. Todas las demás variables de tiempo caen en su correspondiente lugar en la escala.
- Como sólo se utilizan conexiones de fibra en full-duplex, el CSMA/CD no es necesario.
- Las subcapas de IEEE 802.3 dentro de las Capas OSI 1 y 2 se preservan en su mayoría, con pocos agregados para dar lugar a enlaces en fibra de 40 km e interoperabilidad con las tecnologías SONET/SDH.
- Entonces, es posible crear redes de Ethernet flexibles, eficientes, confiables, a un costo de punta a punta relativamente bajo.
- El TCP/IP puede correr en redes LAN, MAN y WAN con un método de Transporte de Capa 2.

El estándar básico que rige el CSMA/CD es IEEE 802.3. Un suplemento al IEEE 802.3, titulado 802.3ae, rige la familia de las 10GbE. Como es típico para las nuevas tecnologías, se están considerando una variedad de implementaciones, que incluye:

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

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.

La Figura 1 representa el caso particular del uso de cuatro fuentes láser de longitudes de onda apenas diferentes. Una vez recibida del medio, la corriente de señal óptica se desmultiplexa en cuatro distintas corrientes de señal óptica. Las cuatro corrientes de señal óptica entonces vuelven a convertirse en cuatro corrientes electrónicas de bits a medida que viajan, usando el proceso inverso a través de las subcapas hacia la capa MAC.

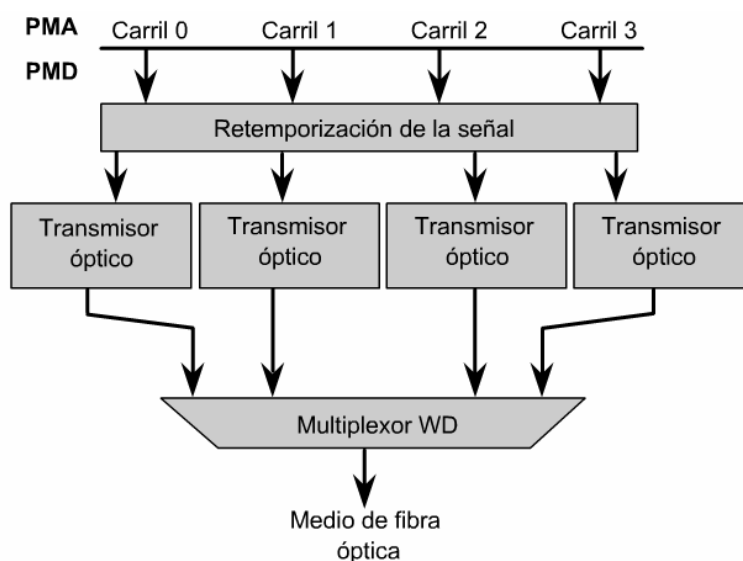


Figura 1

En la actualidad, la mayoría de los productos de 10GbE tienen forma de módulos, o tarjetas de línea, para agregar a los switches y a los routers de nivel superior. A medida que evolucionen las tecnologías de 10GbE, será posible esperar una creciente variedad de componentes para la transmisión de señales. A medida que evolucionen las tecnologías ópticas, se incorporarán mejores transmisores y receptores a estos productos, tomando ventaja adicional de la modularidad. Todas las variedades de 10GbE utilizan medios de fibra óptica. Los tipos de fibra incluyen fibra monomodo de 10μ y fibras multimodo de 50μ y 62.5μ. Admiten un rango de características de dispersión y de atenuación de la fibra, pero limitan las distancias de operación.

Aunque esta tecnología se limita a los medios de fibra óptica, algunas de las longitudes máximas para los cables son sorprendentemente cortas. 2 No se ha definido ningún repetidor para Ethernet de 10 Gigabits ya que explícitamente no admite las conexiones half duplex.

Tal como sucede con las versiones de 10 Mbps, 100 Mbps y 1000 Mbps, es posible modificar levemente algunas de las reglas de arquitectura. Los ajustes de arquitectura posibles están relacionados con la pérdida

de la señal y distorsión a lo largo del medio. Debido a la dispersión de la señal y otros problemas, el pulso de luz se vuelve indescifrable más allá de ciertas distancias.

Implementación	Longitud de onda	Medio	Ancho de banda modal mínimo	Distancia de operación
10GBASE-LX4	1310 nm	62.5µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	50µm MMF	400 MHz/km	2 - 240 m
10GBASE-LX4	1310 nm	50µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	10µm MMF	N/A	2 - 10 km
10GBASE-S	850 nm	62.5µm MMF	160 MHz/km	2 - 26 m
10GBASE-S	850 nm	62.5µm MMF	200 MHz/km	2 - 33 m
10GBASE-S	850 nm	50µm MMF	400 MHz/km	2 - 66 m
10GBASE-S	850 nm	50µm MMF	500 MHz/km	2 - 82 m
10GBASE-S	850 nm	50µm MMF	2000 MHz/km	2 - 300 m
10GBASE-L	1310 nm	10µm SMF	N/A	2 - 10 km
10GBASE-E	1550 nm	10µm SMF	N/A	2 - 30 km

Figura 2

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 presentado 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.

Cuando Ethernet era más lenta, en half-duplex, sujeta a colisiones y a un proceso "democrático" de prioridades, no se consideraba que tuviera las capacidades de Calidad de Servicio (QoS) necesarias para manejar cierto tipo de tráfico. Esto incluía por ejemplo la telefonía IP y el video multicast.

Las tecnologías de Ethernet de alta velocidad y full-duplex que ahora dominan el mercado están resultando ser suficientes a la hora de admitir aplicaciones intensivas inclusive las de QoS. Esto hace que las potenciales aplicaciones de Ethernet sean aún más amplias. Irónicamente, la capacidad de QoS de punta a punta ayudó a dar un empuje a ATM para escritorio y a la WAN a mediados de los 90, pero ahora es Ethernet y no ATM la que está realizando este objetivo.

Resumen

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

- Las similitudes y diferencias entre las Ethernet 10BASE5, 10BASE2 y 10BASE-T.
- La codificación Manchester
- Los factores que afectan los límites de temporización de Ethernet.
- Los parámetros de cableado 10BASE-T
- Las características y tipos principales de Ethernet de 100 Mbps
- La evolución de Ethernet
- Los métodos MAC, los formatos de trama y el proceso de transmisión de Gigabit Ethernet.
- Los usos de los medios y codificación específicos de Gigabit Ethernet.
- Las salidas de pin y el cableado típicos de las distintas implementaciones de Gigabit Ethernet.
- Las similitudes y diferencias entre Gigabit Ethernet y 10 Gigabit Ethernet.
- Las consideraciones arquitectónicas básicas de Gigabit Ethernet y 10 Gigabit Ethernet.

Módulo 8: Conmutación de Ethernet

Descripción general

Ethernet compartida funciona muy bien en circunstancias ideales. Cuando el número de dispositivos que intentan acceder a la red es bajo, el número de colisiones permanece dentro de los límites aceptables. Sin embargo, cuando el número de usuarios de la red aumenta, el mayor número de colisiones puede causar que el rendimiento sea intolerablemente malo. El puenteo se desarrolló para aliviar los problemas de rendimiento que surgieron con el aumento de las colisiones. La conmutación surgió del puenteo y se ha convertido en la tecnología clave de las LAN modernas de Ethernet.

Las colisiones y broadcasts son sucesos esperados en la networking moderna. Ellas, de hecho, están planeadas dentro del diseño de Ethernet y de las tecnologías de capa avanzadas. Sin embargo, cuando las colisiones y broadcasts ocurren en un número que se encuentra por encima del óptimo, el rendimiento de la red se ve afectado. El concepto de dominios de colisión y de broadcast trata las formas en que pueden diseñarse las redes para limitar los efectos negativos de las colisiones y broadcasts. Este módulo explora los efectos de las colisiones y broadcasts sobre el tráfico de red y luego describe cómo se utilizan los puentes y routers para segmentar las redes y mejorar el rendimiento.

Los estudiantes que completen este módulo deberán poder:

- Definir puenteo y conmutación.
- Definir y describir la tabla de memoria de contenido direccionable (Content Addressable Memory, CAM).
- Definir latencia.
- Describir los modos de conmutación de almacenamiento y envío y por método de corte.
- Explicar el protocolo Spanning Tree (Spanning Tree Protocol, STP).
- Definir colisiones, broadcasts y dominios de colisión y de broadcast.
- Identificar los dispositivos de las Capas 1, 2 y 3 utilizados para crear dominios de colisión y de broadcast.
- Discutir el flujo de datos y los problemas con broadcasts.
- Explicar la segmentación de la red y confeccionar una lista de los dispositivos utilizados en la creación de los segmentos.

8.1 Conmutación de Ethernet

8.1.1 Puenteo de Capa 2

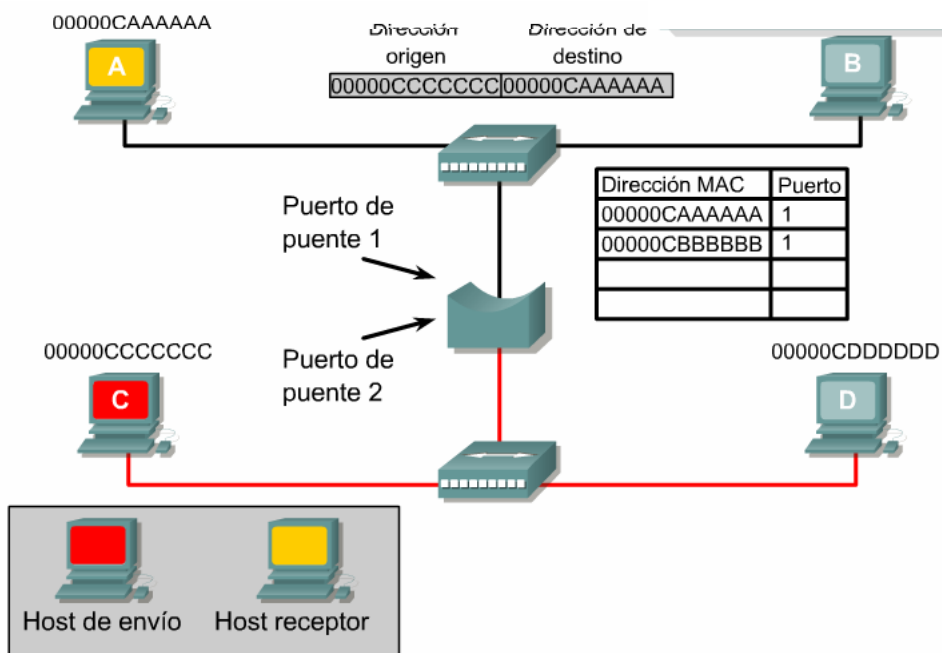


Figura 1

A medida que se agregan más nodos al segmento físico de Ethernet, aumenta la contención de los medios. Ethernet es un medio compartido, lo que significa que sólo un nodo puede transmitir datos a la vez. Al agregar más nodos, se aumenta la demanda sobre el ancho de banda disponible y se impone una carga adicional sobre los medios. Cuando aumenta el número de nodos en un solo segmento, aumenta la probabilidad de que haya colisiones, y esto causa más retransmisiones. Una solución al problema es dividir un segmento grande en partes y separarlo en dominios de colisión aislados.

Para lograr esto, un puente guarda una tabla de direcciones MAC y sus puertos asociados. El puente luego envía o descarta tramas basándose en las entradas de su tabla. Los pasos siguientes ilustran el modo de operación de un puente: ¹

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

Estos son los pasos que utiliza el puente para enviar y descartar tramas que se reciben en cualquiera de sus puertos.

8.1.2 Conmutación a nivel de Capa 2

Por lo general, un puente sólo tiene dos puertos y divide un dominio de colisión en dos partes. Todas las decisiones que toma el puente se basan en un direccionamiento MAC o de Capa 2 y no afectan el direccionamiento lógico o de Capa 3. Así, un puente dividirá el dominio de colisión pero no tiene efecto sobre el dominio lógico o de broadcast. No importa cuántos puentes haya en la red, a menos que haya un dispositivo como por ejemplo un router que funciona en el direccionamiento de Capa 3, toda la red compartirá el mismo espacio de dirección lógica de broadcast. Un puente creará más dominios de colisión pero no agregará dominios de broadcast. ¹

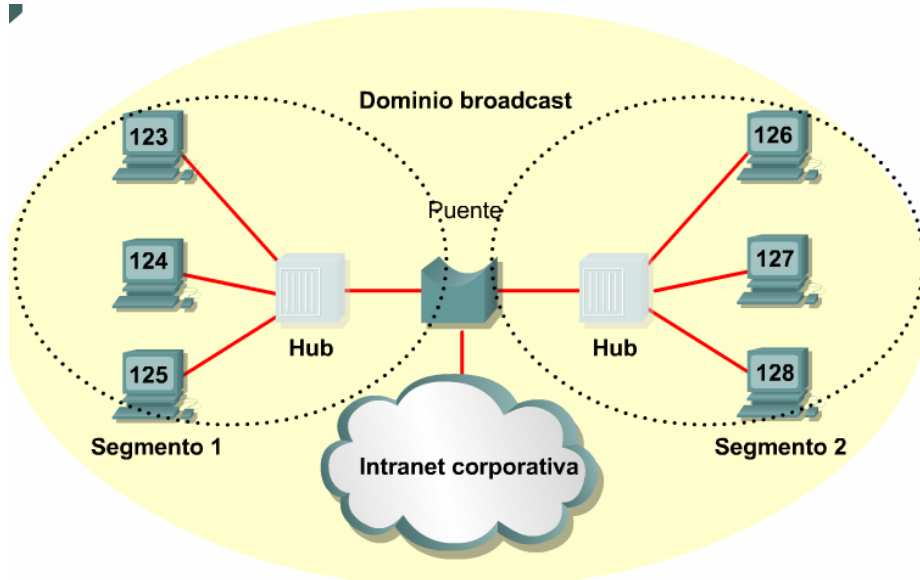
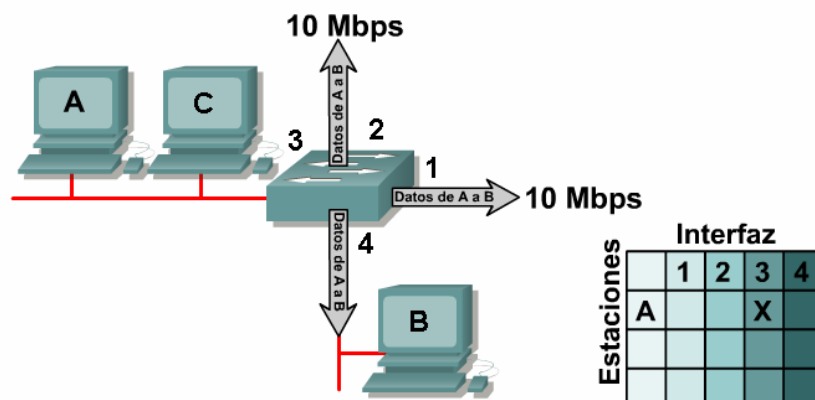


Figura 1

Un switch es básicamente un puente rápido multipuerto, que puede contener docenas de puertos. En vez de crear dos dominios de colisión, cada puerto crea su propio dominio de colisión. En una red de veinte nodos, existen veinte dominios de colisión si cada nodo está conectado a su propio puerto de switch. Si se incluye un puerto uplink, un switch crea veintiún dominios de colisión de un solo nodo. Un switch crea y mantiene de forma dinámica una tabla de memoria de contenido direccionable (Content Addressable Memory, CAM), que contiene toda la información MAC necesaria para cada puerto.

8.1.3 Operación de switches

Un switch es simplemente un puente con muchos puertos. Cuando sólo un nodo está conectado a un puerto de switch, el dominio de colisión en el medio compartido contiene sólo dos nodos. Los dos nodos en este segmento pequeño, o dominio de colisión, constan del puerto de switch y el host conectado a él. Estos segmentos físicos pequeños son llamados microsegmentos. ¹Otra capacidad emerge cuando sólo dos nodos se conectan. En una red que utiliza cableado de par trenzado, un par se usa para llevar la señal transmitida de un nodo al otro. Un par diferente se usa para la señal de retorno o recibida. Es posible que las señales pasen a través de ambos pares de forma simultánea. La capacidad de comunicación en ambas direcciones al mismo tiempo se conoce como full duplex. ²La mayoría de los switch son capaces de admitir full duplex, como también lo son las tarjetas de interfaz de red (Network Interface Card, NIC). En el modo full duplex, no existe contención para los medios. Así, un dominio de colisión ya no existe. En teoría, el ancho de banda se duplica cuando se usa full duplex.



- Envía paquetes sobre la base de su dirección MAC en la tabla de envíos
- Opera en la Capa 2 de OSI
- Conoce la ubicación de una estación examinando la dirección origen

Figura 1

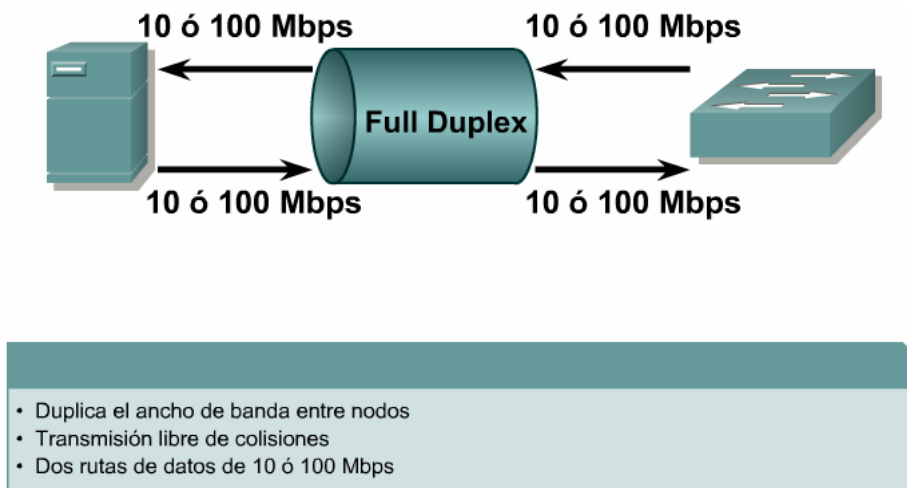


Figura 2

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. ¹ 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. ¹

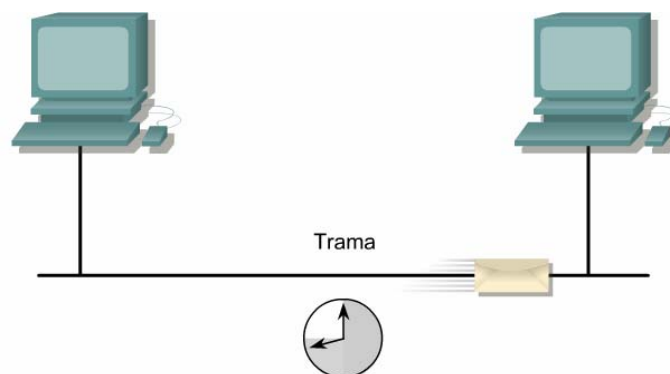


Figura 1

8.1.5 Modos 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. ¹Sin 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 se descubre que la trama es inválida, se descarta en este switch en vez de hacerlo en el destino final. Ya que toda la trama se almacena antes de ser enviada, este modo se llama de almacenamiento y envío. ²El punto medio entre los modos de corte y de almacenamiento y envío es el modo libre de fragmentos. El modo libre de fragmentos lee los primeros 64 bytes, que incluye el encabezado de la trama, y la conmutación comienza antes de que se lea todo el campo de datos y la checksum. Este modo verifica la confiabilidad de direccionamiento y la información del protocolo de control de enlace lógico (Logical Link Control, LLC) para asegurar que el destino y manejo de los datos sean correctos.

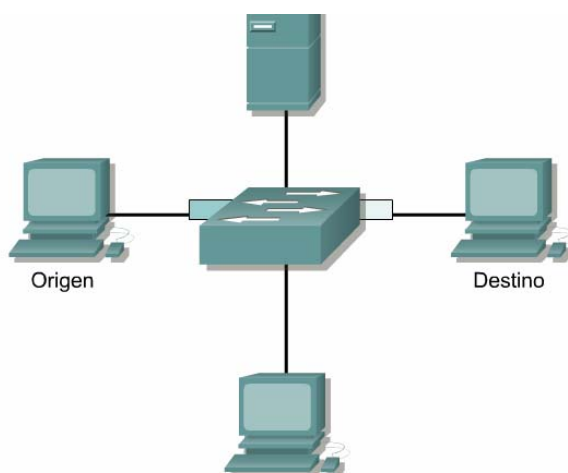


Figura 1

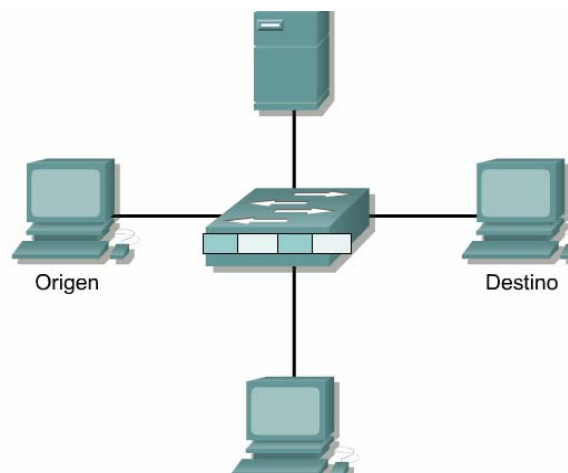


Figura 2

Al usar conmutación por métodos de corte, tanto el puerto origen como el destino deben operar a la misma velocidad de bit para mantener intacta la trama. Esto se denomina conmutación síncrona. Si las velocidades de bit no son iguales, la trama debe almacenarse a una velocidad de bit determinada antes de ser enviada a otra velocidad de bit. Esto se conoce como conmutación asíncrona. En la conmutación asimétrica se debe usar el método de almacenamiento y envío.

Una conmutación asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda, tal como una combinación de puertos de 1000 Mbps y de 100 Mbps. La conmutación asimétrica ha sido optimizada para el flujo de tráfico cliente/servidor en el que muchos clientes se comunican con el servidor de forma simultánea, lo cual requiere mayor ancho de banda dedicado al puerto del servidor para evitar un cuello de botella en ese puerto.

8.1.6 Protocolo de Spanning Tree (árbol de extensión)

Cuando varios switch están ubicados en un árbol jerárquico sencillo, es poco probable que ocurran bucles de conmutación. Sin embargo, a menudo las redes conmutadas se diseñan con rutas redundantes para ofrecer más confiabilidad y tolerancia a fallas. ¹Si 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: ²

- Bloquear
- Escuchar
- Aprender
- Enviar
- Desactivar

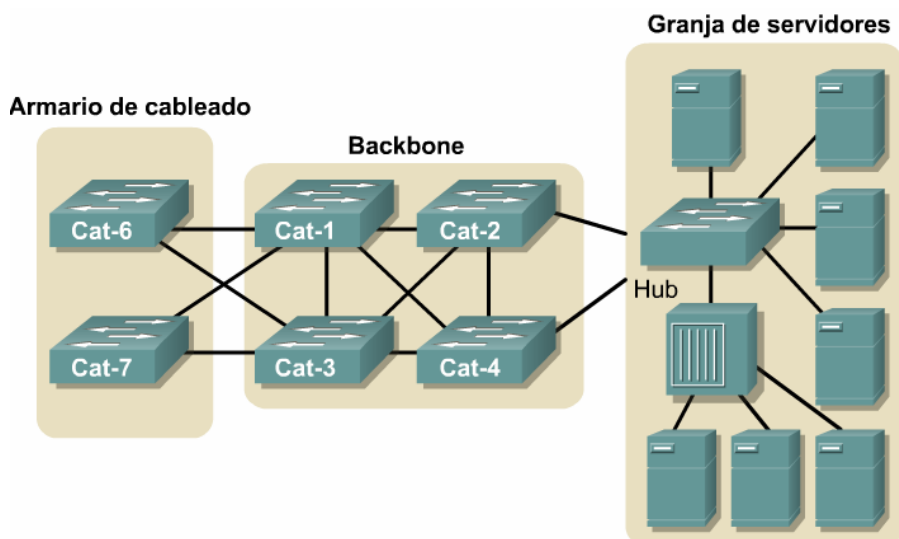


Figura 1

Estados	Propósito
Bloquear	Recibe sólo 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

Figura 2

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.

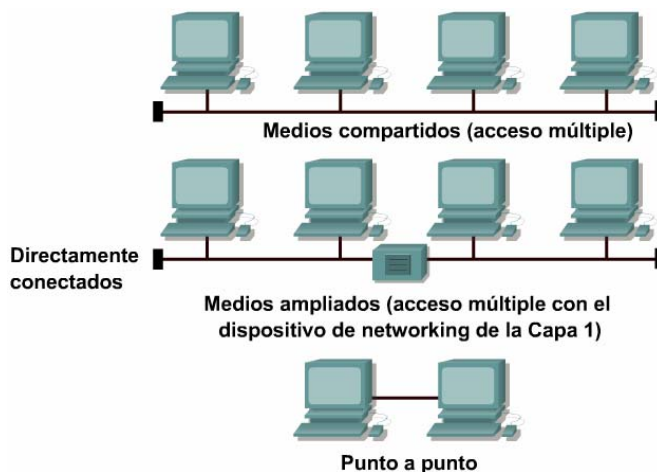


Figura 1

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

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

Es importante saber identificar un entorno de medios compartidos, debido a que las colisiones sólo ocurren en un entorno así. Un sistema de autopistas es un ejemplo de entorno compartido en el que las colisiones pueden ocurrir porque varios vehículos están utilizando las mismas rutas. A medida que más vehículos entran a las rutas, es probable que haya más colisiones. Una red de datos compartida se parece mucho a una autopista. Existen reglas para determinar quién tiene acceso a los medios de red, pero a veces las reglas simplemente no pueden manejar el volumen de tráfico, entonces se producen colisiones.

8.2.2 Dominios de colisión

Los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones. ¹ Las colisiones causan que la red sea ineficiente. Cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período de tiempo. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de la red.

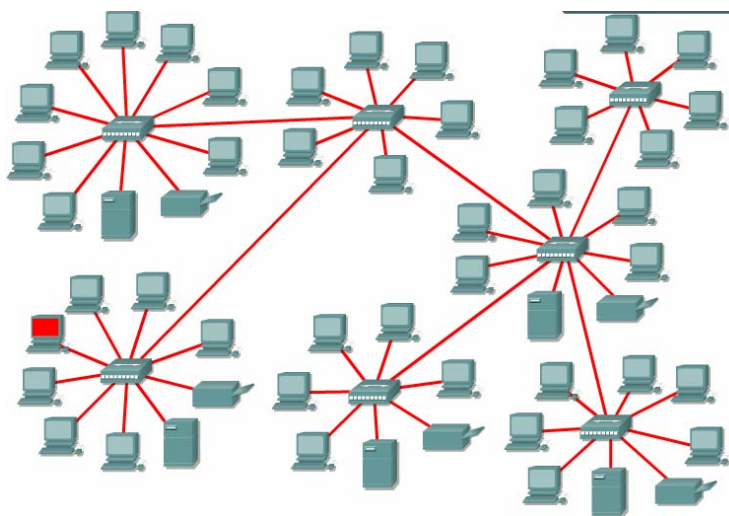


Figura 1

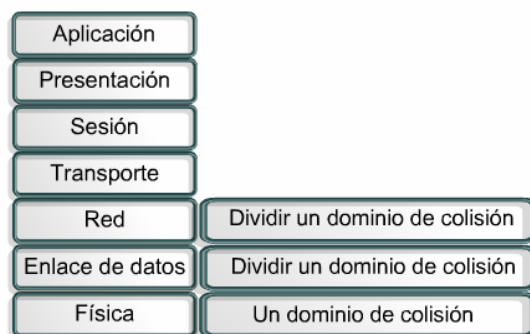


Figura 2

Los tipos de dispositivos que interconectan los segmentos de medios definen los dominios de colisión. ² 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 computadores en esa red exigen anchos de banda elevados. En fin, al colocar dispositivos de Capa 1 se extienden los dominios de colisión, pero la longitud de una LAN puede verse sobrepasada y causar otros problemas de colisión.

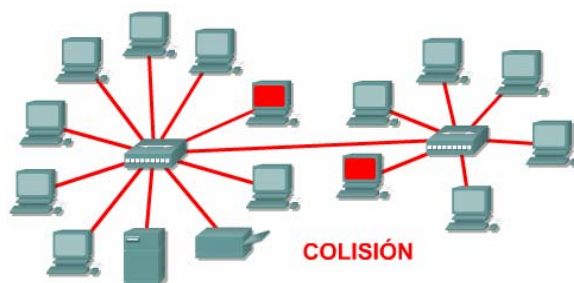
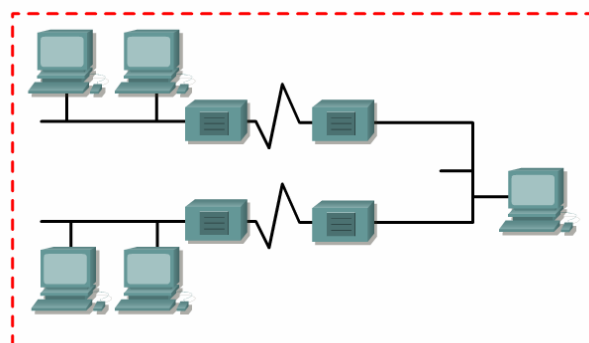


Figura 3

La regla de los cuatro repetidores en Ethernet establece que no puede haber más de cuatro repetidores o hubs repetidores entre dos computadores en la red. Para asegurar que una red 10BASE-T con repetidores funcionará de forma adecuada, el cálculo del retardo del recorrido de ida y vuelta debe estar dentro de ciertos límites, de otro modo todas las estaciones de trabajo no podrán escuchar todas las colisiones en la red. La latencia del repetidor, el retardo de propagación y la latencia de la NIC contribuyen a la regla de 4 repetidores. Si se excede la regla de los cuatro repetidores, esto puede llevar a la violación del límite de retardo máximo. Cuando se supera este límite de retardo, la cantidad de colisiones tardías aumenta notablemente. Una colisión tardía es una colisión que se produce después de la transmisión de los primeros 64 bytes de la trama. Cuando se produce una colisión tardía, no se requiere que los conjuntos de chips en las NIC retransmitan de forma automática. Estas tramas de colisión tardía agregan un retardo denominado retardo de consumo. Con el aumento del retardo de consumo y la latencia, se deteriora el rendimiento de la red.



----- = Dominio de colisión

Figura 4

(retardos del repetidor + retardos del cable + retardos de la NIC) x 2 máximo retardo de recorrido de ida y vuelta
Retardos del repetidor para repetidor 10BASE-TP < 2 microsegundos. Retardos de cable ~ 0,55 microsegundos por 100 meters. Retardos de NIC ~ 1 microsegundo por NIC
Retardo máximo de recorrido de ida y vuelta (el tiempo de bit de 10BASE-T de 0,1 microsegundos multiplicado por el tamaño mínimo de trama de 512 bits) es 51,2 microsegundos.

Figura 5

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

- Cinco segmentos de medios de red.

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

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

8.2.3 Segmentación

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

Una habilidad importante de todo profesional de networking, es la capacidad de reconocer los dominios de colisión. **1** Conectar varios computadores a un solo medio de acceso compartido que no tiene ningún otro dispositivo de networking conectado, crea un dominio de colisión. Esta situación limita el número de computadores que pueden utilizar el medio, también llamado segmento. Los dispositivos de Capa 1 amplían pero no controlan los dominios de colisión.

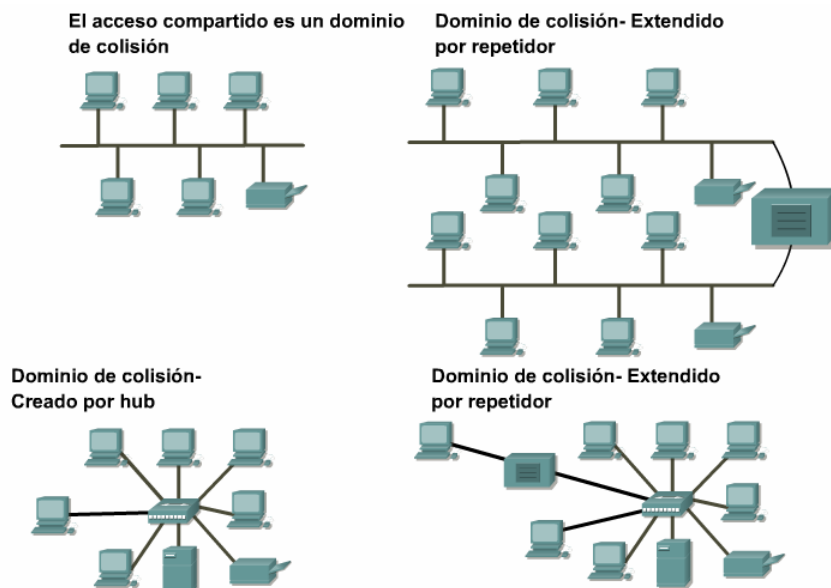


Figura 1

Los dispositivos de Capa 2 dividen o segmentan los dominios de colisión. **2** 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.

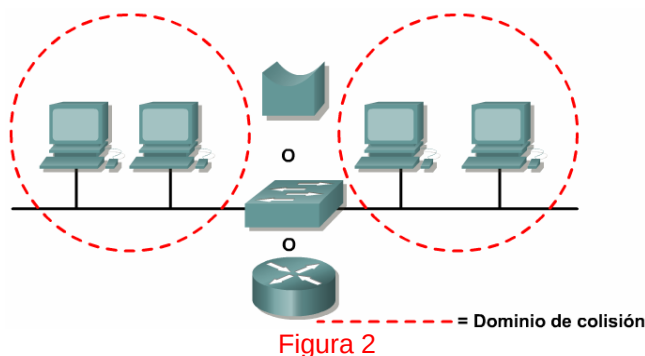


Figura 2

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.

8.2.4 Broadcasts de Capa 2

Para comunicarse con todos los dominios de colisión, los protocolos utilizan tramas de broadcast y multicast a nivel de Capa 2 en el modelo OSI. ¹ Cuando un nodo necesita comunicarse con todos los hosts de la red, envía una trama de broadcast con una dirección MAC destino 0xFFFFFFFFFFFFFF. Esta es una dirección a la cual debe responder la tarjeta de interfaz de la red (Network Interface Card, NIC) de cada host.

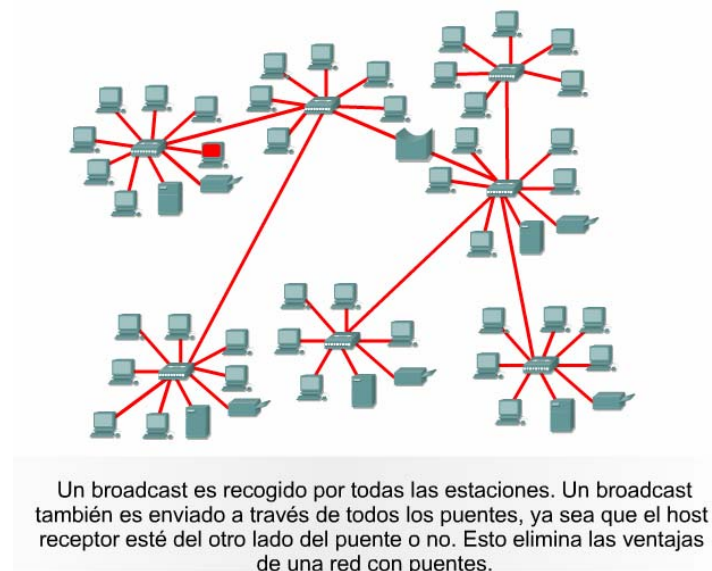


Figura 1

Los dispositivos de Capa 2 deben inundar todo el tráfico de broadcast y multicast. La acumulación de tráfico de broadcast y multicast de cada dispositivo de la red se denomina radiación de broadcast. En algunos casos, la circulación de radiación de broadcast puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones. En este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de broadcast. La probabilidad de las tormentas de broadcast aumenta a medida que crece la red conmutada.

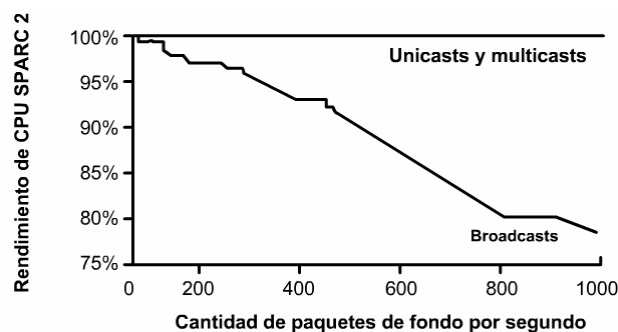


Figura 2

Como la NIC tiene que interrumpir a la CPU para procesar cada grupo de broadcast o multicast al que pertenece, el efecto de radiación de broadcast afecta el rendimiento de los hosts de la red. La Figura ²

muestra los resultados de pruebas que Cisco condujo sobre el efecto de la radiación de broadcast en el rendimiento de un CPU de Sun SPARCstation 2 usando una tarjeta Ethernet estándar incorporada. Como se ve en los resultados, los broadcasts que inundan la red efectivamente pueden desconectar una estación de trabajo IP. Aunque parezca extremo, durante las tormentas de broadcast, se han observado picos de miles de broadcasts por segundo. Pruebas en un entorno controlado con una variedad de broadcasts y multicasts de la red mostraron una degradación del sistema mensurable a tan sólo 100 broadcasts o multicasts por segundo.

La mayoría de las veces, el host no se beneficia al procesar el broadcast, ya que no es el destino buscado. 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. ³Aunque los números en la figura pudieran parecer bajos, representan una red promedio IP bien diseñada. Cuando el tráfico de broadcast y multicast hace un pico debido a una tormenta, la pérdida pico de la CPU puede tener una magnitud mayor al promedio. Las tormentas de broadcast pueden originarse en un dispositivo que requiere información de una red que ha crecido demasiado. La petición original recibe tantas respuestas que el dispositivo no las puede procesar, o la primera petición desencadena peticiones similares de otros dispositivos que efectivamente bloquean el flujo de tráfico en la red.

Cantidad de hosts	Porcentaje promedio de pérdida de CPU por host
100	.14
1000	.96
10000	9.15

Figura 3

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.

8.2.5 Dominios de broadcast

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. ¹ Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host. Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast. En otras palabras,

todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen una encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.

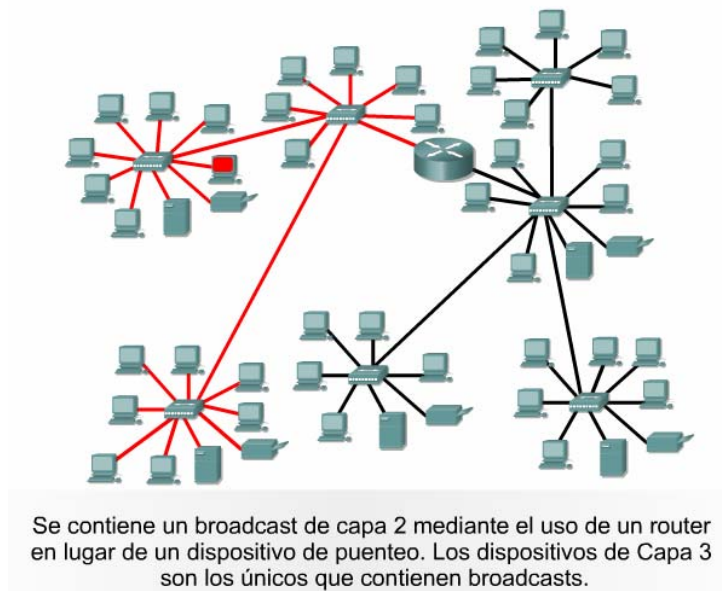


Figura 1

Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe ya haberlo procesado y la información de la trama debe haber sido eliminada. El envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC. Para que un paquete pueda enviarse, debe contener una dirección IP que esté por afuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

8.2.6 Introducción al flujo de datos

El flujo de datos en un contexto de dominios de colisión y de broadcast se centra en la forma en que las tramas se propagan a través de la red. Se refiere al movimiento de datos a través de los dispositivos de Capa 1, 2 y 3 y a la manera en que los datos deben encapsularse para poder realizar esa travesía en forma efectiva. Recuerde que los datos se encapsulan en la capa de la red con una dirección de origen y destino IP, y en la capa de enlace de datos con una dirección MAC origen y destino. ¹

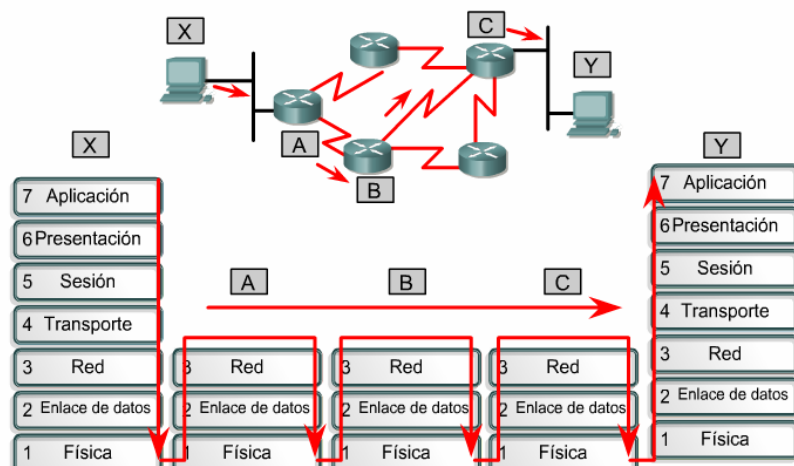


Figura 1

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.

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

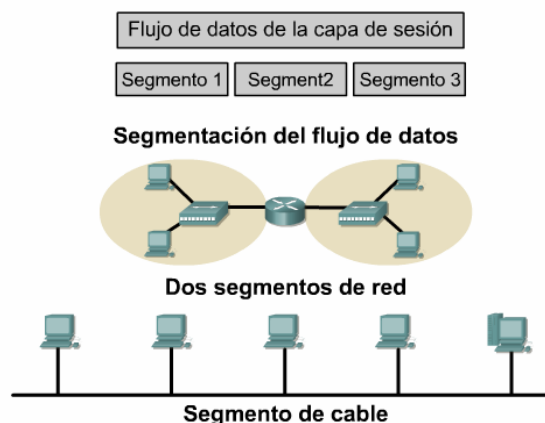
8.2.7 ¿Qué es un segmento de red?

Como ocurre con muchos términos y siglas, segmento tiene varios significados. El diccionario define el término de la siguiente manera:

- Una sección distinta de algo.
- Una de las partes en las que una entidad, o cantidad se divide o es marcada por límites naturales o algo similar a un límite natural.

En el contexto de la comunicación de datos, se utilizan las siguientes definiciones:

- Sección de una red limitada por puentes, routers o switches
- En una LAN que usa topología de bus, un segmento es un circuito de corriente continua que con frecuencia se conecta a otros segmentos similares con repetidores.
- Término usado en la especificación TCP para describir una sola unidad de capa de transporte de información. Los términos datagrama, mensaje, y paquete también se usan para describir agrupamientos de información lógicos en varias capas del modelo de referencia OSI y en varios círculos tecnológicos.



En networking, hay distintos tipos de segmentos. El significado del término "segmentos" depende del contexto de una oración.

Figura 1

Para definir correctamente el término "segmento", se debe presentar el contexto del uso junto con la palabra. Si un segmento se usa en un contexto de TCP, se define como una sección distinta de datos. Si la palabra segmento se utiliza en un contexto de medios físicos de networking en una red enrutada, será visto como una de las partes o secciones de una red total. ¹

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.

Módulo 9: Conjunto de protocolos TCP/IP y direccionamiento IP

Descripción general

Internet se desarrolló para brindar una red de comunicación que pudiera continuar funcionando en tiempos de guerra. Aunque la Internet ha evolucionado en formas muy diferentes a las imaginadas por sus arquitectos, todavía se basa en un conjunto de protocolos TCP/IP. El diseño de TCP/IP es ideal para la poderosa y descentralizada red que es Internet. Muchos de los protocolos utilizados hoy en día se diseñaron utilizando el modelo TCP/IP de cuatro capas.

Resulta útil conocer los modelos de networking OSI y TCP/IP. Cada modelo ofrece su propia estructura para explicar cómo funciona una red, pero los dos comparten muchas características. La falta de comprensión de cualquier de los dos modelos puede hacer que un administrador de sistemas no cuente con la información suficiente para determinar por qué una red funciona de cierta forma.

Todo dispositivo conectado a Internet que desee comunicarse con otros dispositivos en línea debe tener un identificador exclusivo. El identificador se denomina dirección IP porque los Routers utilizan un protocolo de la capa tres, el protocolo IP, para encontrar la mejor ruta hacia dicho dispositivo. 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 computador 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 temporal 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.

Los estudiantes que completen este módulo deberán poder:

- Explicar por qué se desarrolló la Internet y cómo el TCP/IP se ajusta al diseño de la misma.
- Nombrar las cuatro capas del modelo TCP/IP.
- Describir las funciones de cada capa del modelo TCP/IP.
- Comparar el modelo OSI con el TCP/IP.
- Describir la función y la estructura de las direcciones IP.
- Comprender por qué es necesaria la división en subredes.
- Explicar la diferencia entre direccionamiento público y privado.
- Comprender la función de las direcciones IP reservadas.
- Explicar el uso del direccionamiento estático y dinámico para un dispositivo.
- Comprender cómo el direccionamiento dinámico puede realizarse con RARP, BootP y DHCP.
- Utilizar ARP para obtener direcciones MAC a fin de poder enviar un paquete a otro dispositivo.
- Comprender los problemas relacionados con el direccionamiento entre redes.

9.1 Introducción a TCP/IP

9.1.1 Historia y futuro de 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. ¹Para 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.

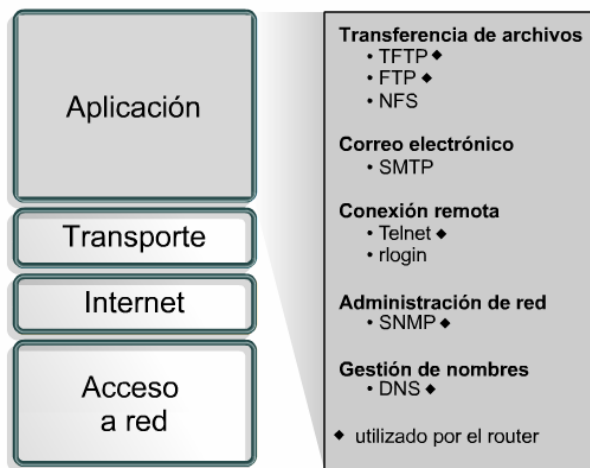


Figura 1

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 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. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:



- **Protocolo de transferencia de archivos (FTP):** es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.
- **Protocolo trivial de transferencia de archivos (TFTP):** es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP). Los Routers utilizan el TFTP para transferir los archivos de configuración e imágenes IOS de Cisco y para transferir archivos entre los sistemas que admiten TFTP. Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.
- **Sistema de archivos de red (NFS):** es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por Sun Microsystems que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.

- **Protocolo simple de transferencia de correo (SMTP):** administra la transmisión de correo electrónico a través de las redes informáticas. No admite la transmisión de datos que no sea en forma de texto simple.
- **Emulación de terminal (Telnet):** Telnet tiene la capacidad de acceder de forma remota a otro computador. Permite que el usuario se conecte a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.
- **Protocolo simple de administración de red (SNMP):** es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.
- **Sistema de denominación de dominio (DNS):** es un sistema que se utiliza en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.

9.1.3 La capa de transporte

La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. Esta capa forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. ¹ Los protocolos de transporte segmentan y reensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

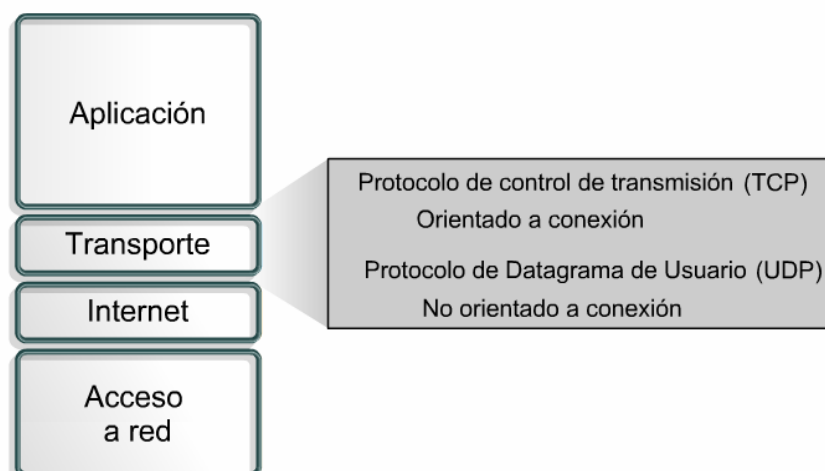


Figura 1

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. ² La nube maneja los aspectos tales como la determinación de la mejor ruta. ³

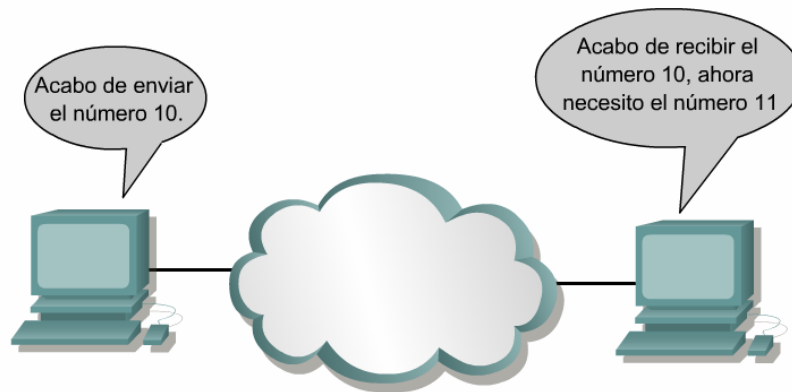


Figura 2

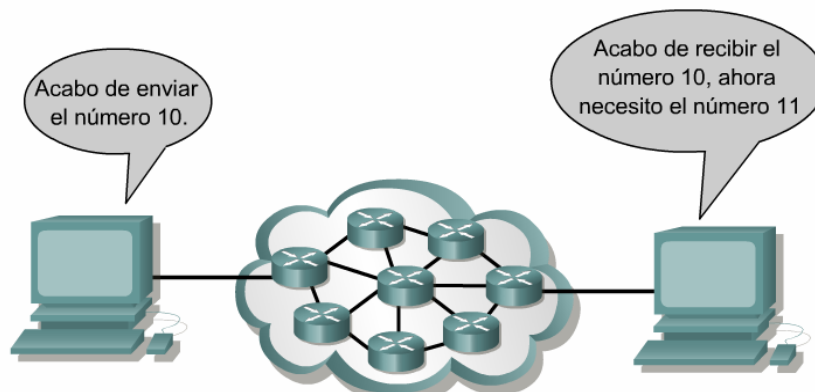


Figura 3

9.1.4 La capa de Internet

El propósito de la capa de Internet es seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurre en esta capa.

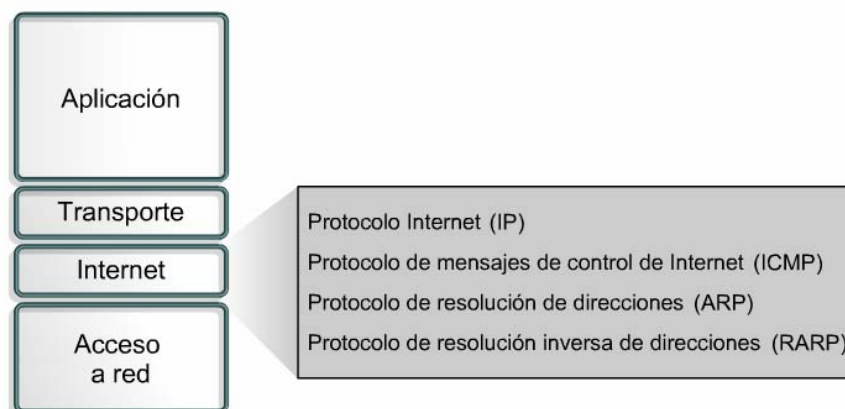


Figura 1

Los siguientes protocolos operan en la capa de Internet TCP/IP: **1**

- IP proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- El Protocolo de mensajes de control en Internet (ICMP) suministra capacidades de control y envío de mensajes.
- El Protocolo de resolución de direcciones (ARP) determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.
- El Protocolo de resolución inversa de direcciones (RARP) determina las direcciones IP cuando se conoce la dirección MAC.

El IP ejecuta las siguientes operaciones: 2

- Define un paquete y un esquema de direccionamiento.
- Transfiere los datos entre la capa Internet y las capas de acceso de red.
- Enruta los paquetes hacia los hosts remotos.

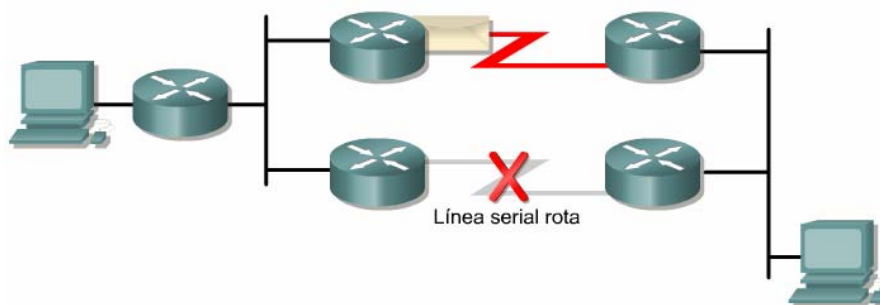


Figura 2

Por último, a modo de aclaración de la terminología, a veces, se considera a IP como protocolo poco confiable. Esto no significa que IP no enviará correctamente los datos a través de la red. Llamar al IP, protocolo poco confiable simplemente significa que IP no realiza la verificación y la corrección de los errores. Dicha función la realizan los protocolos de la capa superior desde las capas de transporte o aplicación.

9.1.5 La capa de acceso de red

La capa de acceso de red también se denomina capa de host a red. 1 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 física y de enlace de datos del modelo OSI.

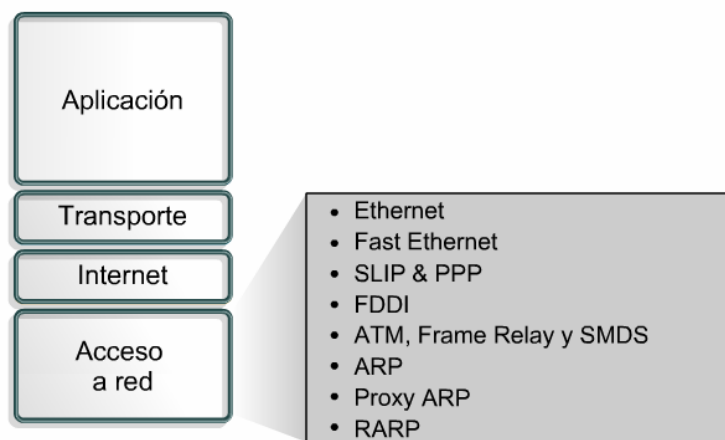


Figura 1

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. Esto puede generar confusión en los usuarios. La mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet del modelo TCP/IP.

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.

Un buen ejemplo de una configuración de la capa de acceso de red sería configurar un sistema Windows utilizando una NIC de otra empresa. De acuerdo con la versión de Windows, la NIC sería automáticamente

detectada por el sistema operativo y luego se instalarían los controladores adecuados. Si esta fuera una versión de Windows antigua, el usuario tendría que especificar el controlador de la tarjeta de la red. El fabricante de la tarjeta provee estos controladores en formato de disco o en CD-ROM.

9.1.6 Comparaión entre el modelo OSI y el TCP/IP

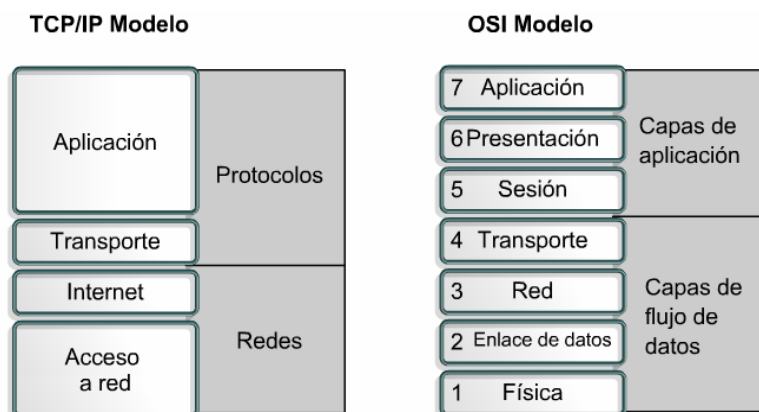
La siguiente es una comparación de los modelos OSI y TCP/IP comparando sus similitudes y diferencias:

Similitudes entre los modelos OSI y TCP/IP:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes y no de conmutación por circuito.
- Los profesionales de networking deben conocer ambos modelos.

Diferencias entre los modelos OSI y TCP/IP:

- TCP/IP combina las capas de presentación y de sesión en una capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.



La Internet se desarrolla de acuerdo con los estándares de los protocolos TCP/IP. El modelo TCP/IP gana credibilidad gracias a sus protocolos. A diferencia, en general, las redes no se contruyen a base del protocolo OSI. El modelo OSI se utiliza como guía para comprender el proceso de comunicación.

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 el computador origen y destino y los computadores 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 computadores 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 computador de la red. Para que un hardware nuevo funcione correctamente, se requiere de la modificación del software. Cualquier falla en un computador 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 computadores 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.

La Figura 1 resume la conexión de una red física a otra por medio de un computador especial que recibe el nombre de Router. Estas redes se describen como conectadas directamente al Router. Se necesita un Router para tomar toda decisión necesaria con respecto a la ruta para que las dos redes que se comuniquen. Hacen falta muchos Routers para administrar los grandes volúmenes del tráfico en las redes.

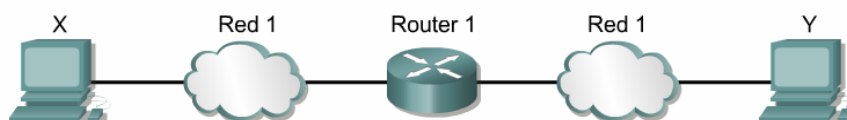


Figura 1

La Figura 2 amplía la idea a tres redes físicas conectadas con dos Routers. Los Routers toman las decisiones complejas para que todos los usuarios de todas las redes puedan comunicarse entre sí. No todas las redes están conectadas directamente a otra. El Router debe contar con alguna metodología para manejar esta situación.

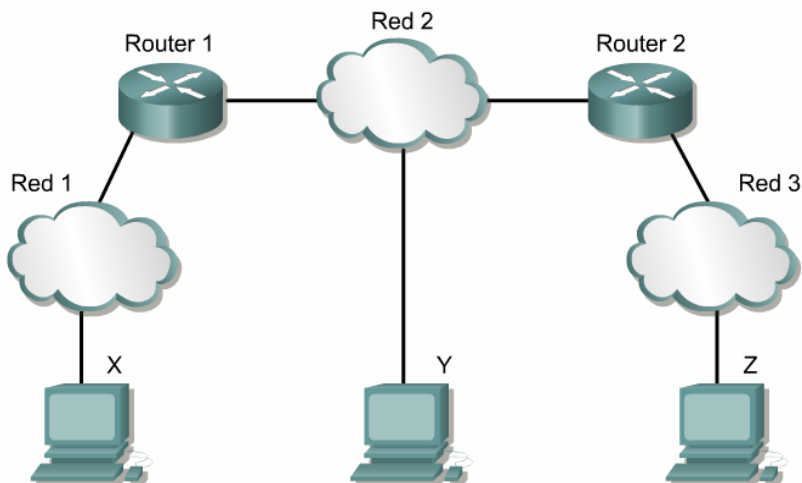


Figura 2

Una opción es que el Router guarde una lista de todos los computadores y todas las rutas hacia ellos. Entonces, el Router decidirá cómo enviar los paquetes de datos a base de esta tabla de referencia. El envío se basa en la dirección IP del computador destino. Esta opción resulta más difícil a medida que crece el número de usuarios. La escalabilidad aparece cuando un Router guarda una lista de todas las redes, pero deja los detalles del envío local a las redes físicas locales. En esta situación, los Routers envían los mensajes a otros Routers. Cada uno comparte la información acerca de cuáles son las redes a las que está conectado. Se construye así la tabla de enrutamiento.

La Figura 3 muestra la transparencia que los usuarios requieren. Sin embargo, las estructuras lógicas y físicas dentro de la nube Internet pueden ser extremadamente complejas como muestra la Figura 4. La Internet ha crecido rápidamente para permitir el ingreso de más y más usuarios. El hecho que haya crecido

de tal forma, con más de 90 000 rutas centrales y 300 000 000 usuarios finales es prueba de la solidez de la arquitectura de la Internet.

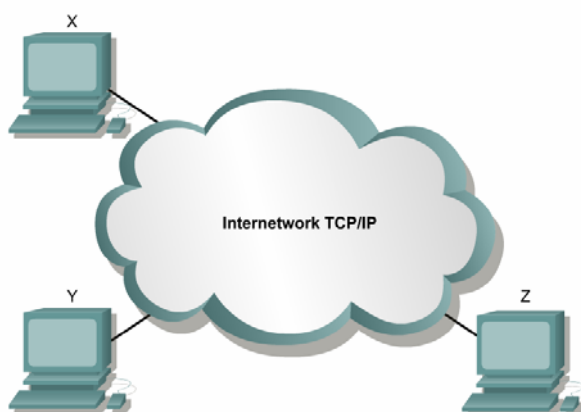


Figura 3

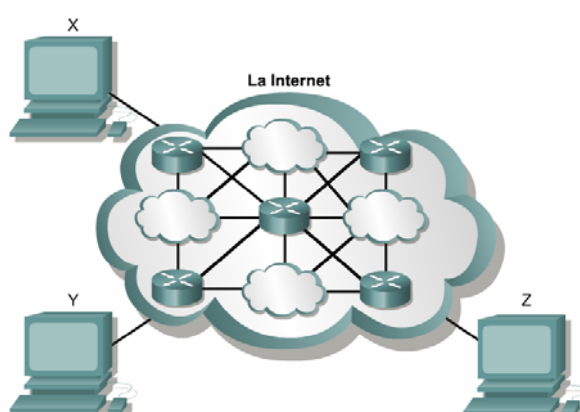


Figura 4

Dos computadores, 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 1 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.

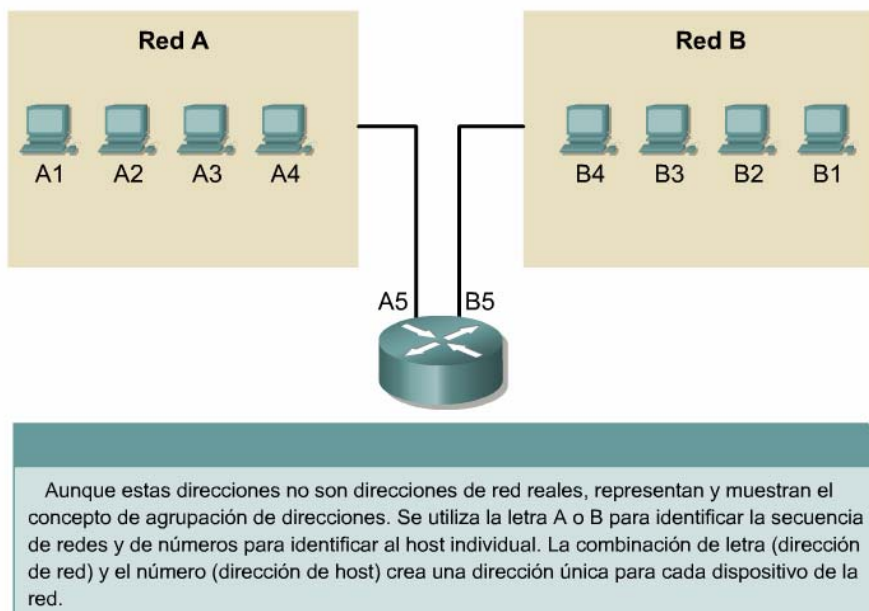


Figura 1

Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador 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 computadores 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 computador 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 un computador localice otro computador en la red. Todos los computadores 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.

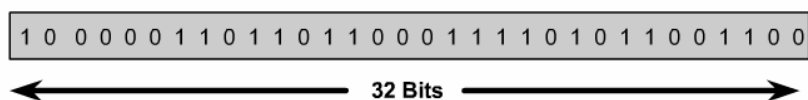


Figura 2

Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura 2 muestra un número de 32 bits de muestra. Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado. En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. Por ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos. Tanto los números binarios como los decimales de la Figura 3 representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada. Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.

Binario: 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001
 Decimal: 192.168.1.8 y 192.168.1.9

Los números binarios y decimales representan los mismos valores pero es mucho más fácil ver con los valores decimales punteados. Este es uno de los problemas más comunes que se encuentran al trabajar directamente con los números binarios. Las largas cadenas de unos y ceros repetidos aumentan la probabilidad de errores de transposición y omisión.

Figura 3

Resulta más sencillo observar la relación entre los números 192.168.1.8 y 192.168.1.9, mientras que 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001 no son fáciles de reconocer. Al observar los binarios, resulta casi imposible apreciar que son números consecutivos.

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. Es posible que el estudiante encuentre que otros métodos son más fáciles. Es cuestión de preferencia personal.

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Figura 1

Al convertir un número decimal a binario, se debe determinar la mayor potencia de dos que pueda caber en el número decimal. 1 Si se ha diseñado este proceso para trabajar con computadores, 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 computadores, 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. 2

Potencia de la posición	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor decimal	104	104	40	8	8	0	0	0
Valor de la posición	128	64	32	16	8	4	2	1
Conteo binario	0	1	1	0	1	0	0	0
Residuo	104	40	8	8	0	0	0	0

Figura 2

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 descrito, se llega a determinar que el número decimal un millón es equivalente al número binario 00001111 01000010 01000000.

La conversión de binario a decimal es el proceso inverso. Simplemente coloque el binario en la tabla y, si se encuentra un uno en una posición de la columna, agregue el valor al total.

9.2.3 Direccionamiento IPv4

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino. 1 Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red. Este sistema funciona de la misma forma que un sistema nacional de correo. Cuando se envía una carta, primero debe enviarse a la oficina de correos de la ciudad destino, utilizando el código postal. Dicha oficina debe entonces localizar el destino final en la misma ciudad utilizando el domicilio. Es un proceso de dos pasos.

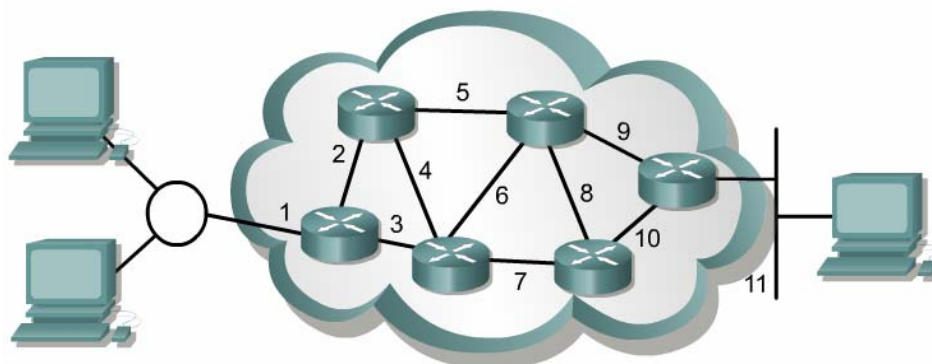
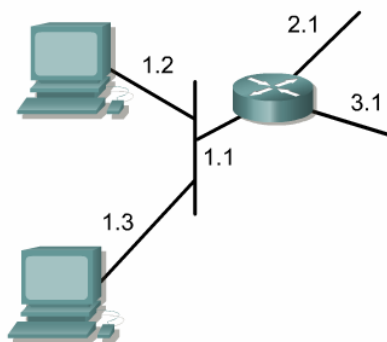


Figura 1

De igual manera, cada dirección IP consta de dos partes. 2 Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red. Como muestra la Figura 3, cada octeto varía de 0 a 255. Cada uno de los octetos se divide en 256 subgrupos y éstos, a su vez, se dividen en otros 256 subgrupos con 256 direcciones cada uno. Al referirse a una dirección de grupo inmediatamente arriba

de un grupo en la jerarquía, se puede hacer referencia a todos los grupos que se ramifican a partir de dicha dirección como si fueran una sola unidad.



Red	Host
1	1 2 3
2	1
3	1

Figura 2

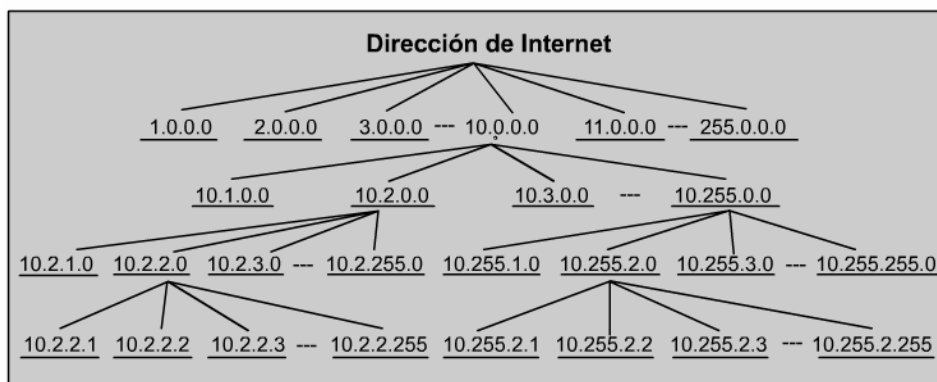


Figura 3

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.

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

Figura 4

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. ⁴ ⁵ 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 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 5

9.2.4 Direcciones IP Clase, A, B, C, D y E

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases. **1** Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host. **2** Un bit o una secuencia de bits al inicio de cada dirección determina su clase.

Clase A	Red	Host		
Octet	1	2	3	4

Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Figura 1

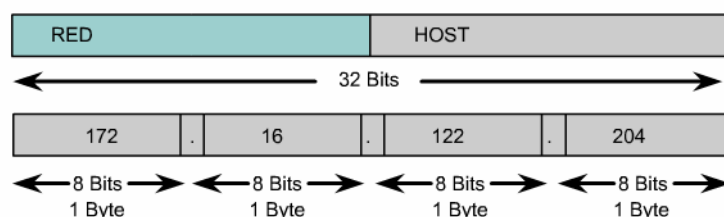


Figura 2

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles. **3** Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

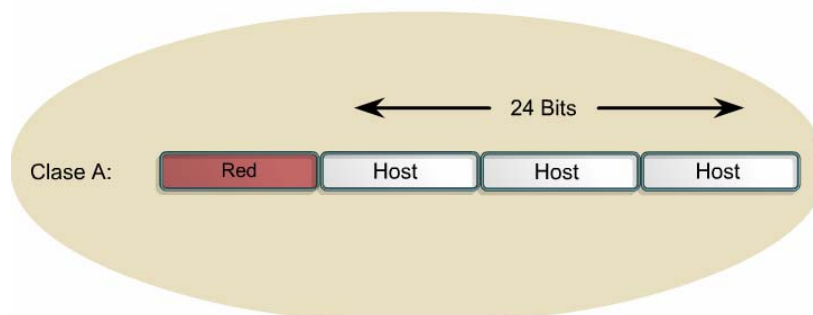


Figura 3

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. ⁴ 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.

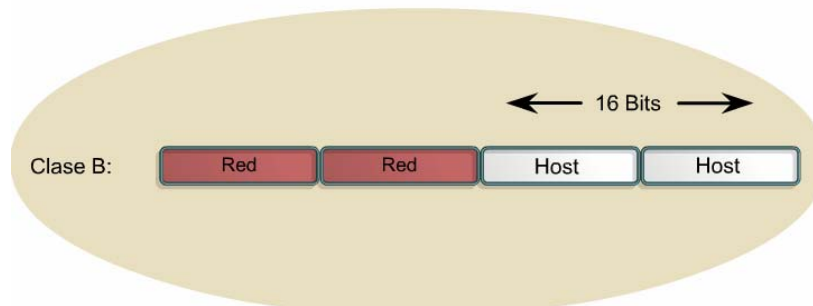


Figura 4

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. ⁵ Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.

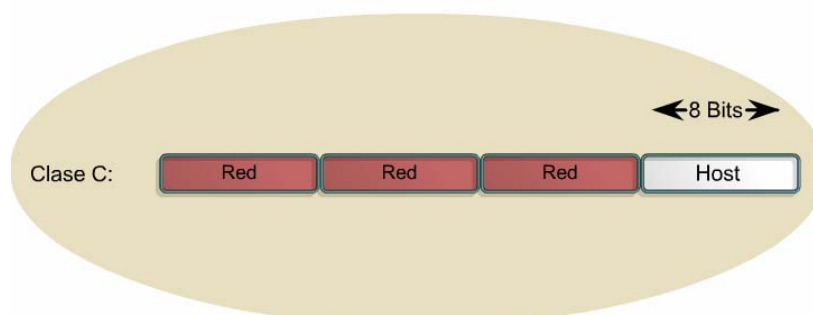


Figura 5

Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

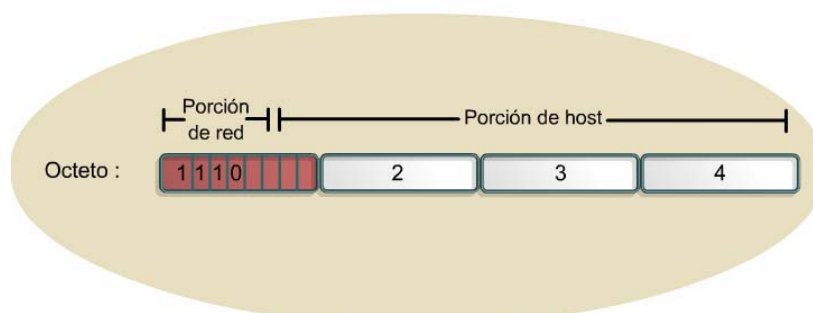


Figura 6

La dirección Clase D se creó para permitir multicast en una dirección IP. ⁶ Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de

direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

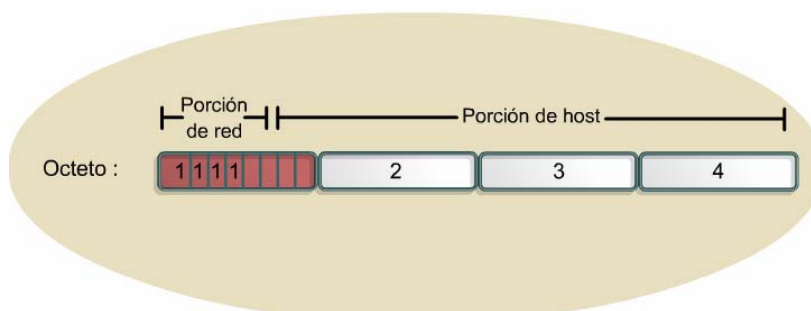


Figura 7

La Figura 8 muestra el rango de las direcciones IP 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 8

9.2.5 Direcciones IP reservadas

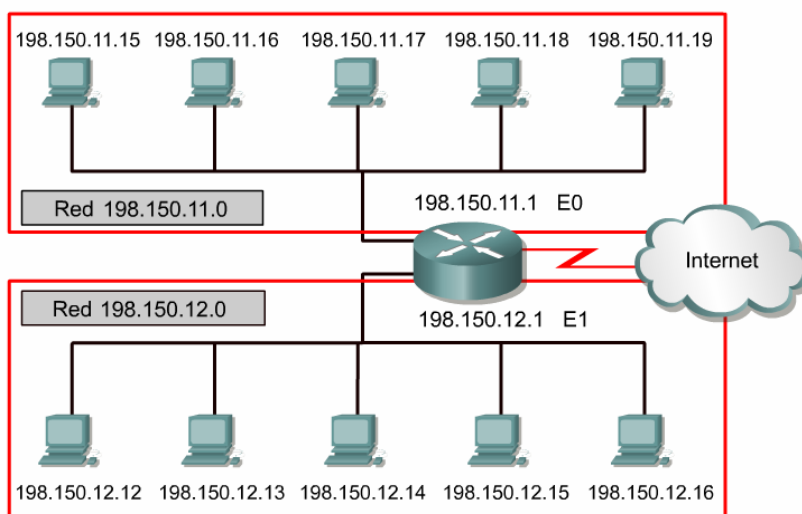


Figura 1

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 1, 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 2, 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). La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que la dirección de broadcast es 198.150.12.255.

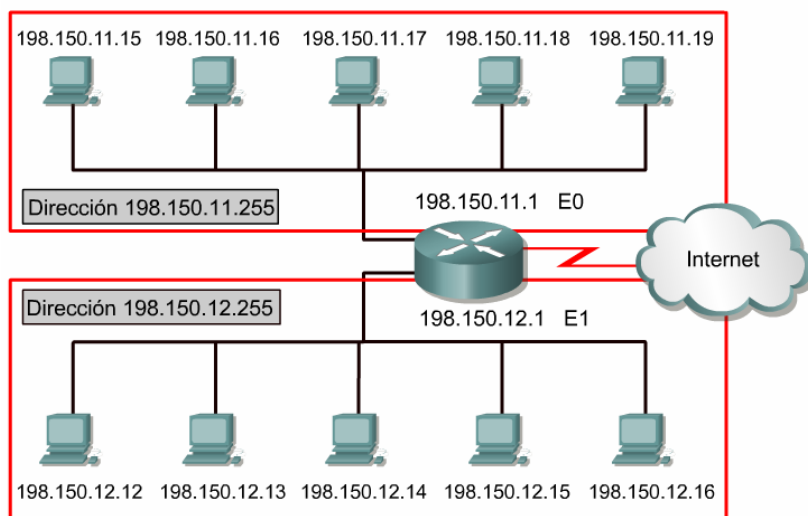


Figura 2

La dirección IP que tiene ceros binarios en todas las posiciones de bits de host queda reservada para la dirección de red. Tomando como ejemplo una red Clase A, 113.0.0.0 es la dirección IP de la red, conocida como el ID (identificador) de la red, que contiene el host 113.1.2.3. Un Router usa la dirección IP de red al enviar datos por Internet. En un ejemplo de red Clase B, la dirección 176.10.0.0 es una dirección de red, como muestra la Figura 3.

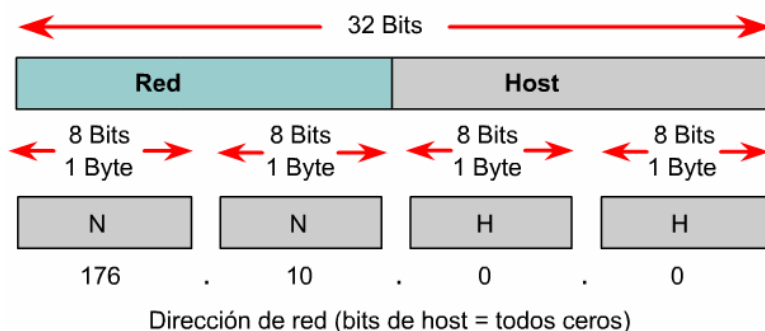


Figura 3

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 la red, se necesita una dirección de broadcast. **4** 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.

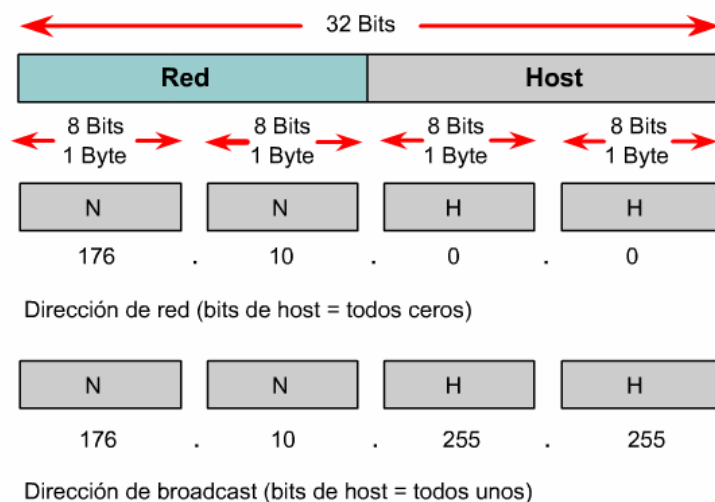


Figura 4

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 **1**, se muestran ciertos aspectos del esquema del direccionamiento de red. Al observar las redes, ambas tienen la dirección 198.150.11.0. El Router que aparece en esta ilustración no podrá enviar los paquetes de datos correctamente. Las direcciones IP de red repetidas hacen que el Router no pueda realizar su trabajo de seleccionar la mejor ruta. Es necesario que cada dispositivo de la red tenga una dirección exclusiva.

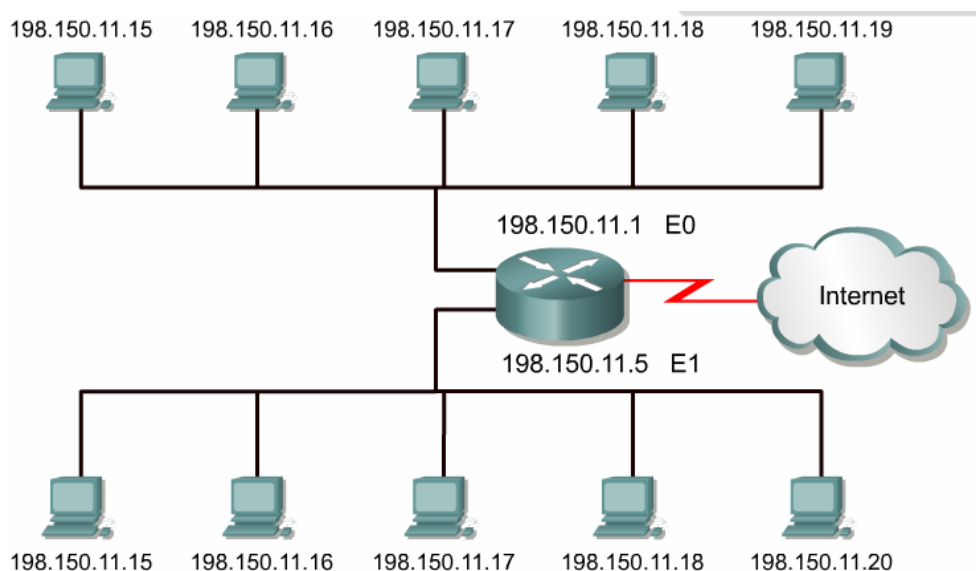


Figura 1

Hizo falta un procedimiento para asegurar que las direcciones fueran, de hecho, exclusivas. En un principio, una organización conocida como el Centro de información de la red Internet (InterNIC) manejaba este procedimiento. InterNIC ya no existe y la Agencia de asignación de números de Internet (IANA) la ha sucedido. IANA administra, cuidadosamente, la provisión restante de las direcciones IP para garantizar que

no se genere una repetición de direcciones utilizadas de forma pública. La repetición suele causar inestabilidad en la Internet y compromete su capacidad para entregar datagramas a las redes.

Las direcciones IP públicas son exclusivas. Dos máquinas que se conectan a una red pública nunca pueden tener la misma dirección IP porque las direcciones IP públicas son globales y están estandarizadas. Todas las máquinas que se conectan a la Internet acuerdan adaptarse al sistema. Hay que obtener las direcciones IP públicas de un proveedor de servicios de Internet (ISP) o un registro, a un costo.

Con el rápido crecimiento de Internet, las direcciones IP públicas comenzaron a escasear. Se desarrollaron nuevos esquemas de direccionamiento, tales como el enrutamiento entre dominios sin clase (CIDR) y el IPv6, para ayudar a resolver este problema. CIDR y IPv6 se tratan más adelante en este curso.

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. ²Estos 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. ³ 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.

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

Figura 2

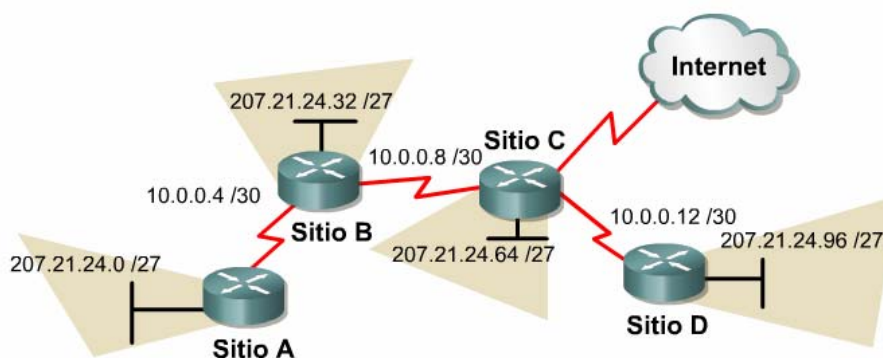


Figura 3

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.

9.2.7 Introducción a la división en subredes

La división en subredes es otro método para administrar las direcciones IP. ¹Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP. Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario

subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesario. **2** Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes. Un ejemplo sería el sistema telefónico de los EE.UU. que se divide en códigos de área, códigos de intercambio y números locales.

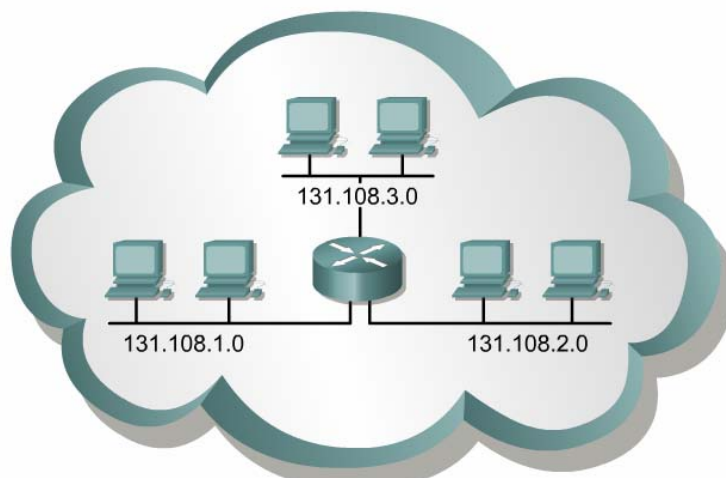


Figura 1

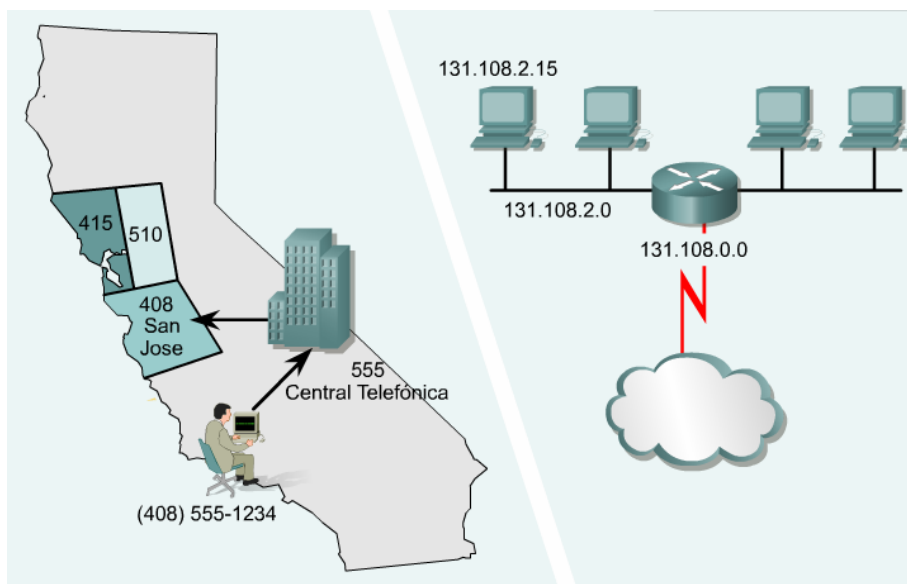


Figura 2

El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red.

Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. **3** El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

Figura 3

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 veinte 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.

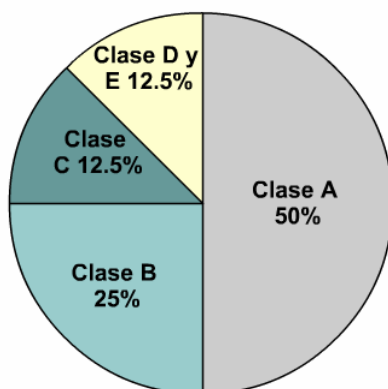


Figura 1

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). **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. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación. Esta versión de IP debe proporcionar suficientes direcciones para las necesidades de comunicación futuras.

Protocolo Internet Versión 4 IPv4	4 octetos
11010001.11011100.11001001.01110001	
209.156.201.113	
4,294,467,295 direcciones IP	

11010001.11011100.11001001.01110001.11010001.11011100.110011001.01110001.11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3.4 x 10 ³⁸ direcciones IP	

Figura 2

La figura **3** muestra las direcciones IPv4 e IPv6. Las direcciones de IPv4 miden 32 bits de longitud, se escriben con números decimales separados por puntos. Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interface pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separados por comas. Los campos IPv6 tienen una longitud de 16 bits. Para que las direcciones sean más fáciles de leer, es posible omitir los ceros iniciales de cada campo. El campo: 0003: se escribe :3:. La representación taquigráfica del IPv6 de los 128 bits utiliza números de 16 dígitos, que se muestran en forma de cuatro dígitos hexadecimales.

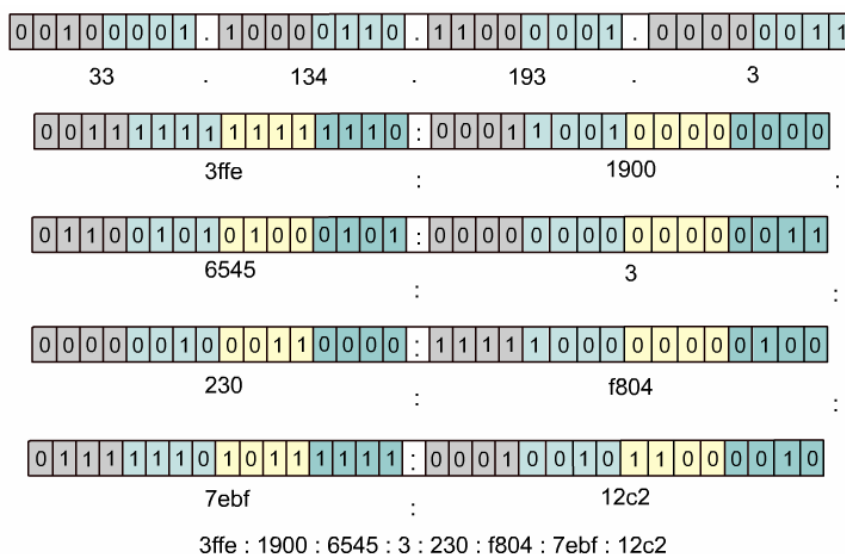


Figura 3

Después de diez años de planificación y desarrollo, el IPv6 lentamente comienza a implementarse en redes selectas. Con el tiempo, el IPv6 podrá reemplazar el IPv4 como el protocolo de Internet dominante.

9.3 Obtener una dirección IP

9.3.1 Cómo obtener una dirección IP

Un host de red necesita obtener una dirección exclusiva a nivel global para poder funcionar en Internet. La dirección MAC o física que posee el host sólo tiene alcance local, para identificar el host dentro de la red del

área local. Como es una dirección de Capa 2, el Router no la utiliza para realizar transmisiones fuera de la LAN.

Las direcciones IP son las direcciones que más frecuentemente se utilizan en las comunicaciones en la Internet. 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. ¹

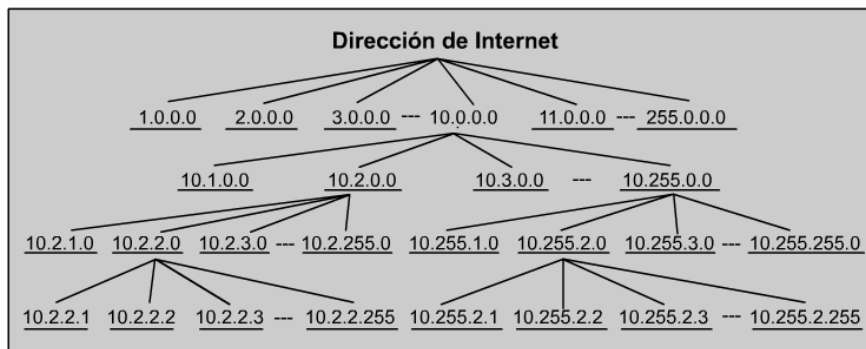


Figura 1

Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico. Más adelante, en esta lección, se tratará el direccionamiento estático y las tres variantes del direccionamiento 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 2, los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.

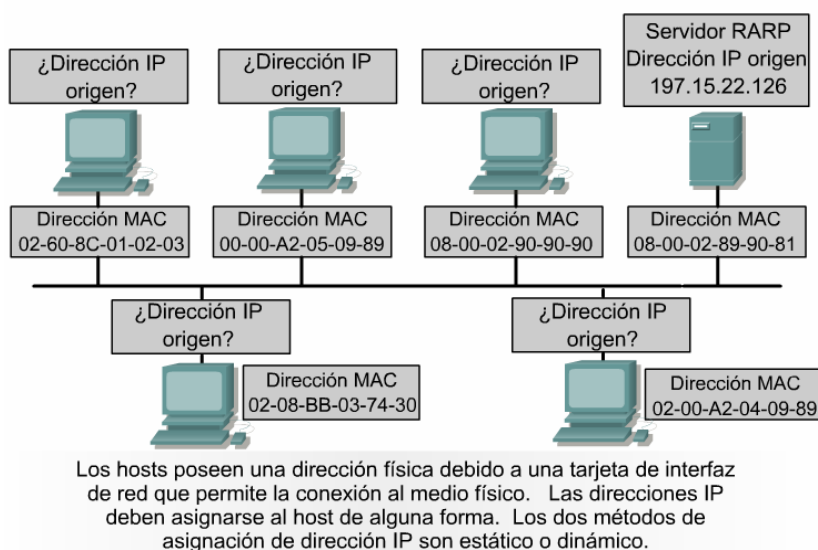


Figura 2

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 computador, 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.

9.3.3 Asignación de direcciones RARP IP

El Protocolo de resolución inversa de direcciones (RARP) asocia las direcciones MAC conocidas a direcciones IP. Esta asociación permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red. Es posible que un dispositivo de red, como por ejemplo una estación de trabajo sin disco, conozca su dirección MAC pero no su dirección IP. RARP permite que el dispositivo realice una petición para conocer su dirección IP. Los dispositivos que usan RARP requieren que haya un servidor RARP en la red para responder a las peticiones RARP.

Considere el caso en que un dispositivo origen desee enviar datos al dispositivo madre. En este ejemplo, el dispositivo fuente conoce su propia dirección MAC pero es incapaz de ubicar su propia dirección IP en la tabla ARP. El dispositivo origen debe incluir tanto su dirección MAC como su dirección IP para que el dispositivo destino retire los datos, los pase a las capas superiores del modelo OSI y responda al dispositivo transmisor. De esta manera, el origen inicia un proceso denominado petición RARP. Esta petición ayuda al dispositivo origen a detectar su propia dirección IP. Las peticiones RARP se envían en broadcast a la LAN y el servidor RARP que por lo general es un Router responde.

RARP utiliza el mismo formato de paquete que ARP. Sin embargo, en una petición RARP, los encabezados MAC y el "código de operación" son diferentes a los de una petición ARP. ¹ ² El formato de paquete RARP contiene lugares para las direcciones MAC tanto de los dispositivos de origen como de los de destino. El campo de dirección IP origen está vacío. El broadcast se dirige a todos los dispositivos de la red. Por lo tanto, la dirección MAC destino deberá ser: FF:FF:FF:FF:FF:FF. Las estaciones de trabajo que admiten RARP tienen códigos en ROM que los dirige a iniciar el proceso de RARP.

0 - 15 bits		16 - 31 bits
Tipo de hardware		Tipo de protocolo
HLen (1 byte)	PLen (1 byte)	Operación
HA emisor (bytes 1 a 4)		
HA emisor (byte 5 - 6)		PA emisor (byte 1 - 2)
PA emisor (byte 3 - 4)		HA objetivo (byte 1 - 2)
HA objetivo (bytes 3 - 6)		
PA objetivo (bytes 1 - 4)		
Estructura de encabezado RARP		

Figura 1

Campo	Descripción
Tipo de hardware	Especifica un tipo de interfaz de hardware para el cual el emisor requiere una respuesta.
Tipo de protocolo	Especifica el tipo de dirección de protocolo de alto nivel que el emisor ha suministrado.
HLen	Longitud de dirección de hardware
PLen	Longitud de dirección de protocolo.
Operation	Las descripciones son las siguientes: 1 Petición ARP. 2 Respuesta ARP. 3 Petición RARP. 4 Respuesta RARP. 5 Petición RARP dinámica. 6 Respuesta RARP dinámica. 7 Error RARP dinámico. 8 Petición InARP. 9 Respuesta InARP.
Dirección de hardware del emisor (HA)	HLen bytes de largo.
Dirección de protocolo del emisor (PA)	PLen bytes de largo.
Dirección de hardware del objetivo (HA)	HLen bytes de largo.
Dirección de protocolo del objetivo (PA)	PLen bytes de largo.

Figura 2

9.3.4 Asignación de direcciones BOOTP IP

El protocolo bootstrap (BOOTP) opera en un entorno cliente-servidor y sólo requiere el intercambio de un solo paquete para obtener la información IP. **1 2** Sin embargo, a diferencia del RARP, los paquetes de BOOTP pueden incluir la dirección IP, así como la dirección de un Router, la dirección de un servidor y la información específica del fabricante.

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 bytes)			
Seconds (2 bytes)		No se utiliza	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4 bytes)			
Chaddr (16 bytes)			
Servidor de nombres de Host (64 bytes)			
Nombre de Archivo de Boteo (128 bytes)			
Área específica del Fabricante (64 bytes)			
Estructura de mensaje BOOTP			

Figura 1

Campo	Descripción
Op	Código de operación de mensaje. Los mensajes pueden ser BOOTREQUEST o BOOTREPLY
Htype	Tipo de dirección de hardware
HLen	Longitud de dirección de hardware
Hops	El cliente coloca un cero, el servidor BOOTP utiliza este campo para enviar una petición a otra red
Xid	ID de transacción
Secs	Número de segundos transcurridos desde que el cliente empezó el proceso de adquisición o renovación de la dirección
Ciaddr	Dirección IP del cliente
Yiaddr	Dirección IP de "usted" (el cliente)
Siaddr	Dirección IP del siguiente servidor a utilizar en bootstrap
Giaddr	Dirección IP de agente de relay utilizada para arrancar a través de un agente de relay
Chaddr	Dirección de hardware del cliente
Server Host Name	Especifica un servidor en particular para obtener información BOOTP de
Boot File Name	Permite el uso de varios archivos de arranque permitiendo a los hosts ejecutar distintos sistemas operativos
Vendor Specific Area	Contiene información optativa específica del vendedor que se puede transmitir al host

Figura 2

Sin embargo, un problema del BOOTP es que no se diseñó para proporcionar la asignación dinámica de las direcciones. Con el BOOTP, un administrador de redes crea un archivo de configuración que especifica los parámetros de cada dispositivo. El administrador debe agregar hosts y mantener la base de datos del BOOTP. Aunque las direcciones se asignan de forma dinámica, todavía existe una relación exacta entre el número de direcciones IP y el número de hosts. Esto significa que para cada host de la red, debe haber un perfil BOOTP con una asignación de dirección IP en él. Dos perfiles nunca pueden tener la misma dirección IP. Es posible que estos perfiles se utilicen al mismo tiempo y esto quiere decir que dos hosts tendrían la misma dirección IP.

Un dispositivo utiliza el BOOTP para obtener una dirección IP cuando se inicializa. El BOOTP utiliza UDP para transportar los mensajes. El mensaje UDP se encapsula en un paquete IP. Un computador utiliza el BOOTP para enviar un paquete IP de broadcast a la dirección IP destino de todos unos, o sea, 255.255.255.255 en anotación decimal punteada. El servidor del BOOTP recibe el broadcast y responde en forma de broadcast. El cliente recibe una trama y verifica la dirección MAC. Si el cliente encuentra su propia dirección MAC en el campo de dirección destino y un broadcast en el campo IP destino, toma la dirección IP y la guarda junto con la otra información proporcionada por el mensaje BOOTP de respuesta.

9.3.5 Administración de direcciones DHCP IP

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 la red se puede obtener en un mensaje. ¹ ² Esto incluye todos los datos que proporciona el mensaje BOOTP más una dirección IP arrendada y una máscara de subred.

0 -7 bits		8 -15 bits		16 - 23 bits		24 - 31 bits	
Op (1)		Htype (1)		HLen (1)		Hops (1)	
Xid (4 bytes)							
Seconds (2 bytes)				Flags (2 bytes)			
Ciaddr (4 bytes)							
Yiaddr (4 bytes)							
Siaddr (4 bytes)							
Giaddr (4bytes)							
Chaddr (16 bytes)							
Servidor de nombres de Host (64 bytes)							
Nombre de Archivo de Boteo (128 bytes)							
Área específica del vendedor (64 bytes)							
Estructura del mensaje DHCP							

Figura 1

Op	Los mensajes de código de operación de mensajes pueden ser BOOTREQUEST o BOOTREPLY	↑ =
Htype	Tipo de dirección de hardware	
Hlen	Longitud de dirección de hardware	
Hops	El cliente coloca un cero, el servidor BOOTP utiliza este campo para enviar una petición a otra red	
Xid	ID de transacción	
Secs	Número de segundos transcurridos desde que el cliente empezó el proceso de adquisición o renovación de la dirección	
Señaladores	Señaladores	
Ciaddr	Dirección IP del cliente	
Yiaddr	Dirección IP de "usted" (el cliente)	
Siaddr	Dirección IP del siguiente servidor a utilizar en bootstrap	
Giaddr	Dirección IP de agente de relay utilizada para arrancar a través	
Chaddr	Dirección de hardware del cliente	
Server Host Name	Especifica un servidor en particular para obtener información	
Boot File Name	Permite el uso de varios archivos de arranque permitiendo a los hosts ejecutar distintos sistemas operativos	
Vendor Specific Area	Contiene información optativa específica del vendedor que se puede transmitir al host	= ↓

Figura 2

La principal ventaja que el DHCP tiene sobre el BOOTP es que permite que los usuarios sean móviles. Esta movilidad 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 significa 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. ¹

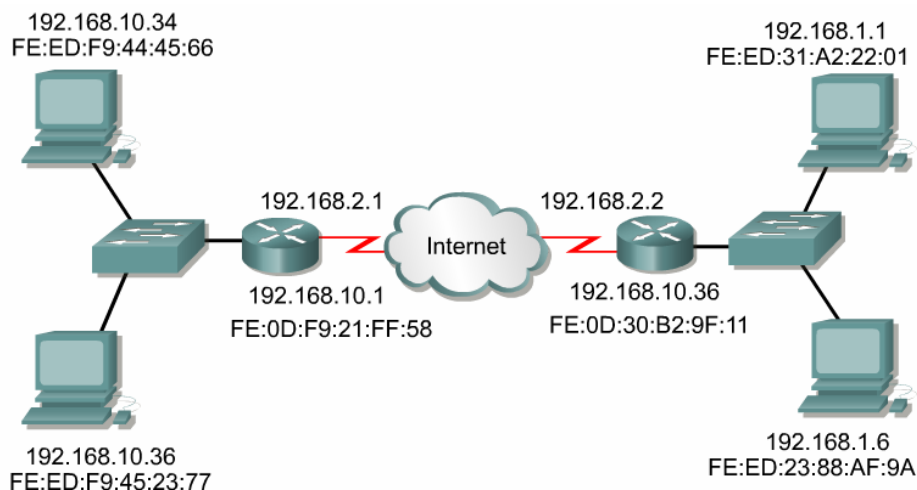


Figura 1

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.

9.3.7 Protocolo de resolución de direcciones (ARP)

Entrada de la tabla ARP.		
Dirección de Internet	Dirección física	Tipo
68.2.168.1	00-50-57-00-76-84	dinámica

Tabla Arp 198.150.11.36	
MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Figura 1

En la red TCP/IP, el paquete de datos debe contener tanto la dirección MAC destino como la dirección IP destino. Si el paquete pierde alguna de las dos, los datos no pasarán de la Capa 3 a las capas superiores. De esta forma, las direcciones MAC e IP actúan como controles y balances entre sí. Una vez que los dispositivos determinan las direcciones IP de los dispositivos destino, pueden agregar las direcciones MAC de destino a los paquetes de datos.

Algunos dispositivos guardan tablas que contienen las direcciones MAC e IP de otros dispositivos conectados a la misma LAN. ¹Estas reciben el nombre de tablas del Protocolo de resolución de direcciones (ARP). Las tablas ARP se guardan en la memoria RAM, donde la información en caché se guarda automáticamente en cada uno de los dispositivos. Resulta muy inusual que un usuario tenga que entrar en la tabla ARP de forma manual. Cada dispositivo de una red lleva su propia tabla ARP. Cuando un dispositivo desea enviar datos a través de la red, utiliza la información que proporciona la tabla ARP.

Cuando un origen determina la dirección IP para un destino, luego consulta la tabla ARP a fin de encontrar la dirección MAC destino. Si el origen encuentra una entrada en su tabla (dirección IP destino a dirección MAC destino), se asigna la dirección IP a la dirección MAC y luego la usa para encapsular los datos. Luego el paquete de datos se envía a través del medio de networking para que el destino lo reciba.

Son dos las formas en las que los dispositivos pueden recolectar las direcciones MAC que necesitan agregar a los datos encapsulados. Una es monitorear el tráfico que se produce en el segmento de la red local. Todas las estaciones de una red Ethernet analizarán todo el tráfico a fin de determinar si los datos son para ellas. Parte de este proceso consiste en registrar la dirección IP y MAC origen del datagrama en una tabla ARP. A medida que los datos se transmiten a la red, los pares de direcciones pueblan la tabla ARP. Otra forma de obtener un par de direcciones para la transmisión de datos es realizar el broadcast de una petición ARP. ²

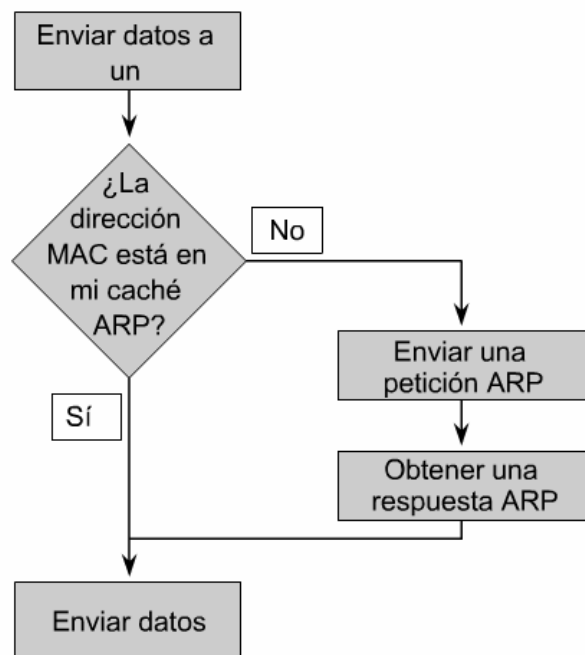


Figura 2

El computador que requiere un par de direcciones IP y MAC envía una petición ARP en broadcast. Todos los demás dispositivos de la red de área local analizan la petición. Si la dirección de uno de los dispositivos locales concuerda con la dirección IP de la petición, envía una respuesta ARP que contiene el par IP-MAC. Si la dirección IP es para la red de área local y el computador no existe o se encuentra apagado, no hay respuesta a la petición ARP. En este caso, el dispositivo origen informa un error. Si la petición es para una red IP diferente, hay otro proceso que se puede utilizar.

Los Routers no envían los paquetes de broadcast. Si la característica está activa, un Router ejecuta un ARP proxy. Un ARP proxy es una variante del protocolo ARP. En esta variante, un Router envía una respuesta ARP con la dirección MAC de la interfaz en la que se recibió la petición al host que la ejecuta. 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.

Resumen

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

- Por qué se desarrolló la Internet y cómo el TCP/IP se ajusta al diseño de la misma.
- Las cuatro capas del modelo TCP/IP.
- Las funciones de cada capa del modelo TCP/IP.
- El modelo OSI en comparación con el modelo TCP/IP.
- El direccionamiento IP le otorga a cada dispositivo conectado a la Internet un identificador exclusivo.
- Las clases de direcciones IP son divisiones lógicas del espacio de direccionamiento que se utiliza para satisfacer las necesidades de los distintos tamaños de redes.
- La división en subredes se utiliza para dividir una red en redes de menor tamaño.
- Las direcciones reservadas cumplen un papel especial en el direccionamiento IP y no se pueden utilizar para ningún otro propósito.
- No se puede enrutar las direcciones privadas a la Internet pública.
- La función de una máscara de subred es mapear las partes de una dirección IP que son de la red y del host.
- Algún día, el IPV4 será totalmente obsoleto y el IPV6 será la versión que se utiliza comúnmente.
- Un computador debe tener una dirección IP para comunicarse por Internet
- Es posible configurar una dirección IP de forma estática o dinámica.
- Una dirección IP dinámica se puede asignar utilizando RARP, BOOTP o DHCP
- El DHCP brinda mayor información al cliente que el BOOTP
- El DHCP hace posible que los computadores sean móviles permitiendo la conexión a muchas redes diferentes.
- El ARP y el ARP proxy pueden utilizarse para resolver problemas de resolución de direcciones.

Módulo 10: Principios básicos de enrutamiento y subredes

Descripción general

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. Este módulo brinda un panorama general de cada uno.

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.

Los estudiantes que completen este módulo deberán poder:

- Describir los protocolos enrutados (enrutables)
- Enumerar los pasos del encapsulamiento de datos en una internetwork a medida que los datos se enrutan a uno o más dispositivos de Capa 3.
- Describir la entrega no orientada a conexión y orientada a conexión.
- Nombrar los campos de los paquetes IP.
- Describir el proceso de enrutamiento.
- Comparar y contrastar los diferentes tipos de protocolos de enrutamiento.
- Enumerar y describir las distintas métricas utilizadas por los protocolos de enrutamiento.
- Enumerar varios usos de la división en subredes.
- Determinar las máscaras de subred para una situación determinada.
- Utilizar máscaras de subred para determinar el ID de subred.

10.1 Protocolo enrutado

10.1.1 Protocolos enrutables y enrutados

Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para aceptar y actuar sobre estos mensajes, los computadores deben contar con definiciones de cómo interpretar el mensaje. Los ejemplos de mensajes incluyen aquellos que establecen una conexión a una máquina remota, mensajes de correo electrónico y archivos que se transmiten en la red.

Un protocolo describe lo siguiente:

- El formato al cual el mensaje se debe conformar
- La manera en que los computadores intercambian un mensaje dentro del contexto de una actividad en particular

Un protocolo enrutado permite que un Router envíe datos entre nodos de diferentes redes. ¹ Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host. Algunos protocolos como los IPX, requieren sólo de un número de red porque estos protocolos utilizan la dirección MAC del Host como número de Host. Otros protocolos, como el IP, requieren una dirección completa que especifique la porción de red y la porción de Host. Estos protocolos también necesitan una máscara de red para diferenciar estos dos números. La dirección de red se obtiene al realizar la operación "AND" con la dirección y la máscara de red.

La razón por la que se utiliza una máscara de red es para permitir que grupos de direcciones IP secuenciales sean considerados como una sola unidad. ² Si no se pudiera agrupar, cada Host tendría que

mapearse de forma individual para realizar el enrutamiento. Esto sería imposible, ya que de acuerdo al Consorcio de Software de Internet (ISC) existen aproximadamente 233.101.500 hosts en Internet.

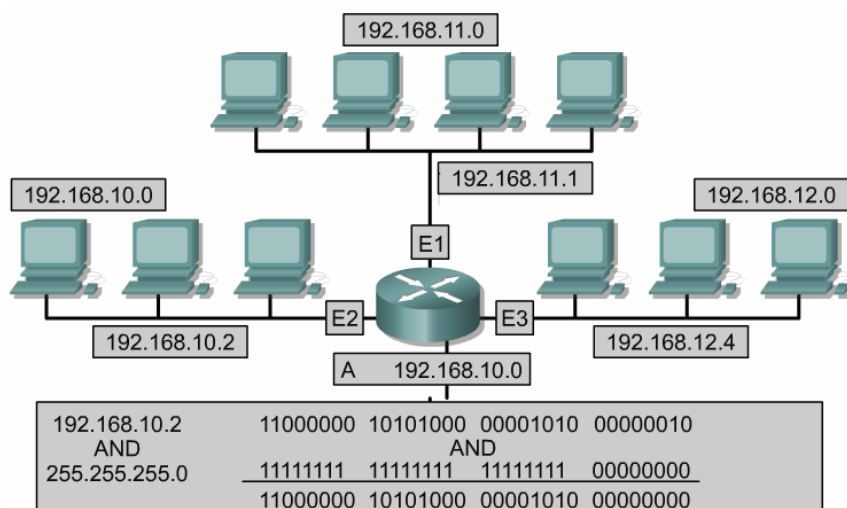


Figura1

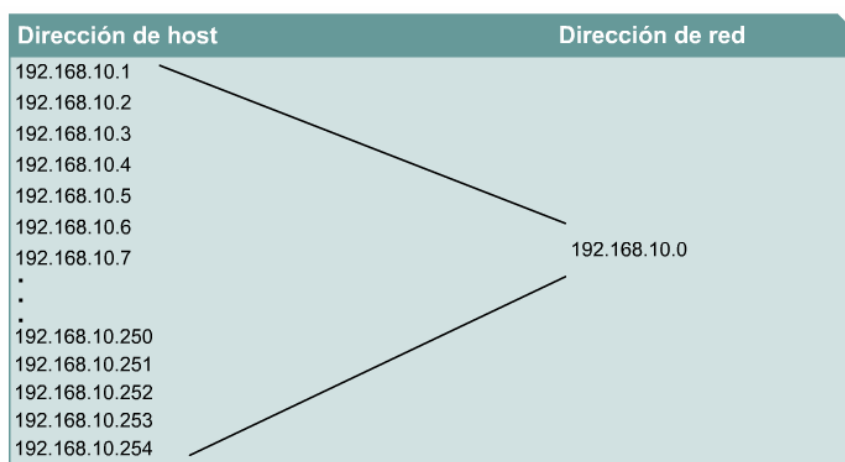


Figura 2

10.1.2 IP como protocolo enrutado

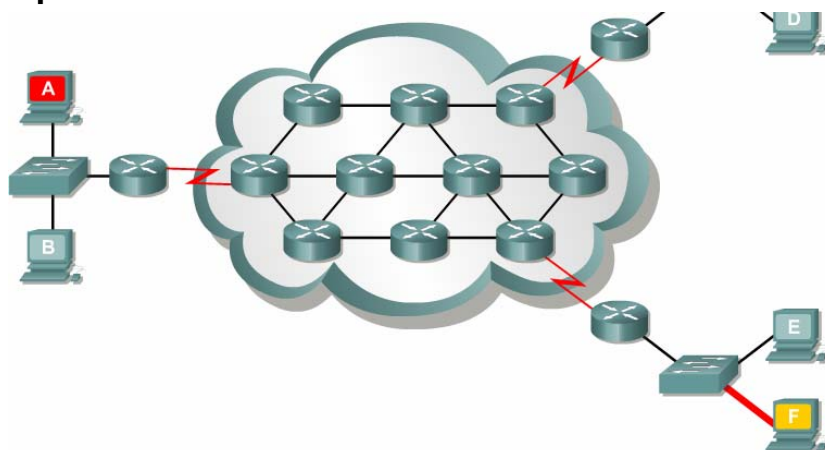


Figura 1

El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es un protocolo de entrega no orientado a la conexión, poco confiable y de máximo esfuerzo. El término no orientado a la conexión significa que no se establece ningún circuito de conexión dedicado antes de la transmisión, como sí lo hay cuando se establece una comunicación telefónica. IP determina la ruta más eficiente para los datos basándose en el protocolo de enrutamiento. Los términos

poco confiables y de máximo esfuerzo no implican que el sistema no sea confiable y que no funcione bien; más bien significan que IP no verifica que los datos lleguen a su destino. La verificación de la entrega no siempre se lleva a cabo.

A medida que la información fluye hacia abajo por las capas del modelo OSI, los datos se procesan en cada capa. ² 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.

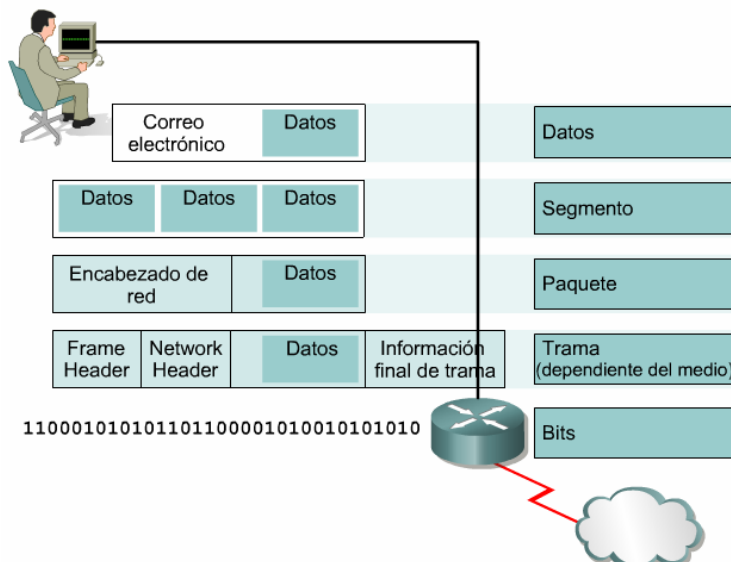
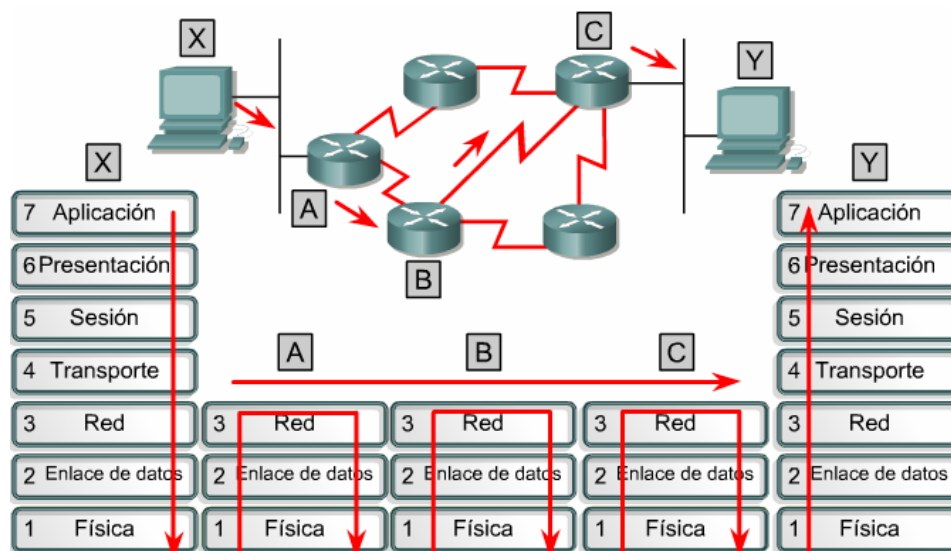


Figura 2

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 reemplazan en cada dispositivo de Capa 3. 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.



Cada router ofrece sus servicios para admitir las funciones de las capas superiores.

Figura 1

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 el 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. Se extrae la información de verificación por redundancia cíclica (CRC) de la información final de la trama aceptada, y la CRC se calcula para verificar que los datos de la trama no tengan errores. La trama se descarta si está dañada. Si la verificación es válida, el encabezado de la trama y la información final se descartan y el paquete pasa hacia arriba a la Capa 3. Allí se verifica el paquete para asegurar que esté realmente destinado al Router, o si tiene que ser enrutado a otro dispositivo en la internetwork. Si la dirección IP destino concuerda con uno de los puertos del Router, se elimina el encabezado de Capa 3 y los datos pasan a la Capa 4. Si es necesario enrutar el paquete, se comparará la dirección IP destino con la tabla de enrutamiento. Si se encuentra una concordancia o si hay una ruta por defecto, el paquete se enviará a la interfaz especificada en la sentencia de concordancia de la tabla de enrutamiento. Cuando el paquete se conmuta a la interfaz de salida, se agrega un nuevo valor de verificación CRC como información final de la trama, y se agrega el encabezado de trama apropiado al paquete. Entonces la trama se transmite al siguiente dominio de broadcast en su viaje hacia el destino final.

10.1.4 Protocolo Internet (IP)

Existen dos tipos de servicios de envío: los no orientados a conexión y los orientados a conexión. Estos dos servicios son los que realmente permiten el envío de datos de extremo a extremo en una internetwork.

La mayoría de los servicios utilizan sistemas de entrega no orientados a conexión. ¹ Es posible que los diferentes paquetes tomen distintas rutas para transitar por la red, pero se reensamblan al llegar a su destino. En un sistema no orientado a conexión, no se comunica con el destino antes de enviar un paquete. Una buena comparación para un sistema no orientado a conexión es el sistema postal. No se comunica con el destinatario para ver si aceptará la carta antes de enviarla. Además, el remitente nunca sabe si la carta llegó a su destino.

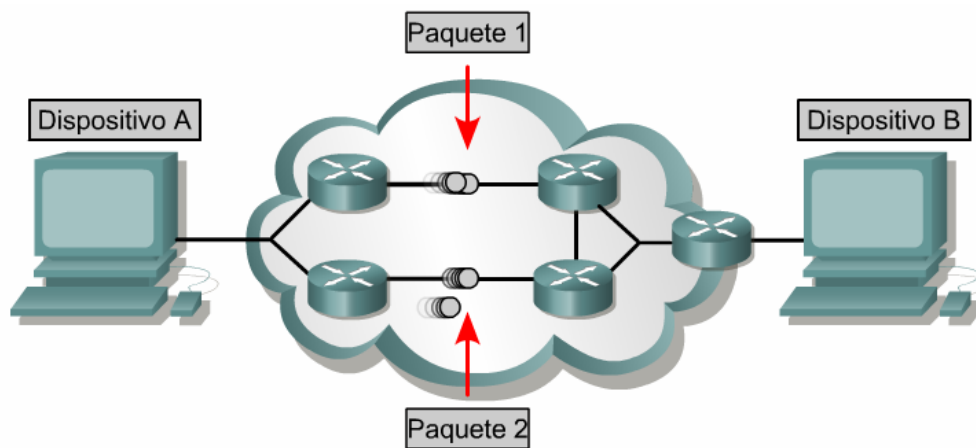


Figura 1

En los sistemas orientados a conexión, se establece una conexión entre el remitente y el destinatario antes de que se transfieran los datos. Un ejemplo de redes orientadas a conexión es el sistema telefónico. Se realiza una llamada, se establece una conexión y luego se produce la comunicación.

Los procesos de red no orientados a conexión también se conocen como procesos de conmutación de paquetes. A medida que los paquetes se transportan desde el origen al destino, pueden tomar rutas diferentes, y es posible que no lleguen en el mismo orden. Los dispositivos determinan la ruta de cada paquete a base de varios criterios. Algunos de los criterios como, por ejemplo, el ancho de banda disponible, pueden variar de un paquete a otro.

Los procesos de red orientados a conexión también se conocen como procesos de conmutación de circuitos. Primero se establece una conexión con el destinatario, y de allí comienza la transferencia de datos. Todos los paquetes viajan en secuencia a través del mismo circuito físico o virtual.

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.

0	4	8	16	19	24	31
VERS	HLEN	Tipo de servicio	Longitud total			
Identificación			Señaladores	Desplazamiento del fragmento		
Tiempo de existencia		Protocolo	Checksum de encabezado			
Dirección IP origen						
Dirección IP destino						
Opciones IP (si existen)					Relleno	
Datos						
...						

Aunque las direcciones de origen y destino IP son importantes, los otros campos del encabezado han hecho que IP sea muy flexible. Los campos del encabezado contienen las direcciones origen y destino del paquete y generalmente incluyen la longitud del mensaje. La información para enrutar el mensaje también está incluida en el encabezado de IP, el cual puede ser largo y complejo.

10.2 Protocolos de enrutamiento IP

10.2.1 Descripción del enrutamiento

La función de enrutamiento es una función de la Capa 3 del modelo OSI. ¹El enrutamiento es un esquema de organización jerárquico que permite que se agrupen direcciones individuales. Estas direcciones individuales son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos. El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro. El dispositivo primario que realiza el proceso de enrutamiento es el Router.

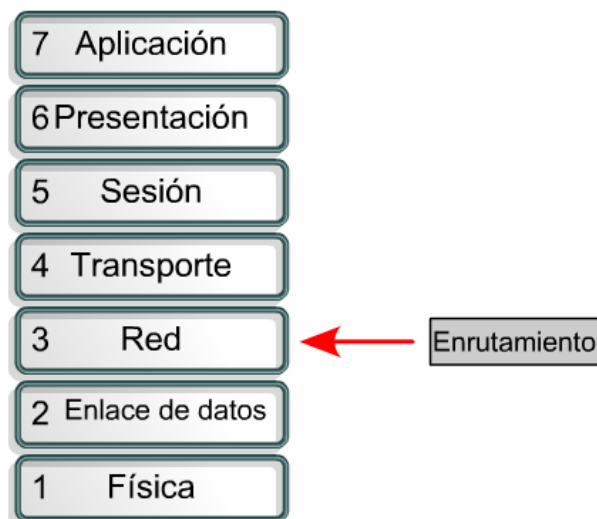


Figura 1

Las siguientes son las dos funciones principales de un Router:

- Los Routers deben mantener tablas de enrutamiento y asegurarse de que otros Routers conozcan las modificaciones a la topología de la red. Esta función se lleva a cabo utilizando un protocolo de enrutamiento para comunicar la información de la red a otros Routers.
- Cuando los paquetes llegan a una interfaz, el Router debe utilizar la tabla de enrutamiento para establecer el destino. El Router envía los paquetes a la interfaz apropiada, agrega la información de enrutamiento necesaria para esa interfaz, y luego transmite la trama.

Un Router es un dispositivo de la capa de red que usa una o más métricas de enrutamiento para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Las métricas de enrutamiento son valores que se utilizan para determinar las ventajas de una ruta sobre otra. Los protocolos de enrutamiento utilizan varias combinaciones de métricas para determinar la mejor ruta para los datos.

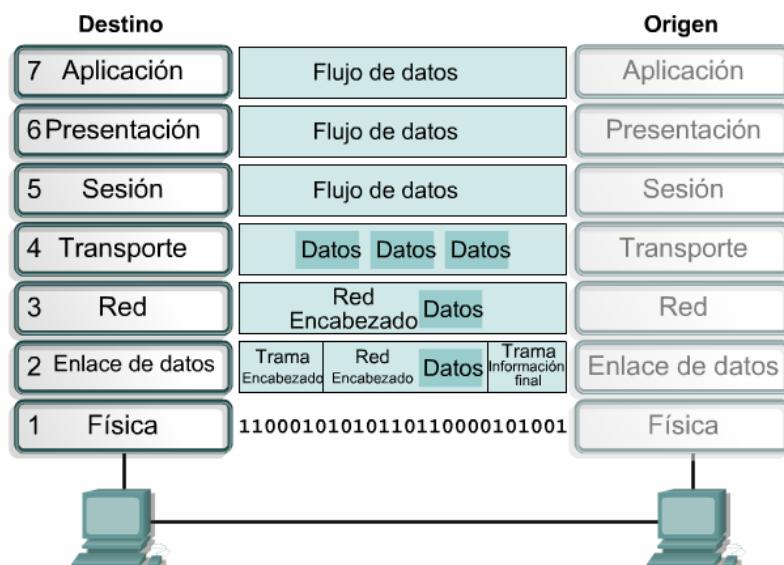


Figura 2

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 encapsulado 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 2, 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.

Este curso se concentra en el protocolo enrutable más común, el protocolo de Internet (IP). 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.

10.2.2 El enrutamiento en comparación con la conmutación

A menudo, se compara el enrutamiento con la conmutación. 1 Un observador inexperto puede pensar que el enrutamiento y la conmutación cumplen la misma función. La diferencia básica es que la conmutación tiene lugar en la Capa 2, o sea, la capa de enlace de los datos, en el modelo OSI y el enrutamiento en la Capa 3. Esta diferencia significa que el enrutamiento y la conmutación usan información diferente en el proceso de desplazar los datos desde el origen al destino.

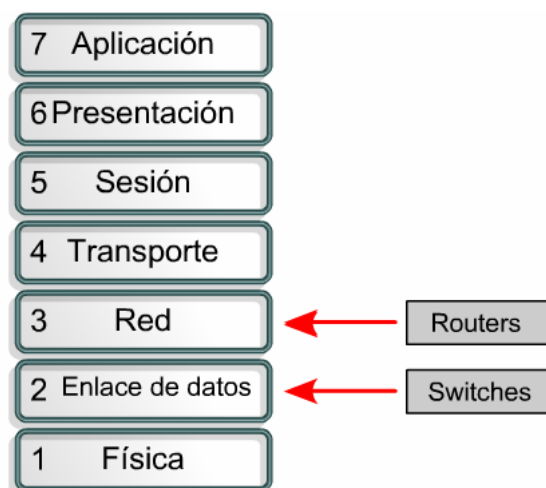
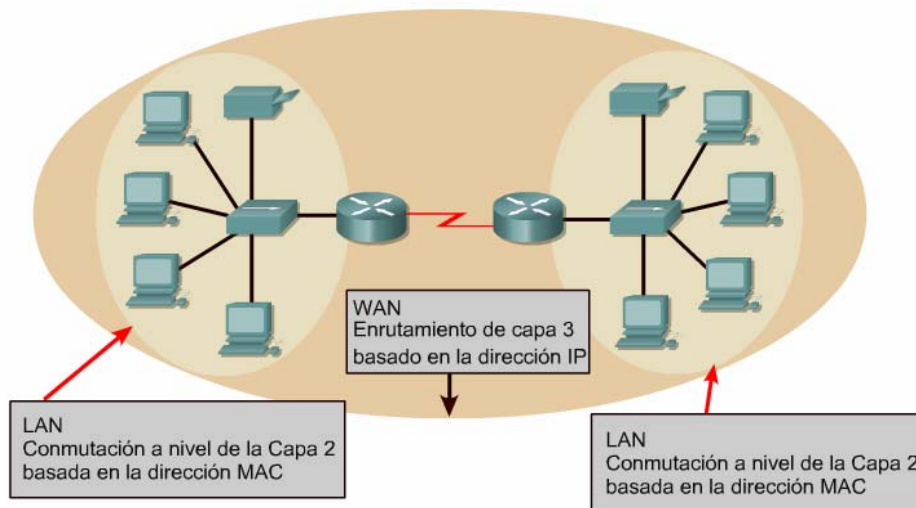


Figura 1

La relación entre la conmutación y el enrutamiento es comparable con la relación entre las comunicaciones telefónicas locales y de larga distancia. Cuando se realiza una comunicación telefónica a un número dentro de un mismo código de área, un Switch local administra la llamada. Sin embargo, el Switch local sólo puede llevar registro de sus propios números locales. El Switch local no puede administrar todos los números telefónicos del mundo. Cuando el Switch recibe un pedido de llamada fuera de su código de área, transfiere la llamada a un Switch de nivel superior que reconoce los códigos de área. El Switch de nivel superior entonces transfiere la llamada de modo que finalmente llegue al Switch local del código de área marcado. 2 El Router tiene una función parecida a la del Switch de nivel superior en el ejemplo del teléfono. La figura 3 muestra las tablas ARP de las direcciones MAC de Capa 2 y las tablas de enrutamiento de las direcciones IP de Capa 3. Cada interfaz de computador y de Router mantiene una tabla ARP para comunicaciones de Capa 2. La tabla ARP funciona sólo para el dominio de broadcast al cual está conectada. El Router también mantiene una tabla de enrutamiento que le permite enrutar los datos fuera del dominio de broadcast. Cada componente de la tabla ARP contiene un par de direcciones IP-MAC (en el gráfico las direcciones MAC están representadas por la sigla MAC, debido a que las direcciones verdaderas son demasiado largas y no caben en el gráfico). Las tablas de enrutamiento también registran cómo se informó la ruta (en este caso ya sea directamente conectada [C] o informada por RIP [R]), la dirección IP de red de las redes alcanzables, el número de saltos o distancia hasta dichas redes, y la interfaz por la que los datos deben enviarse para llegar a la red de destino.



La conmutación de capa 2 se realiza dentro de la LAN. El enrutamiento de capa 3 desplaza el tráfico entre los dominios de broadcast. Esto requiere el formato de direccionamiento jerárquico que proporciona un esquema de direccionamiento de capa 3 como IP.

Figura 2

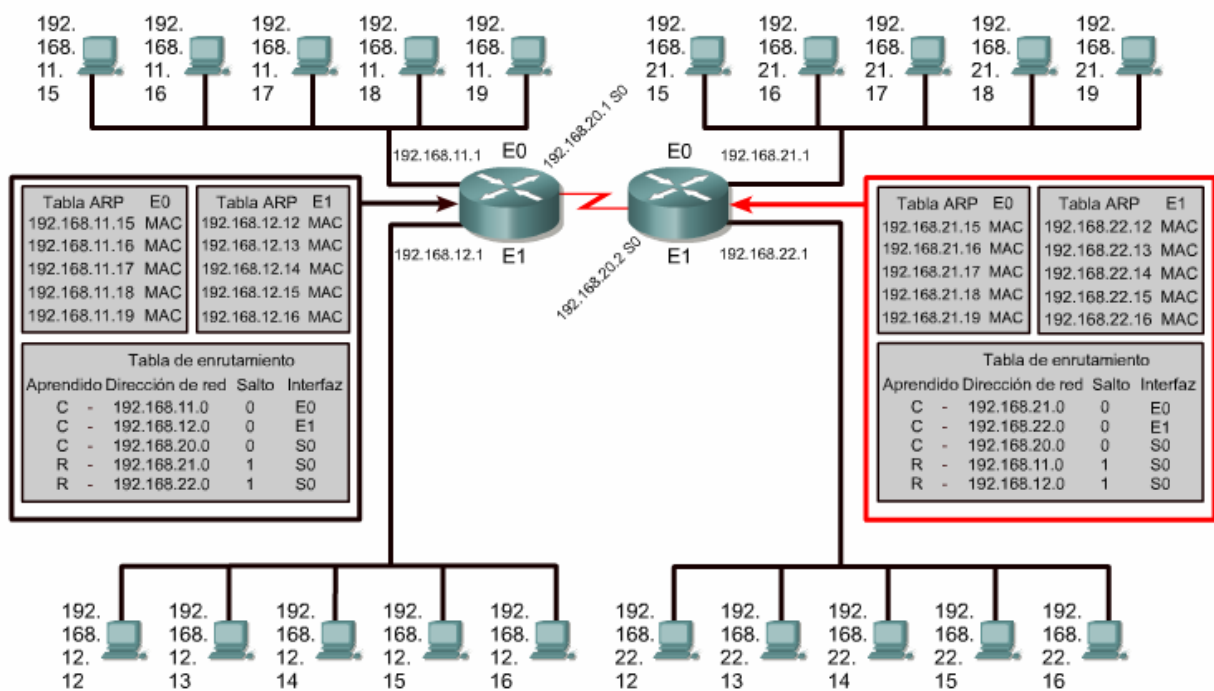


Figura 3

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. ² 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. Si las direcciones IP no estuvieran organizadas, Internet simplemente no funcionaría. Sería como tener una biblioteca que contiene una pila enorme con millones de páginas sueltas de material impreso. Este material resultaría inútil porque sería imposible ubicar un documento en particular. Si las páginas están organizadas en libros y cada página está individualizada, y además los libros están registrados en un índice, es mucho más sencillo ubicar y utilizar la información.

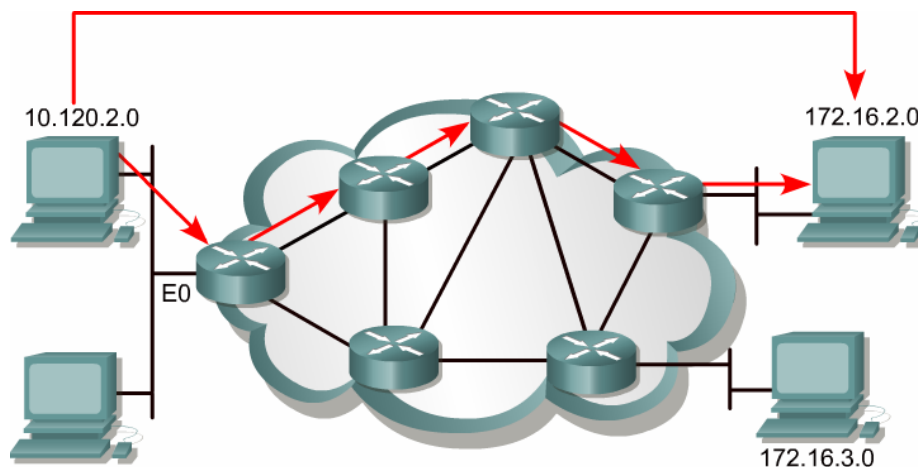
Otra diferencia entre las redes conmutadas y enrutadas es que las redes conmutadas no bloquean los broadcasts. Como resultado, los Switches pueden resultar abrumados por las tormentas de broadcast. Los Routers bloquean los broadcasts de LAN, de modo que una tormenta de broadcast sólo afecta el dominio de broadcast de origen. Debido a que los Routers bloquean broadcasts, pueden brindar un mayor nivel de seguridad y control de ancho de banda que los Switches.

Características	Router	Switch
Velocidad	Más lento	Más rápido
Capas del modelo OSI	Capa 3	Capa 2
Direccionamiento utilizado	IP	MAC
Broadcasts	Bloques	Enviado
Seguridad	Más alto	Más bajo

Figura 4

10.2.3 Enrutado comparado con enrutamiento

Los protocolos usados en la capa de red que transfieren datos de un Host a otro a través de un Router se denominan protocolos enrutados o enrutables. Los protocolos enrutados transportan datos a través de la red. Los protocolos de enrutamiento permiten que los Routers elijan la mejor ruta posible para los datos desde el origen hasta el destino.



El protocolo de enrutamiento transporta los datos de una estación final a otra.

Figura 1

Las funciones de un protocolo enrutado incluyen lo siguiente: **1**

- Incluir cualquier conjunto de protocolos de red que ofrece información suficiente en su dirección de capa para permitir que un Router lo envíe al dispositivo siguiente y finalmente a su destino.
- Definir el formato y uso de los campos dentro de un paquete.

El Protocolo Internet (IP) y el intercambio de paquetes de internetworking (IPX) de Novell son ejemplos de protocolos enrutados. Otros ejemplos son DECnet, AppleTalk, Banyan VINES y Xerox Network Systems (XNS).

Los Routers utilizan los protocolos de enrutamiento para intercambiar las tablas de enrutamiento y compartir la información de enrutamiento. En otras palabras, los protocolos de enrutamiento permiten enrutar protocolos enrutados.

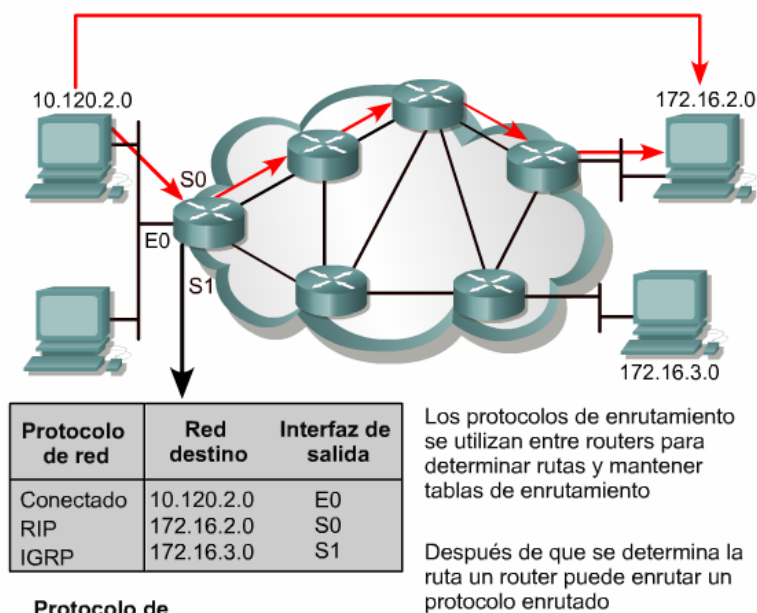


Figura 2

Las funciones de un protocolo de enrutamiento incluyen lo siguiente: 2

- Ofrecer procesos para compartir la información de ruta.
- Permitir que los Routers se comuniquen con otros Routers para actualizar y mantener las tablas de enrutamiento.

Los ejemplos de protocolos de enrutamiento que admiten el protocolo enrutado IP incluyen el Protocolo de información de enrutamiento (RIP) y el Protocolo de enrutamiento de Gateway interior (IGRP), el Protocolo primero de la ruta libre más corta (OSPF), el Protocolo de Gateway fronterizo (BGP), el IGRP mejorado (EIGRP).

10.2.4 Determinación de la ruta

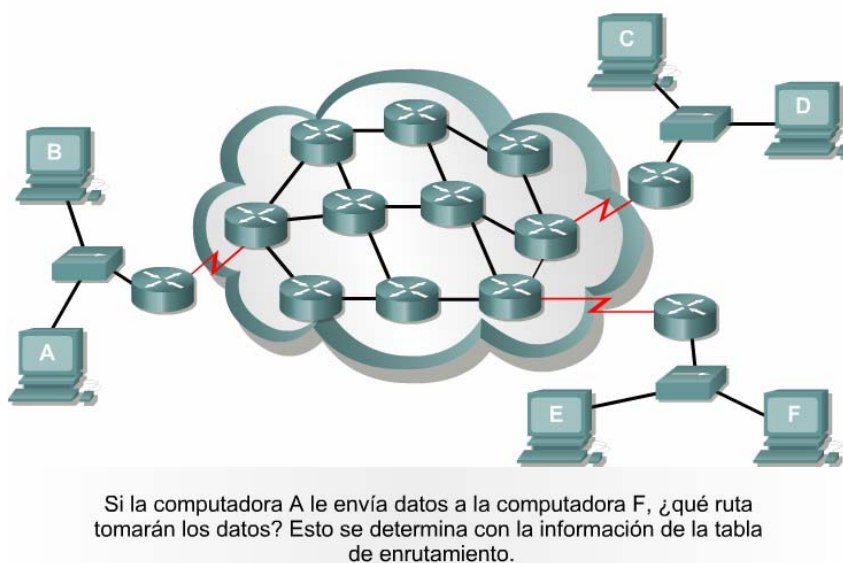


Figura 1

La determinación de la ruta ocurre a nivel de la capa de red. 1 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 determina 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.



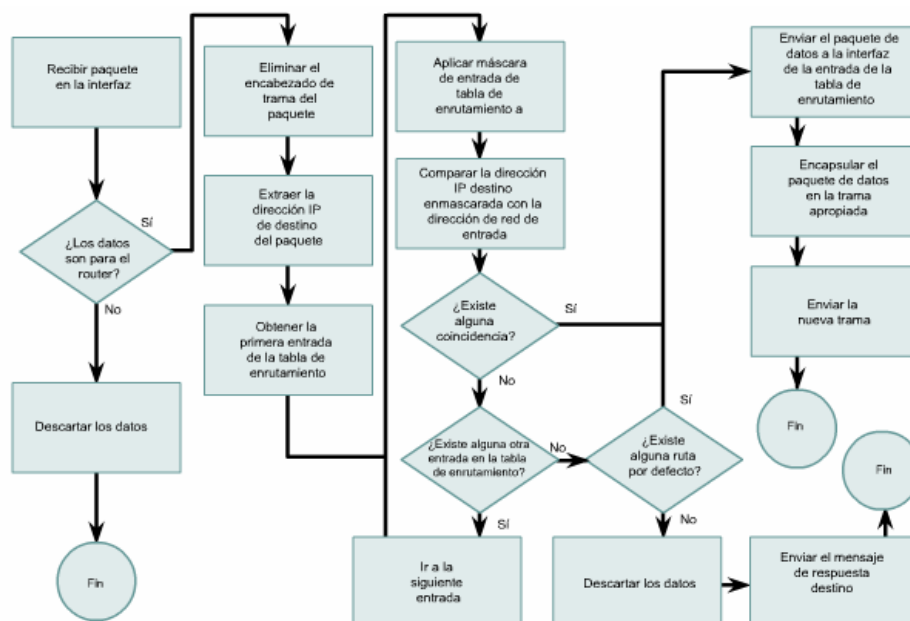
¿Cuál es la mejor ruta de la casa a la universidad? Existen varias opciones posibles pero, ¿cuál es la más rápida, la más segura, la más corta y la más confiable? Las mismas preguntas se formulan y se contestan cuando se realiza el enrutamiento de datos.

Figura 2

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: 3

- 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.



Aunque se han omitido algunos pasos para un mayor esclarecimiento, este es el proceso fundamental que utiliza un router para enrutar datos.

Figura 3

10.2.5 Tablas de enrutamiento

Los Routers utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas. Los dispositivos de Capa 3 interconectan dominios de broadcast o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos. ¹

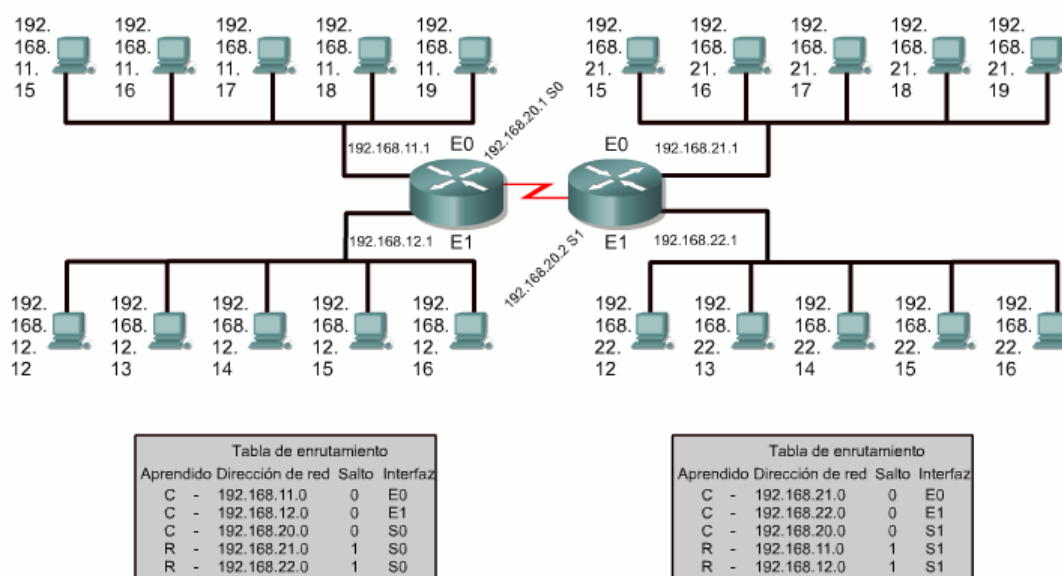


Figura 1

Los Routers mantienen información importante en sus tablas de enrutamiento, que incluye lo siguiente:

- **Tipo de protocolo:** el tipo de protocolo de enrutamiento que creó la entrada en la tabla de enrutamiento.

- **Asociaciones entre destino/siguiente salto:** estas asociaciones le dicen al Router que un destino en particular está directamente conectado al Router, o que puede ser alcanzado utilizando un Router denominado "salto siguiente" en el trayecto hacia el destino final. Cuando un Router recibe un paquete entrante, lee la dirección destino y verifica si hay concordancia entre esta dirección y una entrada de la tabla de enrutamiento.
- **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 número 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 algoritmos de enrutamiento utilizan métricas distintas para determinar la mejor ruta. ¹ Cada algoritmo de enrutamiento interpreta a su manera lo que es mejor. El algoritmo genera un número, denominado valor métrico, para cada ruta a través de la red. Los algoritmos de enrutamiento sofisticados basan la elección de la ruta en varias métricas, combinándolas en un sólo valor métrico compuesto. En general, los valores métricos menores indican la ruta preferida.

Protocolo	Métrica	Número máximo de routers	Orígenes
RIP	Número de saltos	15	Xerox
IGRP	• Ancho de banda • Carga • Retardo • Confiabilidad	255	Cisco

Figura 1

Las métricas pueden tomar como base una sola característica de la ruta, o pueden calcularse tomando en cuenta distintas características. Las siguientes son las métricas más utilizadas en los protocolos de enrutamiento:

- **Ancho de banda:** la capacidad de datos de un enlace. En general, se prefiere un enlace Ethernet de 10 Mbps a una línea arrendada de 64 kbps.
- **Retardo:** la cantidad de tiempo requerido para transportar un paquete a lo largo de cada enlace desde el origen hacia el destino. El retardo depende del ancho de banda de los enlaces intermedios, de la cantidad de datos que pueden almacenarse de forma temporaria en cada Router, de la congestión de la red, y de la distancia física.
- **Carga:** la cantidad de actividad en un recurso de red como, por ejemplo, un Router o un enlace.
- **Confiabilidad:** generalmente se refiere al índice de error de cada enlace de red.
- **Número de saltos:** el número de Routers que un paquete debe atravesar antes de llegar a su destino. La distancia que deben atravesar los datos entre un Router y otro equivale a un salto. Una ruta cuyo número de saltos es cuatro indica que los datos que se transportan a través de esa ruta deben pasar por cuatro Routers antes de llegar a su destino final en la red. Si existen varias rutas hacia un mismo destino, se elige la ruta con el menor número de saltos.
- **Tictacs:** el retardo en el enlace de datos medido en tictacs de reloj PC de IBM. Un tictac dura aproximadamente 1/18 de segundo.
- **Costo:** un valor arbitrario asignado por un administrador de red que se basa por lo general en el ancho de banda, el gasto monetario u otra medida.

10.2.7 IGP y EGP

Un sistema autónomo es una red o conjunto de redes bajo un control común de administración, tal como el dominio cisco.com. Un sistema autónomo está compuesto por Routers que presentan una visión coherente del enrutamiento al mundo exterior.

Los Protocolos de enrutamiento de Gateway interior (IGP) y los Protocolos de enrutamiento de Gateway exterior (EGP) son dos tipos de protocolos de enrutamiento. ¹

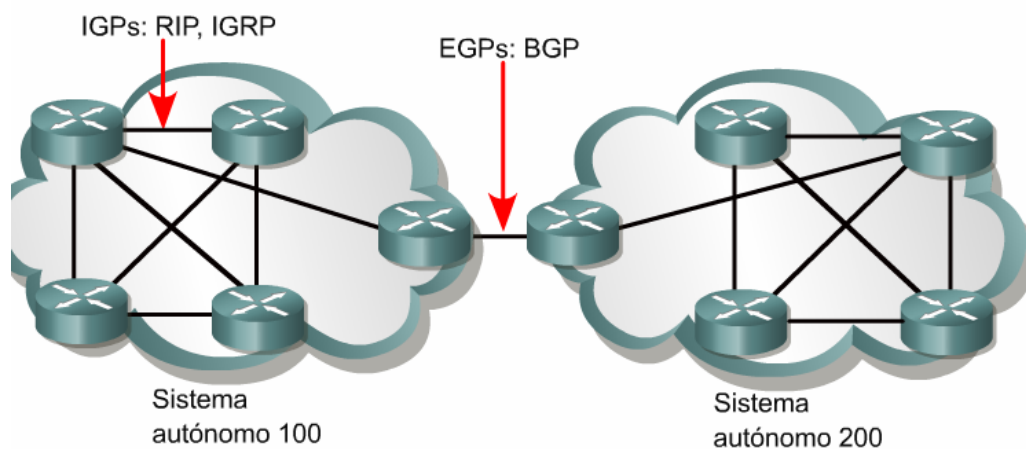


Figura 1

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. Los protocolos de enrutamiento de estado de enlace envían actualizaciones periódicas, conocidas como renovaciones de estado de enlace a rangos más prolongados; por ejemplo, 30 minutos.

Cuando una ruta o enlace se modifica, el dispositivo que detectó el cambio crea una publicación de estado de enlace (LSA) en relación a ese enlace. Luego la LSA se transmite a todos los dispositivos vecinos. Cada dispositivo de enrutamiento hace una copia de la LSA, actualiza su base de datos de estado de enlace y envía la LSA a todos los dispositivos vecinos. Se necesita esta inundación de LAS para estar seguros de que todos los dispositivos de enrutamiento creen bases de datos que reflejen de forma precisa la topología de la red antes de actualizar sus tablas de enrutamiento.

Por lo general, los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta. Ejemplos de protocolos de estado de enlace son: Primero la Ruta Libre Más Corta (OSPF) y el Sistema Intermedio a Sistema Intermedio (IS-IS).

10.2.9 Protocolos de enrutamiento

RIP es un protocolo de enrutamiento vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier enlace en internetwork. Si existen varias rutas hasta un destino, RIP elige la ruta con el menor número de saltos. Sin embargo, debido a que el número de saltos es la única métrica de enrutamiento que RIP utiliza, no siempre elige el camino más rápido hacia el destino. Además, RIP no puede enrutar un paquete más allá de los 15 saltos. RIP Versión 1 (RIPv1) necesita que todos los dispositivos de la red utilicen la misma máscara de subred, debido a que no incluye la información de la máscara en sus actualizaciones de enrutamiento. Esto también se conoce como enrutamiento con clase.

RIP Versión 2 (RIPv2) ofrece un prefijo de enrutamiento y envía información de la máscara de subred en sus actualizaciones. Esto también se conoce como enrutamiento sin clase. En los protocolos sin clase, las distintas subredes dentro de la misma red pueden tener varias máscaras de subred. El uso de diferentes máscaras de subred dentro de la misma red se denomina máscara de subred de longitud variable (VLSM).

IGRP es un protocolo de enrutamiento por vector-distancia desarrollado por Cisco. El IGRP se desarrolló específicamente para ocuparse de los problemas relacionados con el enrutamiento de grandes redes que no se podían administrar con protocolos como, por ejemplo, RIP. IGRP puede elegir la ruta disponible más rápida basándose en el retardo, el ancho de banda, la carga y la confiabilidad. IGRP también posee un límite máximo de número de saltos mucho mayor que RIP. IGRP utiliza sólo enrutamiento con clase.

OSPF es un protocolo de enrutamiento de estado de enlace desarrollado por la Fuerza de tareas de ingeniería de Internet (IETF) en 1988. El OSPF se elaboró para cubrir las necesidades de las grandes internetworks escalables que RIP no podía cubrir.

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, como se vio con anterioridad en este módulo. Para administrar de forma eficiente un número limitado de direcciones IP, todas las clases pueden subdividirse en subredes más pequeñas. La Figura 1 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 1

10.3.2 Introducción y razones para realizar subredes

Para crear la estructura de subred, los bits de host se deben reasignar como bits de subred. Este proceso es a veces denominado "pedir bits prestados". Sin embargo, un término más preciso sería "prestar" bits. El punto de inicio de este proceso se encuentra siempre en el bit del Host del extremo izquierdo, aquel que se encuentra más cerca del octeto de red anterior.

Las direcciones de subred incluyen la porción de red Clase A, Clase B o Clase C además de un campo de subred y un campo de Host. El campo de subred y el campo de Host se crean a partir de la porción de Host original de la dirección IP entera. Esto se hace mediante la reasignación de bits de la parte de host a la parte original de red de la dirección. La capacidad de dividir la porción de Host original de la dirección en nuevas subredes y campos de Host ofrece flexibilidad de direccionamiento al administrador de la red.

Además de la necesidad de contar con flexibilidad, la división en subredes permite que el administrador de la red brinde contención de broadcast y seguridad de bajo nivel en la LAN. La división en subredes ofrece algo de seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un Router. Además, el uso de listas de acceso puede ofrecer seguridad en el acceso. Estas listas pueden permitir o negar el acceso a la subred, tomando en cuenta varios criterios, de esta manera brindan mayor seguridad. Más tarde se estudiarán las listas de acceso. Algunos propietarios de redes Clases A y B

han descubierto que la división en subredes crea una fuente de ingresos para la organización a través del alquiler o venta de direcciones IP que anteriormente no se utilizaban.

Dirección de red 192.168.10.0 clase C

11000000.10101000.00001010.00000000

N . N . N . H

11000000.10101000.00001010.00000000

N . N . N . sN H

En este ejemplo se han asignado tres bits para designar la subred.

Dirección de red 147.10.0.0 clase B

10010011.00001010.00000000.00000000

N . N . H . H

10010011.00001010.00000000.00000000

N . N . sN H . H

En este ejemplo se han asignado cinco bits para designar la subred.

Dirección de red 28.0.0.0 clase A

00011100.00000000.00000000.00000000

N . H . H . H

00011100.00000000.00000000.00000000

N . sN . sN H . H

En este ejemplo se han asignado doce bits para designar la subred.

Figura 1

Una LAN se percibe como una sola red sin conocimiento de su estructura de red interna. Esta visión de la red hace que las tablas de enrutamiento sean pequeñas y eficientes. Dada una dirección de nodo local 147.10.43.14 de la subred 147.10.43.0, el mundo exterior sólo puede ver la red mayor que se anuncia, la 147.10.0.0. Esto tiene su razón en que la dirección de la subred local 147.10.43.0 sólo es válida dentro de la LAN donde se aplica el subneteo.

10.3.3 Cómo establecer la dirección de la máscara de subred

La selección del número de bits a utilizar en el proceso de división en subredes dependerá del número máximo de Hosts que se requiere por subred. Es necesario tener una buena comprensión de la matemática binaria básica y del valor de posición de los bits en cada octeto para calcular el número de subredes y Hosts creados cuando se pide bits prestados. ¹

Bits pedidos	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1

Figura 1

Es posible que los últimos dos bits del último octeto nunca se asignen a la subred, sea cual sea la clase de dirección IP. Estos bits se denominan los dos últimos bits significativos. El uso de todos los bits disponibles para crear subredes, excepto los dos últimos, dará como resultado subredes con sólo dos Hosts utilizables. Este es un método práctico de conservación de direcciones para el direccionamiento de enlace serial de Routers. Sin embargo, para una LAN que está en funcionamiento, puede que esto origine gastos prohibitivos en equipos.

Formato de barra diagonal	/25	/26	/27	/28	/29	/30	N/A	N/A
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

Figura 2

La máscara de subred da al Router la información necesaria para determinar en qué red y subred se encuentra un Host determinado. 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. ³ 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.

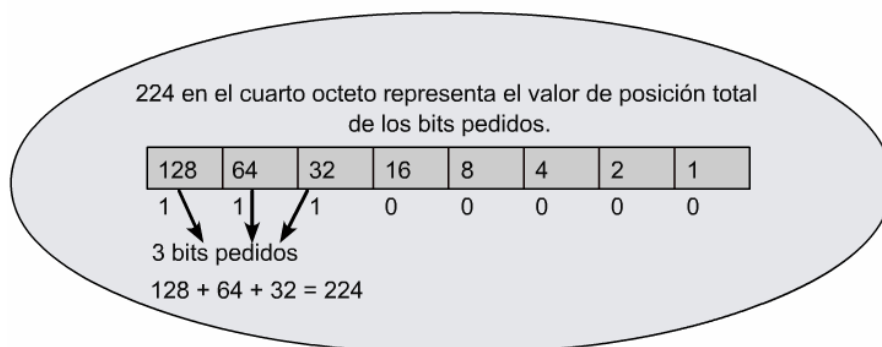


Figura 3

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 subredes. ⁴ Al consultar la fila denominada "Hosts Utilizables", se ve en la tabla que para 30 Hosts se requieren tres bits. La tabla también muestra que esto crea seis subredes utilizables, que satisfacen los requisitos de este esquema. La diferencia entre las direcciones válidas y el total es el resultado del uso de la primera dirección como el ID de la subred y de la última como la dirección de broadcast para cada subred. El tomar prestados el número adecuado de bits para obtener un número determinado de subredes y de hosts por subred puede generar el desperdicio de direcciones válidas en algunas subredes. La habilidad de usar estas direcciones no la proporciona un enrutamiento con distinción de clase. Sin embargo, el enrutamiento sin distinción de clase, el cual se cubrirá más adelante en el curso, permite el uso de estas direcciones.

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 4

El método que se utilizó para crear la tabla de subred puede usarse para resolver todos los problemas con subredes. ⁴ Este método utiliza la siguiente fórmula:

El número de subredes que se pueden usar es igual a dos a la potencia del número de bits asignados a subred, menos dos. La razón de restar dos es por las direcciones reservadas de ID de red y la dirección de broadcast.

$(2^{\text{potencia de bits prestados}}) - 2 = \text{subredes utilizables}$

$(2^3) - 2 = 6$

Número de Hosts utilizables = dos elevado a la potencia de los bits restantes, menos dos (direcciones reservadas para el ID de subred y el broadcast de subred)

$(2^{\text{potencia de los bits restantes del Host}}) - 2 = \text{Hosts utilizables}$

$(2^5) - 2 = 30$

10.3.4 Aplicación de la máscara de subred

Una vez que la máscara está establecida, puede utilizarse para crear el esquema de subred. ¹La tabla de la Figura es un ejemplo de subredes y direcciones que se crean al asignar tres bits al campo de la subred. Esto creará ocho subredes con 32 Hosts por subred. Comience desde cero (0) al asignar números a las subredes. La primera subred es siempre llamada subred cero.

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 1

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. ² 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.

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 2

Al consultar la tabla de subredes o al utilizar la fórmula, los tres bits asignados al campo de la subred darán como resultado 32 Hosts en total, asignados a cada subred. ² Esta información da el número de pasos de cada ID de subred. El ID de cada subred se establece agregando 32 a cada número anterior, comenzando con cero. ¹Observe que el ID de la subred tiene ceros binarios en la porción de Host.

El campo de broadcast es el último número en cada subred, y tiene unos binarios en la porción de Host. La dirección tiene la capacidad de emitir broadcast sólo a los miembros de una sola subred. ¹Ya que el ID de subred para la subred cero es 192.168.10.0 y hay un total de 32 Hosts, el ID de broadcast será 192.168.10.31 Comenzando con el cero, el trigésimo segundo número secuencial es el 31. Es importante recordar que cero (0) es un número real en el mundo de networking.

El resultado de la columna ID de broadcast puede completarse usando el mismo proceso que fue utilizado para la columna ID de la subred. Simplemente agregue 32 al ID de broadcast anterior de la subred. Otra opción es comenzar por el final de la columna y calcular hacia arriba restando uno al ID de subred anterior.

10.3.5 Cómo 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. ¹ ²

Dirección de red 147.10.0.0 clase B (14 bits disponible)			
11001011.00001010.00000000.00000000			
N . N . H . H			
10010011.00001010.00000000.00000000			
N . N . sN . sN H			

En este ejemplo, se han asignado 12 bits para designar la subred.

Figura 1

Dirección de red 28.0.0.0 clase A (22 bits disponibles)			
00011100.00000000.00000000.00000000			
N . H . H . H			
00011100.00000000.00000000.00000000			
N . sN . sN . sN H			

En este ejemplo, se han asignado 20 bits para designar la subred.

Figura 2

Al asignar 12 bits de una dirección de Clase B a un campo de subred, se crea una máscara de subred de 255.255.255.240 o /28. Los ocho bits fueron asignados al tercer octeto dando como resultado 255, el valor total de los ocho bits juntos. Se asignaron cuatro bits en el cuarto octeto dando 240 como resultado. Recuerde que el número después de la barra inclinada equivale a la suma total de todos los bits asignados al campo de subred más los bits de red fijos. ³

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	2	4	8	16	32	64	128	256

Figura 3

Al asignar 20 bits de una dirección de Clase B a un campo de subred, se crea una máscara de subred de 255.255.255.240 o /28. Los ocho bits del segundo y tercer octeto fueron asignados al campo de subred y a cuatro bits del cuarto octeto.

En esta situación, parece que las máscaras de subred de las direcciones de Clase A y Clase B son idénticas. A menos que la máscara esté relacionada con una dirección de red, no es posible descifrar cuántos bits fueron asignados al campo de subred.

No importa qué clase de dirección se necesite dividir en subredes, las reglas son las siguientes:

Subredes totales = 2 ^{a la potencia de los bits pedidos}

Hosts totales = 2 ^{a la potencia de los bits restantes}

Subredes utilizables = $2^{\text{a la potencia de los bits pedidos}}$ **menos 2**
Hosts utilizables = $2^{\text{a la potencia de los bits restantes}}$ **menos 2**

10.3.6 Cálculo de la subred de residencia utilizando la operación "AND"

Los Routers utilizan máscaras de subred para establecer las subredes de origen para nodos individuales. Este proceso se denomina operación "AND" lógico. La operación "AND" es un proceso binario por medio del cual un Router calcula el ID de la subred para un paquete entrante. **1** La operación "AND" es parecida a la multiplicación.

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

Figura 1

Dirección de paquete	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Máscara	255.255.255.224	11111111.11111111.11111111.11100000
ID de subred	201.10.11.64	11001001.00001010.00001011.01000000

Figura 2

Este proceso se administra a un nivel binario. Por lo tanto, es necesario ver la dirección IP y la máscara de forma binaria. **2** 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 ninguna clase, durante el examen de certificación.

Resumen

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

- Características de los protocolos enrutados o enrutables.
- Los pasos del encapsulamiento de los datos en internetwork a medida que los datos se enruta a uno o más dispositivos de Capa 3.
- Entrega no orientada a la conexión y orientada a la conexión.
- Campos de paquetes IP
- Los Routers operan a nivel de la capa de red. Inicialmente, el Router recibe una trama de Capa 2 con un paquete encapsulado de Capa 3 en su interior. El Router debe quitar la trama de Capa 2 y examinar el paquete de Capa 3. Una vez que el Router está listo para transmitir el paquete, el Router debe encapsular el paquete de Capa 3 en una nueva trama de Capa 2.
- Los protocolos enrutados definen el formato y uso de los campos dentro de un paquete. Los paquetes generalmente se transfieren de un sistema final a otro.
- La conmutación de LAN tiene lugar en la Capa 2 del modelo de referencia OSI, y el enrutamiento en la Capa 3.
- Se utilizan protocolos de enrutamiento entre los Routers para determinar la ruta y guardar las tablas de enrutamiento. Se utilizan protocolos enrutados para dirigir el tráfico del usuario.
- El enrutamiento implica dos actividades principales: Determinación de las mejores rutas posibles y transportación de paquetes por la internetwork.

- Los algoritmos de enrutamiento procesan actualizaciones de enrutamiento y construyen tablas de enrutamiento con las mejores rutas.
- Las tablas de enrutamiento contienen las mejores rutas hacia todas las redes conocidas. Estas rutas pueden ser estáticas (de ingreso manual) o dinámicas (que se conocen a través de protocolos de enrutamiento)
- La convergencia describe la velocidad a la que todas los Routers llegan a un acuerdo con respecto a una modificación en la red.
- Los protocolos de enrutamiento interior enrutan los datos dentro de sistemas autónomos, mientras que los protocolos de enrutamiento exterior enrutan los datos entre sistemas autónomos.
- Los Routers que utilizan protocolos de enrutamiento vector-distancia envían actualizaciones en forma periódica que contienen toda o parte de su tabla de enrutamiento. Los Routers que usan protocolos de enrutamiento de estado de enlace, utilizan publicaciones de estado de enlace (LSA) para enviar actualizaciones sólo cuando ocurren cambios en la topología de la red, y envían tablas de enrutamiento completas con mucha menos frecuencia.
- Los usos de la división en subredes.
- Cómo determinar la máscara de subred apropiada para una situación dada.
- Cómo dividir las redes de Clase A, B y C en subredes.
- Cómo utilizar máscaras de subred para determinar el ID de subred.

Módulo 11: Capas de aplicación y transporte de TCP/IP

Descripción general

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.

Los estudiantes que completen este módulo deberán poder:

- Describir las funciones de la capa de transporte TCP/IP.
- Describir el control de flujo.
- Describir los procesos que se usan para establecer una conexión entre sistemas pares o iguales.
- Describir el uso de ventanas.
- Describir los acuses de recibo.
- Identificar y describir los protocolos de la capa de transporte.
- Describir los formatos de encabezado TCP y UDP.
- Describir los números de puerto TCP y UDP.
- Hacer una lista de los protocolos principales de la capa de aplicación TCP/IP.
- Suministrar una descripción breve acerca de las características y operaciones de las aplicaciones TCP/IP conocidas.

11.1 TCP/IP Capa de Transporte

11.1.1 Introducción a la capa de transporte

Las tareas principales de la capa de transporte, la Capa 4 del modelo OSI, son transportar y regular el flujo de información desde el origen hasta el destino, de forma confiable y precisa. El control de extremo a extremo y la confiabilidad se suministran a través de ventanas deslizantes, números de secuencia y acuses de recibo. ¹

El transporte confiable puede lograr lo siguiente:

- Asegúrese de que se acuse recibo de los segmentos entregados al remitente
- Realizar la retransmisión de cualquier segmento que no genere acuse de recibo.
- Volver a poner los segmentos en su secuencia correcta en el destino.
- Evitar y controlar la congestión.

Figura 1

Para comprender qué son la confiabilidad y el control de flujo, piense en alguien que estudia un idioma extranjero durante un año y luego visita el país en el que se habla ese idioma. Mientras uno conversa, las palabras se deben repetir para que exista confiabilidad y se debe hablar lentamente de modo que el significado de la conversación no se pierda; esto es lo que se denomina control de flujo.

La capa de transporte brinda servicios de transporte desde el host origen hasta el host destino. Establece una conexión lógica entre los puntos de terminación de la red. Los protocolos de la capa de transporte segmentan y reensamblan los datos mandados por las aplicaciones de capas superiores en el mismo flujo de datos de capa de transporte. Este flujo de datos de la capa de transporte brinda servicios de transporte de extremo a extremo.

El flujo de datos de la capa de transporte es una conexión lógica entre los puntos de terminación de una red. Sus tareas principales son las de transportar y regular el flujo de información desde el origen hasta el

destino de forma confiable y precisa. La tarea principal de la Capa 4 es suministrar control de extremo a extremo usando ventanas deslizantes y brindar confiabilidad para los números de secuencia y los acuses de recibo. La capa de transporte define la conectividad de extremo a extremo entre las aplicaciones del host. Los servicios de transporte incluyen los siguientes servicios básicos:

- Segmentación de los datos de las aplicaciones de capa superior
- Establecimiento de las operaciones de extremo a extremo
- Transporte de segmentos desde un host final a otro host final
- Control de flujo, suministrado por las ventanas deslizantes
- Confiabilidad, suministrada por los números de secuencia y los acuses de recibo

TCP/IP es una combinación de dos protocolos individuales. IP opera en la Capa 3 y es un servicio no orientado a conexión que proporciona una entrega de máximo esfuerzo a través de una red. TCP opera en la Capa 4, y es un servicio orientado a conexión que suministra control de flujo y confiabilidad. Al unir estos protocolos, se suministra una gama de servicios más amplia. De forma conjunta, constituyen la base para un conjunto completo de protocolos que se denomina conjunto de protocolos TCP/IP. La Internet se basa en este conjunto de protocolos 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. ¹

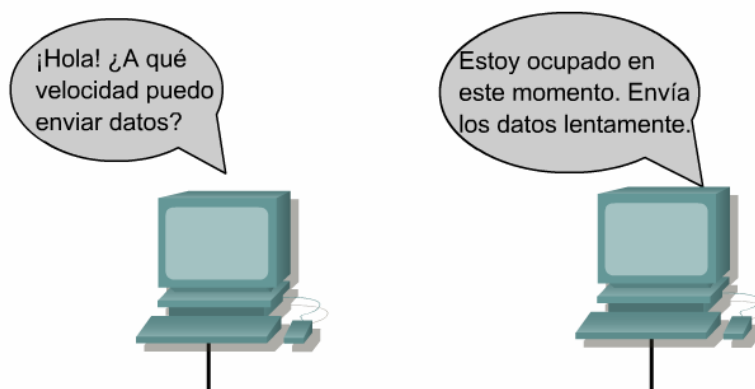


Figura 1

11.1.3 Descripción general del establecimiento, mantenimiento y terminación de sesión

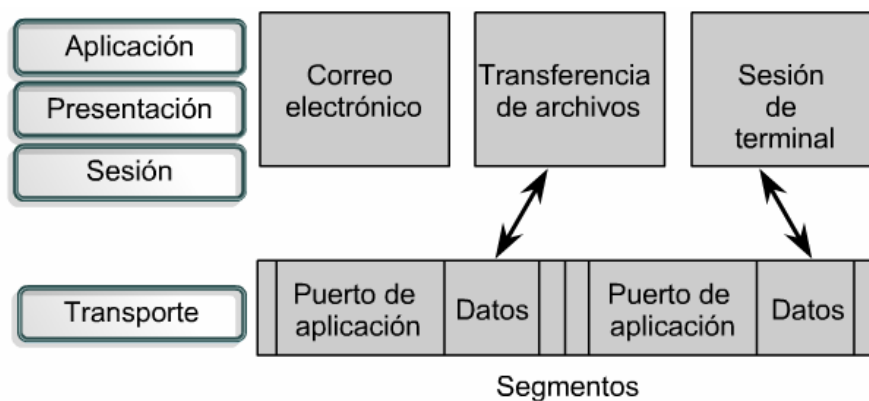


Figura 1

Múltiples aplicaciones pueden compartir la misma conexión de transporte en el modelo de referencia OSI. ¹ 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 el modelos de referencia OSI. Esto se denomina multiplexión de conversaciones de capas superiores. 1 Varias conversaciones simultáneas de las capas superiores se pueden multiplexar en una sola conexión.

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. Un nodo inicia la conexión, que debe ser aceptada por el otro. Los módulos de software de protocolo en los dos sistemas operativos se comunican entre sí enviando mensajes a través de la red a fin de verificar que la transferencia esté autorizada y que ambos lados estén preparados.

Después de que se haya establecido toda la sincronización, se establece la conexión y comienza la transferencia de datos. Durante la transferencia, los dos dispositivos siguen comunicándose con su software de protocolo para verificar que estén recibiendo los datos correctamente.

La Figura 2 muestra una conexión típica entre sistemas emisores y receptores. El primer intercambio de señal solicita la sincronización. El segundo y el tercer intercambio de señales acusan recibo de la petición inicial de sincronización, y sincronizan los parámetros de conexión en sentido opuesto. El segmento final del intercambio de señales es un acuse de recibo que se utiliza para informar al destino que ambos lados aceptan que se ha establecido una conexión. A partir del momento en que se establece la conexión, comienza la transferencia de datos.

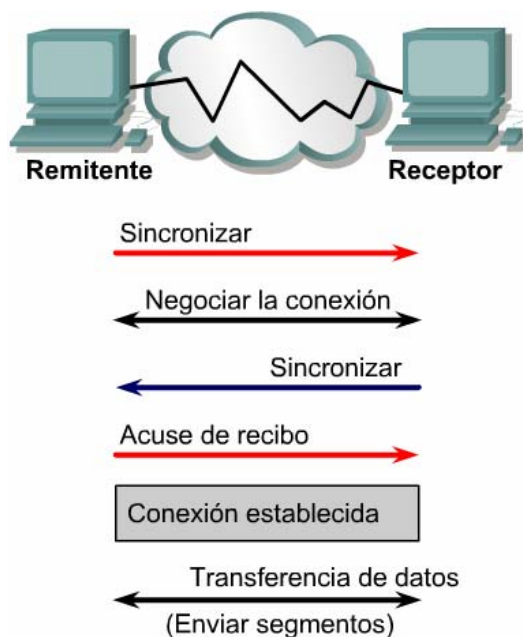


Figura 2

Un congestionamiento puede ocurrir durante la transferencia de datos por dos razones:

- Primero, una computadora de alta velocidad es capaz de generar tráfico más rápido que lo que la red tarda en transmitirla.
- Segundo, si varias computadoras requieren mandar datagramas simultáneamente a un mismo destino, éste puede experimentar un congestionamiento, aunque no se tenga un origen único.

Cuando los datagramas llegan demasiado rápido como para que un host o gateway los procese, se almacenan temporalmente en la memoria. Si el tráfico continúa, tarde o temprano el host o el gateway agota su memoria y debe descartar cualquier otro datagrama que llegue.

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.

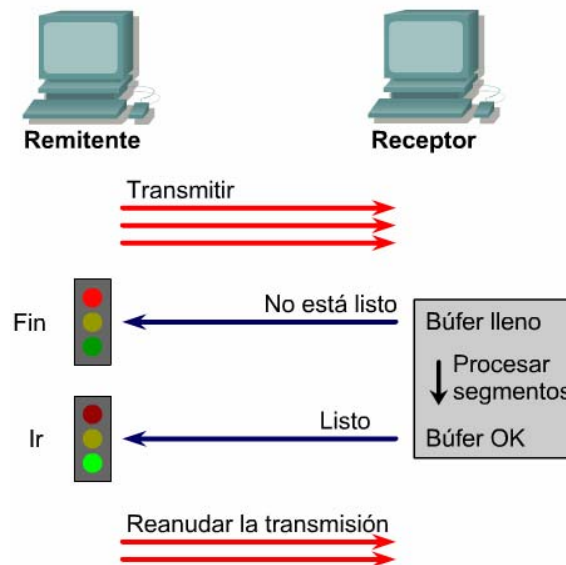


Figura 3

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.

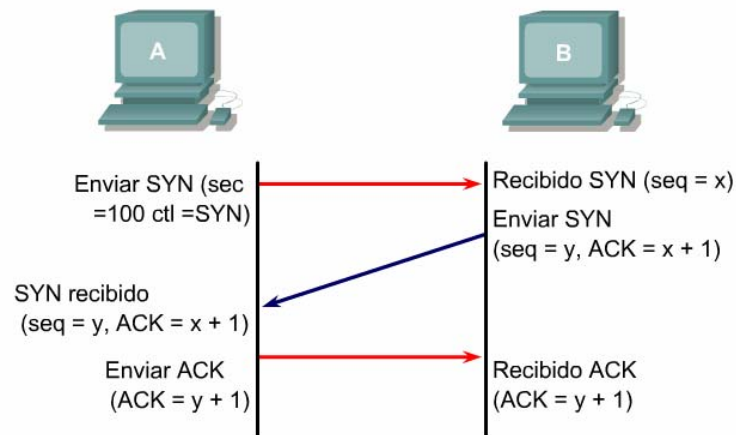


Figura 1

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. Cada una de las partes también debe recibir el INS de la otra parte y enviar un ACK de confirmación. La secuencia es la siguiente:

1. El origen (A) inicializa una conexión mandando un paquete de SYN hacia el host destino (B) indicando su INS = X:
A → B SYN, seq de A = X
2. B recibe el paquete, graba que el seq de A = X, responde con un ACK de X + 1, e indica que su INS = Y. El ACK de X + 1 significa que el host B recibió todos los octetos incluyendo X y ahora espera X + 1 siguiente:
B → A ACK, seq de A = X, SYN seq de B = Y, ACK = X + 1

3. A recibe el paquete de B, y sabe que el seq de B = Y, y responde con un ACK de Y + 1, el cual termina el proceso de conexión:
A→B ACK, seq de B = Y, ACK = Y + 1

Este intercambio se denomina intercambio de señales de tres vías. ¹

El intercambio de señales de tres vías es necesario dado que los números de secuencia no están conectados a ningún reloj global de la red y los protocolos TCP pueden tener distintos mecanismos para elegir el ISN. El receptor del primer SYN no tiene forma de saber si el segmento es un antiguo segmento demorado, a menos que recuerde el último número de secuencia utilizado en la conexión. No siempre es posible recordar ese número. Por lo tanto, debe solicitar al emisor que verifique este SYN.

11.1.5 Uso de ventanas

Los paquetes de datos se deben enviar al receptor en el mismo orden en los que se transmitieron para lograr una transferencia de datos confiable, orientada a conexión. Los protocolos fallan si algún paquete se pierde, se daña, se duplica o se recibe en un orden distinto. Una solución sencilla es que el receptor acuse recibo de cada paquete antes de que se envíe el siguiente paquete. ¹

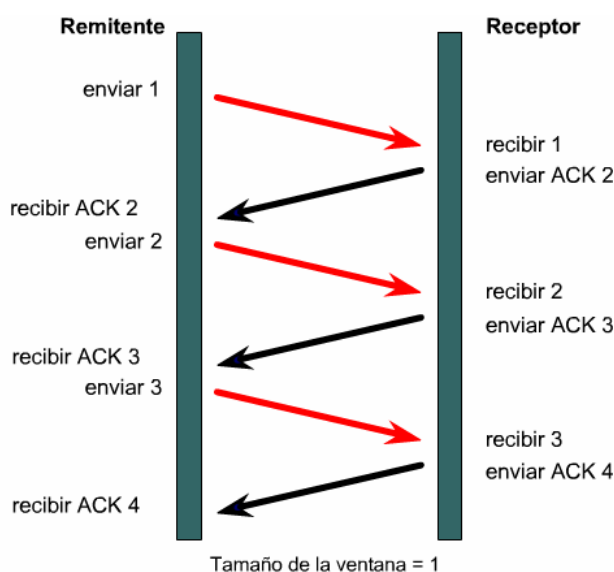


Figura 1

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 termina 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.

Como se muestra en la Figura ², el emisor envía tres paquetes antes de recibir un ACK (acuse de recibo). Si el receptor puede manejar un tamaño de ventana de sólo dos paquetes, la ventana descarta el paquete tres, especifica tres como el siguiente paquete y especifica un nuevo tamaño de ventana de dos. El emisor

envía los dos siguientes paquetes, pero continúa especificando un tamaño de ventana de tres. Esto significa que el emisor continúa esperando recibir un acuse de recibo de tres paquetes de parte del receptor. El receptor responde solicitando el paquete cinco y especifica nuevamente un tamaño de ventana de dos.

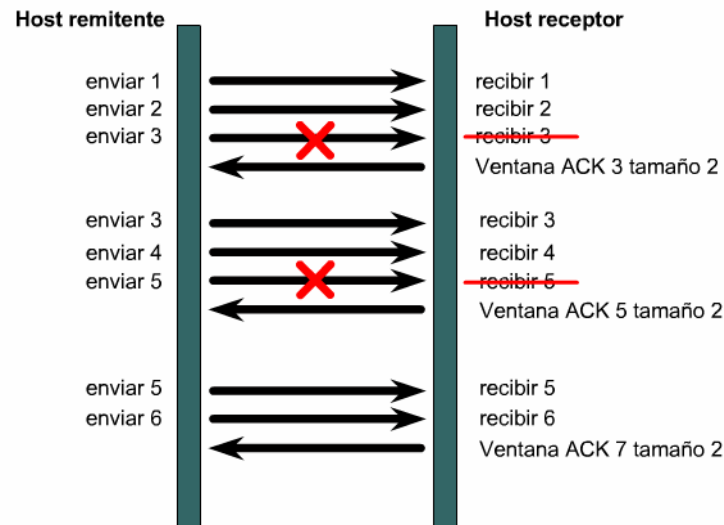


Figura 2

11.1.6 Acuse de recibo

La entrega confiable garantiza que una corriente de datos enviada desde un dispositivo sea entregada a través de un enlace de datos a otro dispositivo sin que se dupliquen o pierdan los datos. El acuse de recibo positivo con retransmisión es una técnica que garantiza la entrega confiable de los datos. El acuse de recibo positivo requiere que el receptor se comuniquen con el origen, enviando un mensaje de acuse de recibo una vez que recibe los datos. El emisor mantiene un registro de cada paquete de datos (segmento TCP) que envía y del que espera recibir un acuse de recibo. El emisor también inicia un temporizador cada vez que envía un segmento y retransmite el segmento si el temporizador expira antes de que llegue el acuse de recibo.

La figura 1 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.

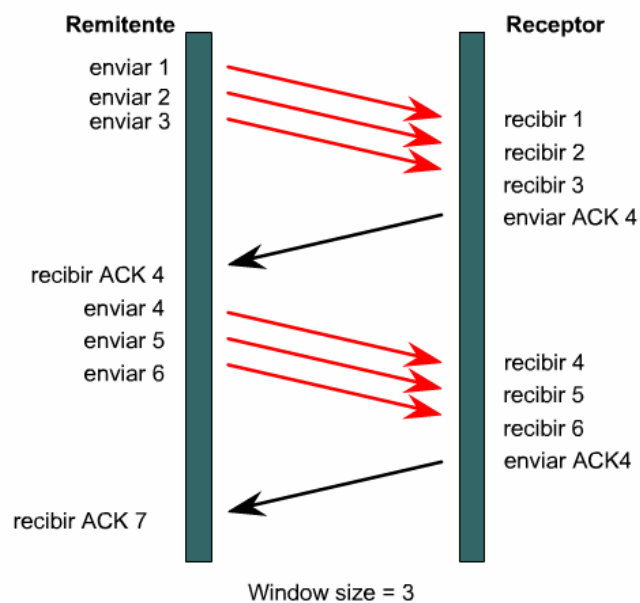
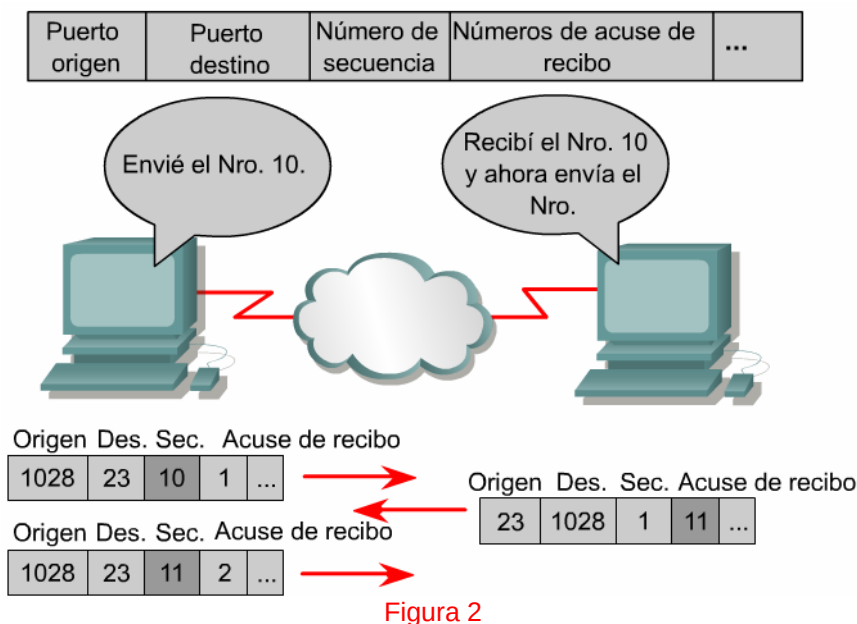


Figura 1

TCP suministra secuenciamiento de segmentos con un acuse positivo de recibo de referencia de envío. Cada segmento se enumera antes de la transmisión. ²En la estación receptora, TCP reensambla los segmentos hasta formar un mensaje completo. Si falta un número de secuencia en la serie, el segmento se vuelve a transmitir. Los segmentos para los cuales no se acusa recibo dentro de un período determinado de tiempo darán como resultado una retransmisión.



11.1.7 Protocolo para el Control de la Transmisión (TCP)

El Protocolo para el control de la transmisión (TCP) es un protocolo de Capa 4 orientado a conexión que suministra una transmisión de datos full-duplex confiable. TCP forma parte de la pila del protocolo TCP/IP. En un entorno orientado a conexión, se establece una conexión entre ambos extremos antes de que se pueda iniciar la transferencia de información. TCP es responsable por la división de los mensajes en segmentos, reensamblándolos en la estación destino, reenviando cualquier mensaje que no se haya recibido y reensamblando mensajes a partir de los segmentos. TCP suministra un circuito virtual entre las aplicaciones del usuario final.

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

Bit 0				Bit 15		Bit 16		Bit 31	
Puerto origen (16)				Puerto destino (16)					
Número de secuencia (32)									
Número de acuse de recibo (32)									
Longitud del encabezado (4)		Reservado (6)		Bits de código (6)		Ventana (16)			
Checksum (16)				Urgente (16)					
Opciones (0 ó 32 si las hay)									
Datos (varía)									

20 Bytes

Figura 1

Las siguientes son las definiciones de los campos de un segmento TCP: ¹

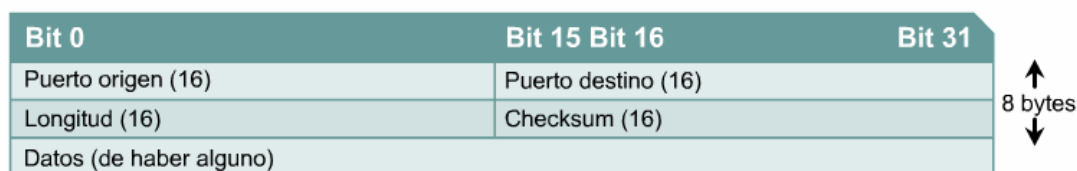
- **Puerto origen:** El número del puerto que realiza la llamada.
- **Puerto destino:** El número del puerto al que se realiza la llamada.
- **Número de secuencia:** El número que se usa para asegurar el secuenciamiento correcto de los datos entrantes.

- **Número de acuse de recibo:** Siguiendo 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.

11.1.8 Protocolo de Datagrama de Usuario (UDP)

El Protocolo de datagrama de usuario (UDP: User Datagram Protocol) es el protocolo de transporte no orientado a conexión de la pila de protocolo TCP/IP. El UDP es un protocolo simple que intercambia datagramas sin acuse de recibo ni garantía de entrega. El procesamiento de errores y la retransmisión deben ser manejados por protocolos de capa superior.

El UDP no usa ventanas ni acuses de recibo de modo que la confiabilidad, de ser necesario, se suministra a través de protocolos de la capa de aplicación. El UDP está diseñado para aplicaciones que no necesitan ensamblar secuencias de segmentos.



Los protocolos que usan UDP incluyen:

- TFTP (Protocolo trivial de transferencia de archivos)
- (SNMP) Protocolo simple de administración de red
- DHCP (Protocolo de configuración dinámica del host)
- DNS (Sistema de denominación de dominios)

Las siguientes son las definiciones de los campos de un segmento UDP:

- **Puerto origen:** Número del puerto que realiza la llamada
- **Puerto destino:** Número del puerto al que se realiza la llamada
- **Longitud:** Número de bytes que se incluyen en el encabezado y los datos
- **Checksum (suma de comprobación):** Suma de comprobación calculada a partir de los campos del encabezado y de los datos.
- **Datos:** Datos de protocolo de capa superior.

11.1.9 Números 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.

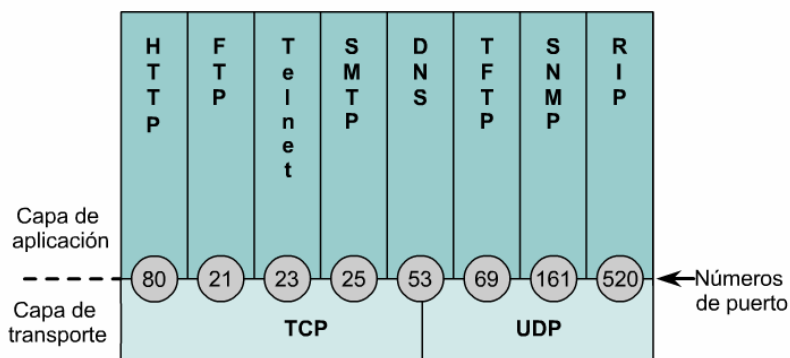


Figura 1

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). ¹ 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.

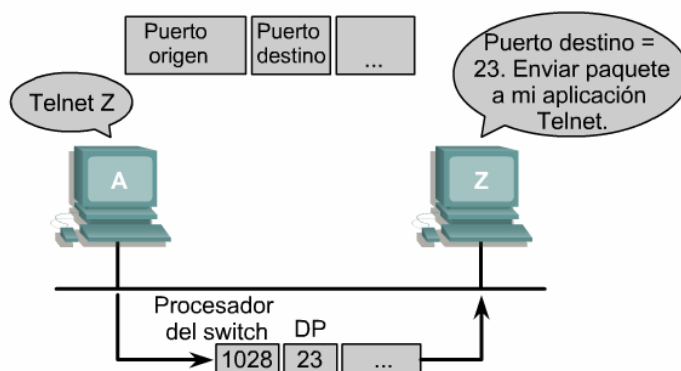


Figura 2

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.

²

11.2 Capa de Aplicación

11.2.1 Introducción a la capa de aplicación TCP/IP

Cuando se diseñó el modelo TCP/IP, las capas de sesión y de presentación del modelo OSI se agruparon en la capa de aplicación del modelo TCP. Esto significa que los aspectos de representación, codificación y control de diálogo se administran en la capa de aplicación en lugar de hacerlo en las capas inferiores individuales, como sucede en el modelo OSI. Este diseño garantiza que el modelo TCP/IP brinda la máxima flexibilidad, en la capa de aplicación, para los desarrolladores de software.

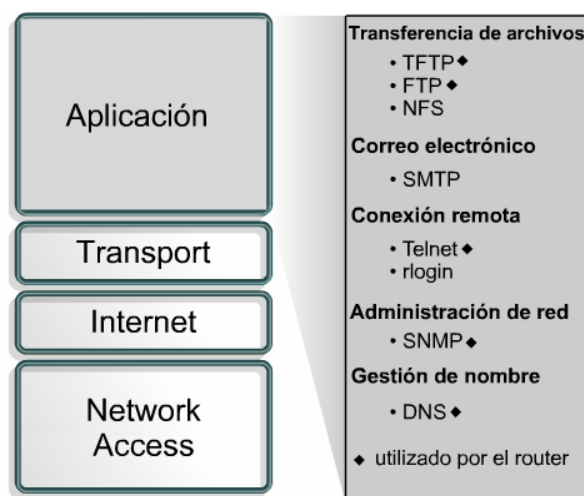


Figura 1

Los protocolos TCP/IP que admiten transferencia de archivos, correo electrónico y conexión remota probablemente sean los más familiares para los usuarios de la Internet. ¹ Estos protocolos incluyen las siguientes aplicaciones:

- Sistema de denominación de dominios (DNS)
- Protocolo de transferencia de archivos (FTP)
- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo simple de administración de red (SNMP)
- Telnet

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 computadores 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 computador 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 computadores 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. Una vez que se ha completado toda la sesión para copiar y trasladar archivos, el vínculo de comandos se cierra cuando el usuario se desconecta y finaliza la sesión.

TFTP es un servicio no orientado a conexión que usa el Protocolo de datagramas del usuario (UDP). TFTP se usa en el router para transferir archivos de configuración e imágenes de Cisco IOS y para transferir archivos entre sistemas que admiten TFTP. TFTP está diseñado para ser pequeño y fácil de implementar. Por lo tanto, carece de la mayoría de las características de FTP. TFTP puede leer o escribir archivos desde o hacia un servidor remoto pero no puede listar los directorios y no tiene manera de proporcionar autenticación de usuario. Es útil en algunas LAN porque opera más rápidamente que FTP y, en un entorno estable, funciona de forma confiable.

11.2.4 HTTP

El Protocolo de transferencia de hipertexto (http: Hypertext Transfer Protocol) funciona con la World Wide Web, que es la parte de crecimiento más rápido y más utilizada de Internet. Una de las principales razones de este crecimiento sorprendente de la Web es la facilidad con la que permite acceder a la información. Un navegador de Web es una aplicación cliente/servidor, lo que significa que requiere que haya tanto un componente de cliente como de servidor para que funcione. Un navegador de Web presenta datos en formatos multimediales en las páginas Web que usan texto, gráficos, sonido y vídeo. Las páginas Web se

crean con un lenguaje de formato denominado Lenguaje de etiquetas por hipertexto (HTML: Hypertext Markup Language). HTML dirige a un navegador de Web en una página Web en particular para crear el aspecto de la página de forma específica. Además, HTML especifica la colocación del texto, los archivos y objetos que se deben transferir desde el servidor de Web al navegador de Web.

Los hipervínculos hacen que la World Wide Web sea fácil de navegar. Un hipervínculo es un objeto, una frase o una imagen en una página Web. Cuando se hace clic en el hipervínculo, transfiere el navegador a otra página Web. La página Web a menudo contiene oculta dentro de su descripción HTML, una ubicación de dirección que se denomina Localizador de Recursos Uniforme (URL: Uniform Resource Locator).

En el URL `http://www.cisco.com/edu/`, los caracteres "`http://`" le indican al navegador cuál es el protocolo que debe utilizar. La segunda parte, "`www`", es el nombre de host o nombre de una máquina determinada con una dirección IP determinada. La última parte identifica la carpeta específica que contiene la página web por defecto en el servidor. ¹

<code>http://</code>	<code>www.</code>	<code>cisco.com</code>	<code>/edu/</code>
Le indica al navegador qué tipo de protocolo se debe usar.	Identifica el nombre de host o el nombre de un aparato determinado	Representa la entidad de dominio del sitio Web.	Identifica la carpeta donde se localiza la página Web en el servidor. Adicionalmente, ya que no se especificó un nombre, el navegador cargará la página por defecto identificada por el servidor

Figura 1

Un navegador de Web generalmente se abre en una página de inicio o "home" (de presentación). El URL de la página de presentación ya se ha almacenado en el área de configuración del navegador de Web y se puede modificar en cualquier momento. Desde la página de inicio, haga clic en uno de los hipervínculos de la página Web o escriba un URL en la barra de dirección del navegador. 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. ¹ 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.

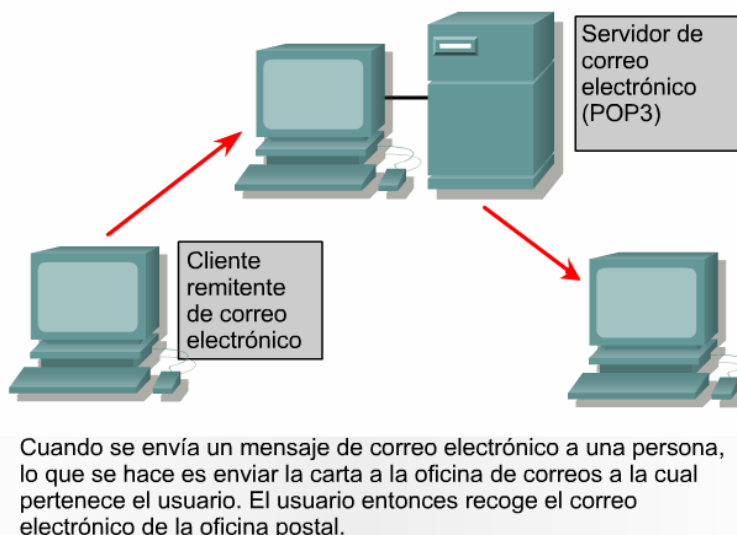


Figura 1

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 protocolo SMTP no brinda muchas funciones de seguridad y no requiere ninguna autenticación. A menudo, los administradores no permiten que los hosts que no forman parte de su red usen el servidor SMTP para enviar o transmitir correo. Esto es para evitar que los usuarios no autorizados usen los servidores como transmisores de correo.

11.2.6 SNMP

El Protocolo simple de administración de red (SNMP: Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. El SNMP permite que los administradores de red administren el rendimiento de la red, detecten y solucionen los problemas de red y planifiquen el crecimiento de la red. El SNMP usa UDP como su protocolo de capa de transporte.

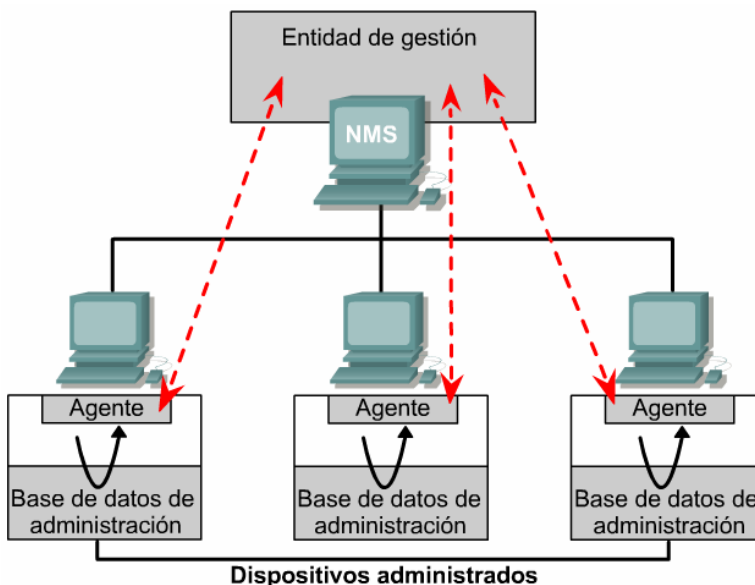


Figura 1

Una red administrada con SNMP está compuesta por los tres componentes clave que se detallan a continuación: **1**

- **Sistema de administración de la red (NMS: Network Management System):** El NMS ejecuta aplicaciones que monitorean y controlan los dispositivos administrados. La gran mayoría de los recursos de procesamiento y de memoria que se requieren para la administración de red se suministra a través del NMS. Deben existir uno o más NMS en cualquier red administrada.
- **Dispositivos administrados:** Los dispositivos administrados son nodos de red que contienen un agente SNMP y que residen en una red administrada. Los dispositivos administrados recopilan y guardan información de administración y ponen esta información a disposición de los NMS usando SNMP. Los dispositivos administrados, a veces denominados elementos de red, pueden ser routers, servidores de acceso, switches y puentes, hubs, hosts del computador o impresoras.
- **Agentes:** Los agentes son módulos del software de administración de red que residen en los dispositivos administrados. Un agente tiene conocimiento local de la información de administración y convierte esa información a un formato compatible con SNMP.

11.2.7 Telnet

El software de cliente Telnet brinda la capacidad de conectarse a un host de Internet remoto que ejecuta una aplicación de servidor Telnet y, a continuación, ejecutar comandos desde la línea de comandos. Un cliente Telnet se denomina host local. El servidor Telnet, que usa un software especial denominado daemon, se denomina host remoto.

Para realizar una conexión desde un cliente Telnet, se debe seleccionar la opción de conexión. Generalmente, un cuadro de diálogo indica que se debe colocar un nombre de host y un tipo de terminal. El nombre de host es la dirección IP o el nombre DNS del computador 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 del computador 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.

Resumen

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

- Las funciones de la capa de transporte de TCP/IP
- Control de flujo
- Los procesos que se usan para establecer una conexión entre sistemas pares o iguales
- Uso de ventanas
- Acuse de recibo
- Protocolos de la capa de transporte
- Formatos del encabezado TCP y UDP
- Números de puerto TCP y UDP
- Los procesos y protocolos principales de la capa de aplicación TCP/IP
- Servicios de denominación de dominio
- Protocolos de transferencia de archivos
- Protocolo simple de transferencia de correo
- Protocolo simple de administración de red
- Telnet

MicroCisco - staky



CCNA 2: Principios básicos de routers y enrutamiento v3.1

CCNA 2: Routers y Principios básicos de enrutamiento es el segundo de los cuatro cursos necesarios para obtener la certificación como Asociado de Red Certificado de Cisco (CCNA). CCNA 2 se concentra en la configuración inicial del router, la administración del software Cisco IOS, la configuración del protocolo de enrutamiento, TCP/IP y las listas de control de acceso (ACLs). Los estudiantes desarrollarán capacidades que les permitirán configurar un router, administrar el software Cisco IOS, configurar los protocolos de enrutamiento y crear listas de acceso que controlen el acceso al router.

Módulo 1: Las WAN y los routers

Descripción general

Una red de área amplia (WAN) es una red de comunicaciones de datos que cubre una extensa área geográfica. Las WAN presentan varias características importantes que las distinguen de las LAN. La primera lección de este módulo proporcionará un panorama de las tecnologías y protocolos WAN. También explicará las similitudes y diferencias entre las redes WAN y LAN.

Resulta importante entender los componentes de la capa física de un router. Esta comprensión sienta las bases para otros conocimientos y habilidades necesarios para configurar los routers y administrar las redes enrutadas. Este módulo proporciona una detallada inspección de los componentes físicos internos y externos de un router. También describe las técnicas para establecer una conexión física entre las distintas interfaces de los routers.

Los estudiantes que completen este módulo deberán poder:

- Identificar las organizaciones responsables de los estándares WAN.
- Explicar la diferencia entre una WAN y una LAN y el tipo de direcciones que utiliza cada una de ellas.
- Describir la función de un router en una WAN
- Identificar los componentes internos del router y describir sus funciones.
- Describir las características físicas del router.
- Identificar los puertos comunes de un router.
- Conectar, correctamente, los puertos de Ethernet, de WAN serial y de consola.

1.1 Redes WAN

1.1.1 Introducción a las redes WAN

Una red de área amplia (WAN) es una red de comunicación de datos que cubre una extensa área geográfica como por ejemplo un estado, una provincia o un país. A menudo, las WAN utilizan instalaciones de transmisión provistas por los proveedores de servicios de telecomunicaciones comunes, por ejemplo: las compañías telefónicas. ¹

Distancia entre los dispositivos	Ubicación de los hosts	Nombre
10m	Habitación	Red de área local Aula
100m	Edificio	Red de área local Escuela
1000m = 1km	Campus	Red de área local Universidad
10,000m = 10km	Ciudad	Red de área metropolitana
100,000m = 100km	País	Red de área amplia de Cisco Systems, Inc.
1,000,000m = 1,000km	Continente	Red de área amplia África
10,000,000m = 10,000km	Planeta	Red de área amplia Internet
100,000,000m = 100,000km	Sistemas tierra-luna	Red de área amplia Tierra y satélites artificiales

Figura 1

Las características principales de las WAN son las siguientes:

- Conectan dispositivos que están separados por áreas geográficas extensas.
- Utilizan los servicios de proveedores de telecomunicaciones tales como las empresas operativas Regional Bell (RBOC), Sprint, MCI y VPM Internet Services Inc.
- Usan conexiones seriales de diversos tipos para acceder al ancho de banda a través de áreas geográficas extensas.

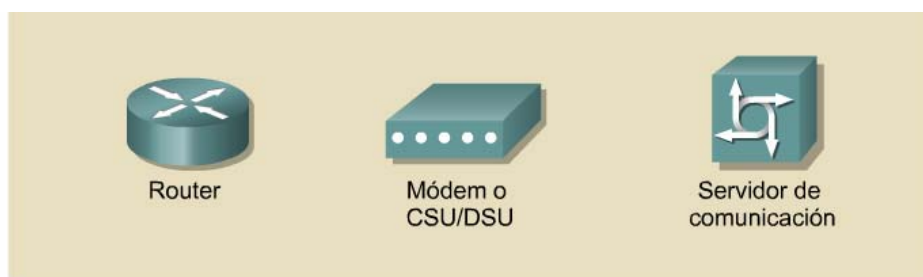
Una WAN difiere de una LAN (redes de área local) de varias formas. Por ejemplo, a diferencia de una LAN, que conecta estaciones de trabajo, periféricos, terminales y otros dispositivos dentro de un sólo edificio o en

una área geográfica pequeña, una WAN realiza conexiones de datos a través de una amplia área geográfica. Las compañías usan las WAN para conectar sus distintos establecimientos de modo que se pueda intercambiar información entre oficinas distantes.

Una WAN opera en la capa física y la capa de enlace de datos del modelo de referencia OSI. Interconecta las LAN que normalmente se encuentran separadas por grandes áreas geográficas. Las WAN permiten el intercambio de paquetes y tramas de datos entre routers y switches y las LAN que mantienen.

Los siguientes dispositivos se usan en las WAN: 2 3

- Los routers ofrecen varios servicios, entre ellos el internetworking y los puertos de interfaz WAN
- Los módems incluyen servicios de interfaz de grado de voz; unidades de servicio de canal/unidades de servicio de datos (CSU/DSU) que realizan la interfaz con los servicios T1/E1; y los Adaptadores de terminal/Terminación de red 1 (TA/NT1) que realizan la interfaz con los servicios de Red digital de servicios integrados (RDSI)
- Los servidores de comunicación concentran las comunicaciones de usuarios de acceso telefónico entrante y saliente.



Las WAN se diseñan para:

- Operan dentro de un área geográfica extensa
- Permite la opción de una conexión serial de bajo ancho de banda y de bajo costo o una conexión ATM o fibra óptica de mayor ancho de banda y de mayor costo.
- Suministran conectividad parcial y continua

Figura 2

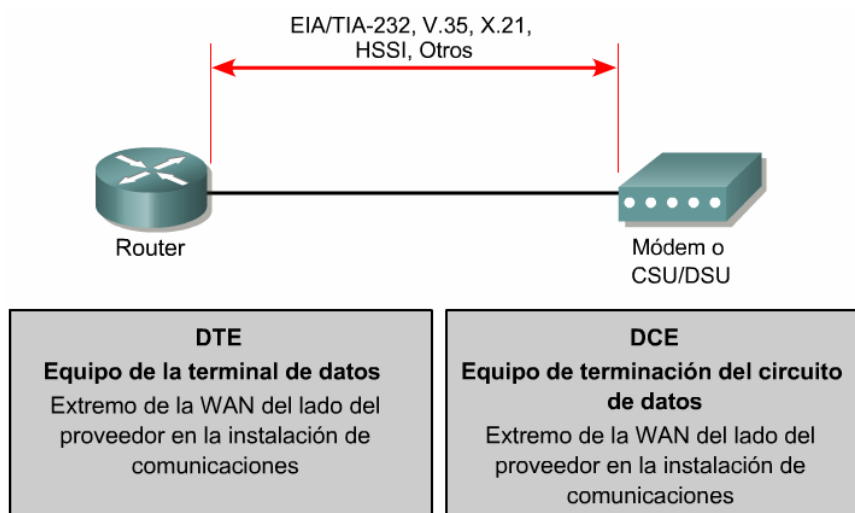


Figura 3

Los protocolos de enlace de datos WAN describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos. 4 Incluyen protocolos diseñados para operar a través de servicios dedicados de conmutación de punto a punto, multipunto y multiacceso, como Frame Relay. Los estándares WAN son definidos y administrados por una serie de autoridades reconocidas, incluyendo las siguientes:

- Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), antiguamente denominado Comité Consultivo Internacional Telegráfico y Telefónico (CCITT)

- Organización Internacional de Normalización (ISO)
- Fuerza de Tareas de Ingeniería de Internet (IETF)
- Asociación de Industrias Electrónicas (EIA)

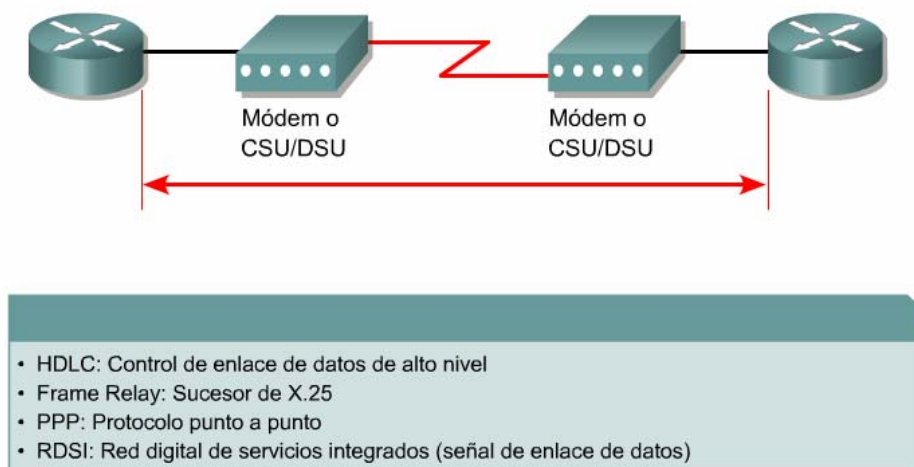


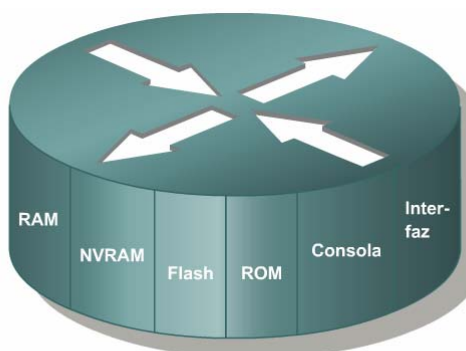
Figura 4

1.1.2 Introducción a los routers de una WAN

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida. Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio. Por ejemplo, los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema operativo de internetworking (IOS) para ejecutar los archivos de configuración. Estos archivos de configuración contienen las instrucciones y los parámetros que controlan el flujo del tráfico entrante y saliente de los routers. Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre cuál es la mejor ruta para los paquetes. El archivo de configuración especifica toda la información necesaria para una correcta configuración y uso de los protocolos enrutados y de enrutamiento seleccionados, o habilitados, en el router.

Este curso mostrará cómo usar los comandos IOS para crear archivos de configuración a fin de que el router ejecute varias funciones de red esenciales. El archivo de configuración del router puede parecer complejo a primera vista, pero, al terminar el curso, no lo parecerá tanto.



Coloque el cursor sobre cada término dentro del router para ver una descripción

Figura 1

Los principales componentes internos del router son la memoria de acceso aleatorio (RAM), la memoria de acceso aleatorio no volátil (NVRAM), la memoria flash, la memoria de sólo lectura (ROM) y las interfaces. ¹ La RAM, también llamada RAM dinámica (DRAM), tiene las siguientes características y funciones:

- Almacena las tablas de enrutamiento.
- Guarda el caché ARP.
- Guarda el caché de conmutación rápida.
- Crea el buffer de los paquetes (RAM compartida).
- Mantiene las colas de espera de los paquetes.
- Brinda una memoria temporal para el archivo de configuración del router mientras está encendido.
- Pierde el contenido cuando se apaga o reinicia el router.

La NVRAM tiene las siguientes características y funciones:

- Almacena el archivo de configuración inicial.
- Retiene el contenido cuando se apaga o reinicia el router.

La memoria flash tiene las siguientes características y funciones:

- Guarda la imagen del sistema operativo (IOS)
- Permite que el software se actualice sin retirar ni reemplazar chips en el procesador.
- Retiene el contenido cuando se apaga o reinicia el router.
- Puede almacenar varias versiones del software IOS.
- Es un tipo de ROM programable, que se puede borrar electrónicamente (EEPROM)

La memoria de sólo lectura (ROM) tiene las siguientes características y funciones:

- Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).
- Guarda el programa bootstrap y el software básico del sistema operativo.
- Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.

Las interfaces tienen las siguientes características y funciones:

- Conectan el router a la red para permitir que las tramas entren y salgan.
- Pueden estar en el motherboard o en un módulo aparte.

1.1.3 Los routers en las LAN y WAN

Aunque se pueda usar un router para segmentar las LAN, su uso fundamental es como dispositivo WAN. ¹ Los routers tienen interfaces LAN y WAN. De hecho, los routers se comunican entre sí por medio de conexiones WAN. ² Los routers son la columna vertebral de las grandes redes internas y de Internet. Operan en la capa 3 del modelo OSI, tomando decisiones basadas en las direcciones de red. Las dos principales funciones de un router son la selección de la mejor ruta para y la conmutación de las tramas hacia la interfaz correspondiente. Los routers logran esto por medio de la creación de tablas de enrutamiento y el intercambio de información de red de estas tablas con otros routers.

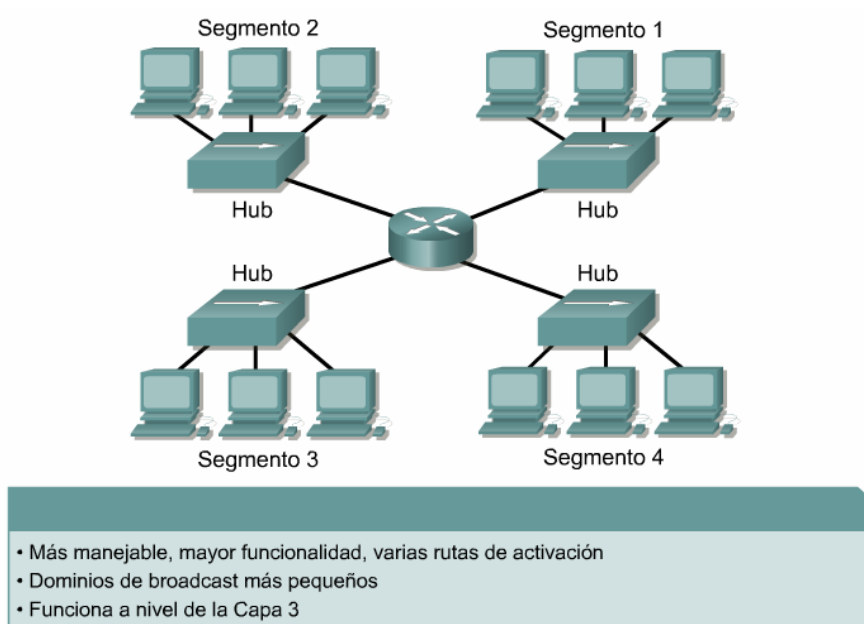


Figura 1

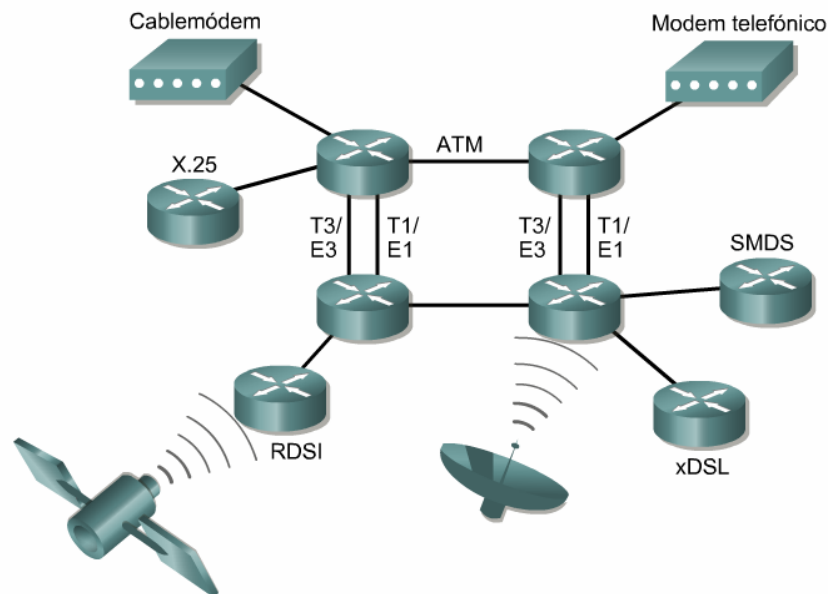


Figura 2

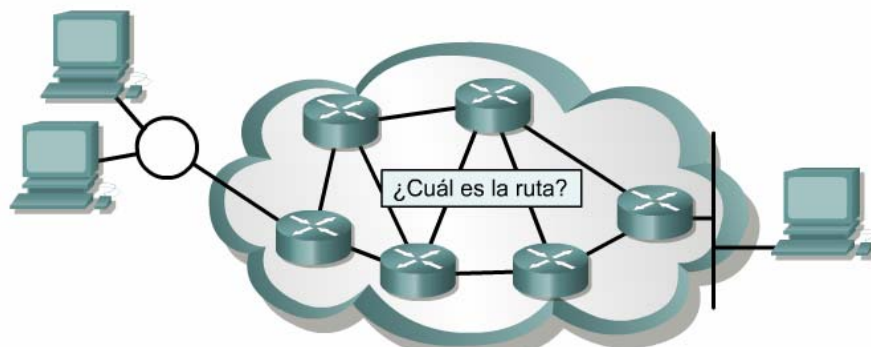


Figura 3

Un administrador puede mantener las tablas de enrutamiento configurando las rutas estáticas, pero, por lo general, las tablas de enrutamiento se mantienen de forma dinámica a través del uso de un protocolo de enrutamiento que intercambia información de la topología (ruta) de red con otros routers.

Si, por ejemplo, un computador (x) necesita comunicarse con un computador (y) en un lugar del mundo y con otro computador (z) en otro lugar lejano, es necesario poder enrutar el flujo de la información y contar con rutas redundantes para asegurar la confiabilidad. 4 Muchas decisiones y tecnologías de diseño de red tienen su origen en el deseo de que los computadores x, y, z puedan comunicarse entre sí.



Figura 4

Una internetwork correctamente configurada brinda lo siguiente:

- Direccionamiento coherente de extremo a extremo
- Direcciones que representan topologías de red

- Selección de la mejor ruta
- Enrutamiento estático o dinámico.
- Conmutación.

1.1.4 La función del router en una WAN

Se dice que una WAN opera en la capa física y en la capa de enlace de datos. Esto no significa que las otras cinco capas del modelo OSI no se hallen en una WAN. Simplemente significa que las características que distinguen una red WAN de una LAN, en general, se encuentran en la capa física y en la capa de enlace de datos. En otras palabras, los estándares y protocolos que se usan en la capa 1 y capa 2 de las WAN son diferentes a aquellas que se utilizan en las mismas capas de las LAN.

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de transmisión de datos (DCE). Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o CSU/DSU. ¹

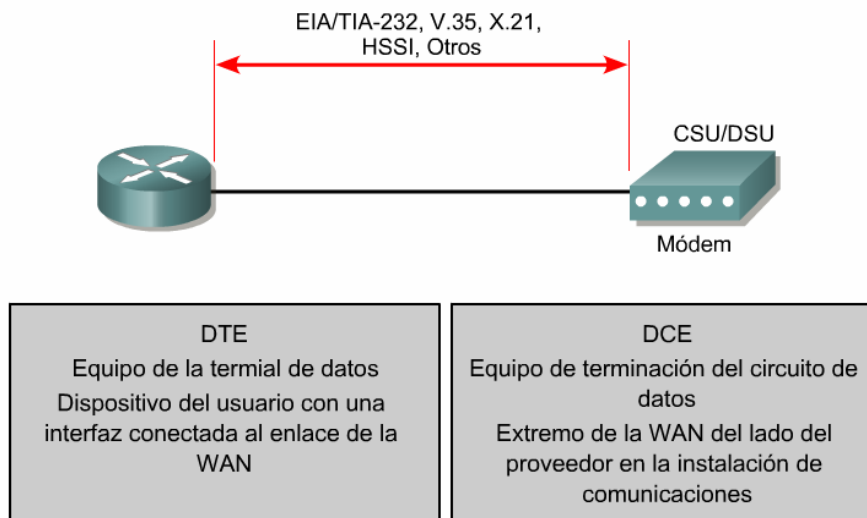


Figura 1

La función principal de un router es enrutar. El enrutamiento se produce en la capa de red, la capa 3, pero si la WAN opera en las capas 1 y 2, ¿un router es un dispositivo LAN o un dispositivo WAN? La respuesta es ambos, como sucede tan a menudo en el campo de las redes y telecomunicaciones. Un router puede ser exclusivamente un dispositivo LAN, o puede ser exclusivamente un dispositivo WAN, pero también puede estar en la frontera entre una LAN y una WAN y ser un dispositivo LAN y WAN al mismo tiempo.

Una de las funciones de un router en una WAN es enrutar los paquetes en la capa 3, pero esta también es la función de un router en una LAN. Por lo tanto, el enrutamiento no es estrictamente una función de un router en la WAN. Cuando un router usa los protocolos y los estándares de la capa de enlace de datos y física asociados con las WAN, opera como dispositivo WAN. Las funciones principales de un router en una WAN, por lo tanto, no yacen en el enrutamiento sino en proporcionar las conexiones con y entre los diversos estándares de enlace de datos y físico WAN. Por ejemplo, un router puede tener una interfaz RDSI que usa encapsulamiento PPP y una interfaz serial que termina en una línea T1 que usa encapsulamiento de Frame Relay. El router debe ser capaz de pasar una corriente de bits desde un tipo de servicio, por ejemplo el RDSI, a otro, como el T1, y cambiar el encapsulamiento de enlace de datos de PPP a Frame Relay.

Muchos de los detalles de los protocolos WAN de Capa 1 y Capa 2 se tratarán más adelante en este curso, pero algunos de los protocolos y estándares WAN clave aparecen en la siguiente lista de referencia.

Los protocolos y estándares de la capa física WAN:

- EIA/TIA -232
- EIA/TIA -449
- V.24
- V.35
- X.21
- G.703

- EIA-530
- RDSI
- T1, T3, E1 y E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

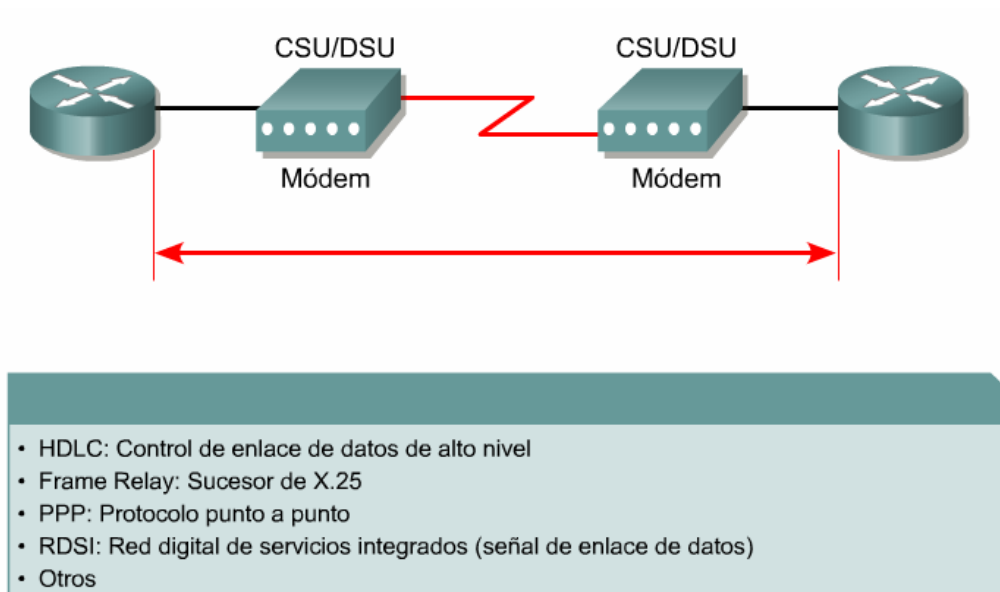


Figura 2

Los protocolos y estándares de la capa de enlace de datos WAN: **2**

- Control de enlace de datos de alto nivel (HDLC)
- Frame Relay
- Protocolo punto a punto (PPP)
- Control de enlace de datos síncrono (SDLC)
- Protocolo Internet de enlace serial (SLIP)
- X.25
- ATM
- LAPB
- LAPD
- LAPF

1.1.5 El enfoque de la Academia en las actividades prácticas

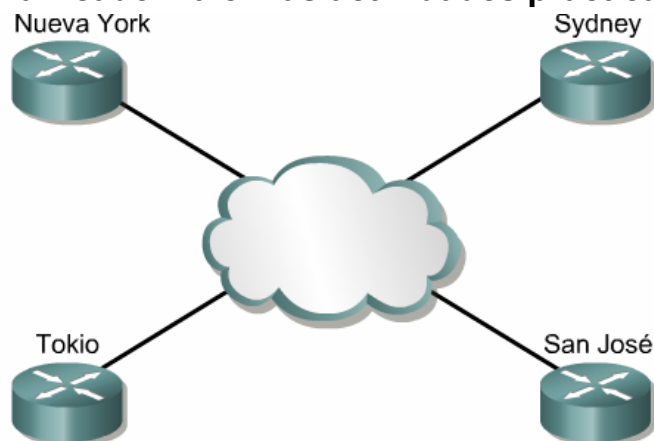
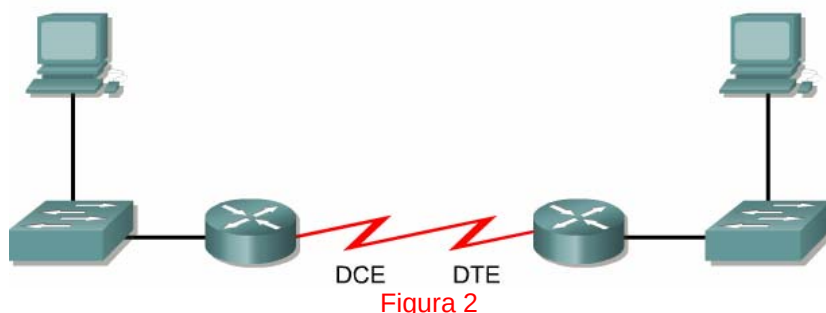


Figura 1

En el laboratorio de la academia, todas las redes estarán conectadas con cables Ethernet o seriales y los estudiantes podrán ver y tocar todo el equipo físicamente. **1**A diferencia de la configuración del laboratorio, en el mundo real, los cables seriales no están conectados de forma consecutiva. En una situación real, un router puede estar en Nueva York mientras que el otro puede estar en Sidney, Australia. Un administrador

en Sidney tendría que conectarse al router de Nueva York a través de la nube WAN a fin de diagnosticar las fallas en el router de Nueva York.

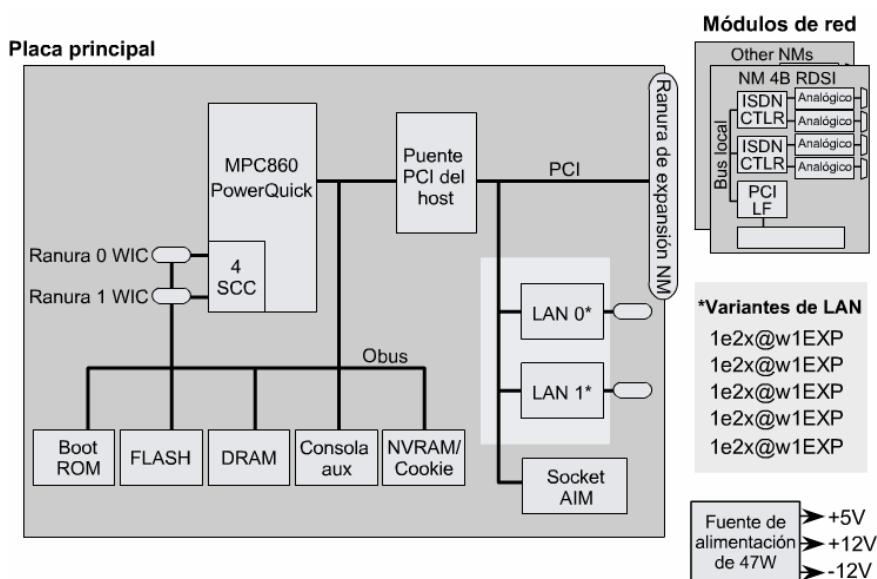
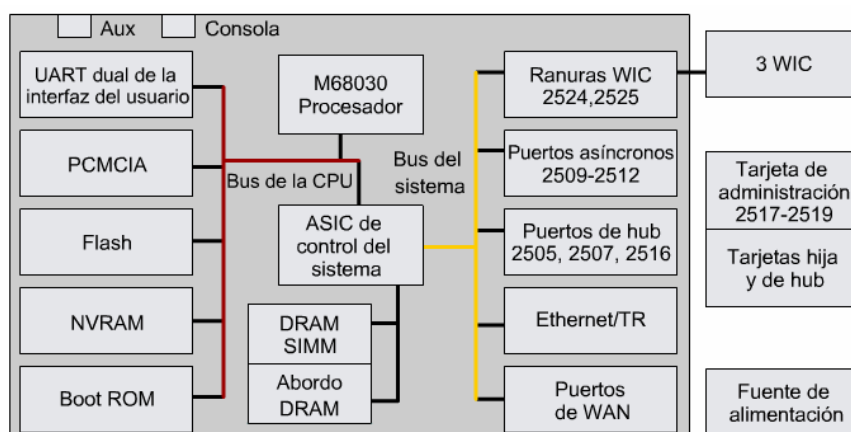
En el laboratorio de la academia, la conexión consecutiva entre los cables DTE-DCE simula los dispositivos que conforman la nube WAN. La conexión desde la interfaz s0/0 de un router a la interfaz s0/1 del otro router simula toda la nube de circuitos.



1.2 Routers

1.2.1 Componentes internos de los routers

Aunque la arquitectura exacta de un router varía de modelo a modelo, esta sección presentará los principales componentes internos. Las Figuras 1 y 2 muestran los componentes internos de algunos de los modelos de routers de Cisco. Los componentes básicos se describen en los siguientes párrafos.



CPU: La unidad central de procesamiento. (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

RAM: La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

Memoria flash: La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

Buses: La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

La CPU usa el bus para tener acceso a los componentes desde el almacenamiento del router. Este bus transfiere las instrucciones y los datos hacia o desde las direcciones de memoria especificadas.

ROM: La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

Interfaces: Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares.

Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares.

Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.

Fuente de alimentación: La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externo al router.

1.2.2 Características físicas de un router

No es necesario conocer la ubicación de los componentes físicos dentro del router para saber cómo utilizarlo. Sin embargo, en algunas situaciones, tales como agregar memoria, puede resultar muy útil.

Los componentes exactos que se utilizan y su ubicación en el router varían de modelo a modelo. La Figura 1 identifica los componentes internos de un router 2600.

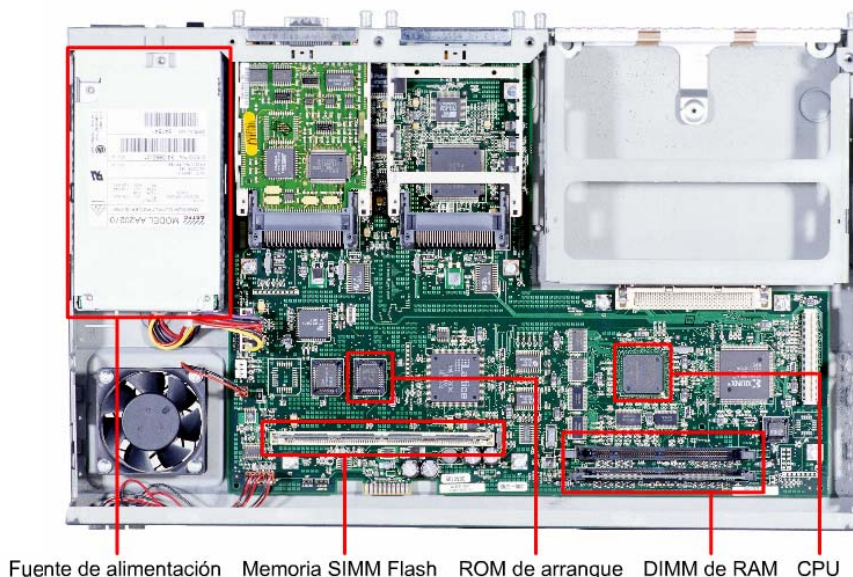


Figura 1

La Figura 2 muestra algunos de los conectores externos de un router 2600.

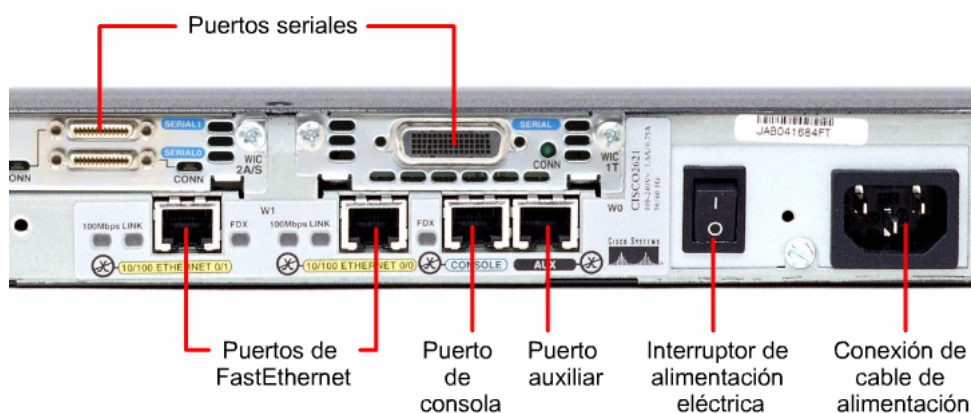
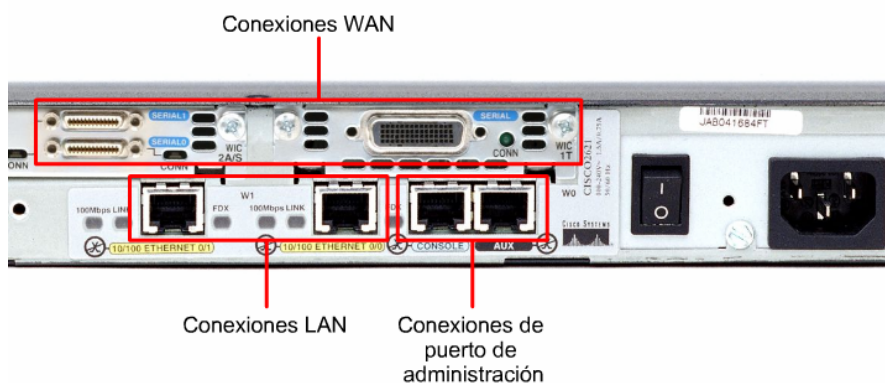


Figura 2

1.2.3 Conexiones externas del router



Los tres tipos de conexiones básicas de un router son las interfaces LAN, las interfaces WAN y los puertos de administración. Las interfaces LAN permiten que el router se conecte a los medios de la Red del área local. Por lo general, esta es una forma de Ethernet. Sin embargo, podría ser alguna otra tecnología LAN, como por ejemplo el Token Ring o FDDI.

Las conexiones WAN proporcionan conexiones a través de un proveedor del servicio a un sitio lejano o a la Internet. Estas pueden ser conexiones seriales o cualquier número de otras interfaces WAN. En algunos tipos de interfaces WAN, se requiere de un dispositivo externo, como por ejemplo una CSU, para conectar el router a la conexión local del proveedor del servicio. En otros tipos de conexiones WAN, el router puede estar conectado directamente al proveedor del servicio.

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son puertos seriales asíncronos EIA-232. Están conectados a un puerto de comunicaciones de un computador. El computador debe ejecutar un programa de emulación de terminal para iniciar la sesión basada en texto con el router. A lo largo de esta sesión, el administrador de la red puede administrar el dispositivo.

1.2.4 Conexiones del puerto de administración

El puerto de consola y el puerto auxiliar (AUX) son puertos de administración. Estos puertos seriales asíncronos no se diseñaron como puertos de networking. Uno de estos dos puertos es necesario para la configuración inicial del router. Se recomienda el puerto de consola para esta configuración inicial. No todos los routers cuentan con un puerto auxiliar.

Cuando el router entra en servicio por primera vez, los parámetros de networking no están configurados. ¹ Por lo tanto, el router no puede comunicarse con ninguna red. Para prepararlo para la puesta en marcha y configuración iniciales, conecte una terminal ASCII RS-232 o un computador que emule una terminal ASCII terminal al puerto de consola del sistema. Entonces, se podrán ingresar los comandos de configuración para poner en marcha el router.

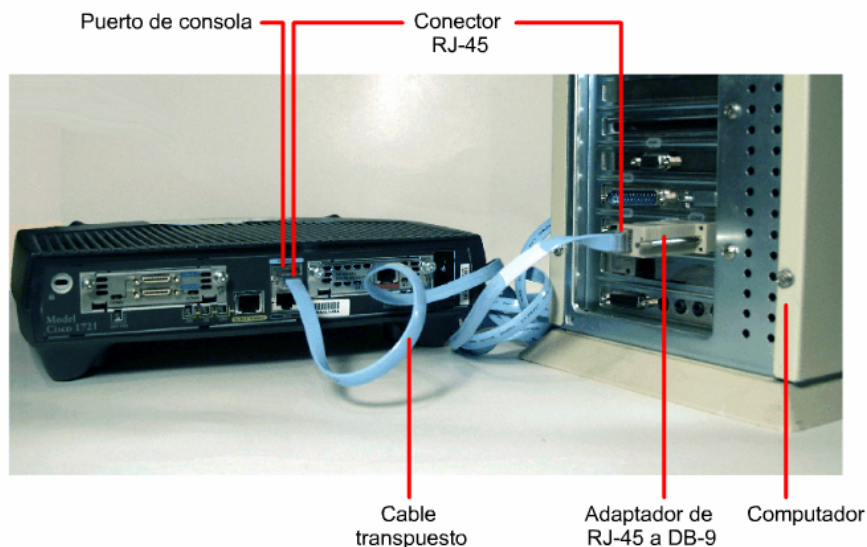


Figura 1

Una vez que la configuración inicial se ha introducido en el router a través del puerto de consola o auxiliar, entonces, se puede conectar el router a la red para realizar un diagnóstico de fallas o monitoreo.

Además, el router puede configurarse desde un lugar remoto haciendo telnet a una línea de terminal virtual o marcando el número de un módem conectado al puerto de consola o auxiliar del router. ²

Se prefiere el puerto de consola al puerto auxiliar para el diagnóstico de fallas también. Esto es porque muestra por defecto la puesta en marcha del router, la depuración y los mensajes de error. El puerto de consola también puede usarse cuando aún no se han iniciado o cuando han fallado los servicios de

networking. Por lo tanto, el puerto de consola se puede usar para los procedimientos de recuperación de contraseñas y de desastre.

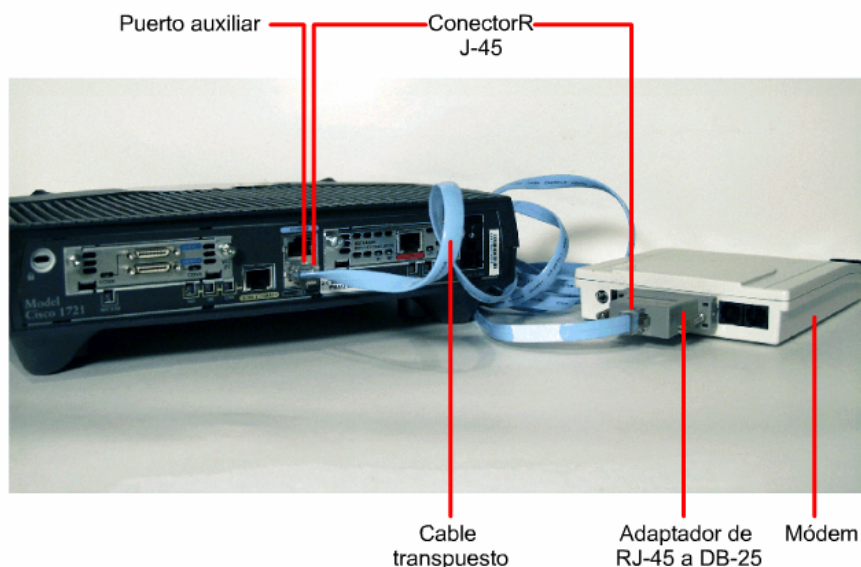


Figura 2

1.2.5 Conexión de las interfaces de consola

El puerto de consola es un puerto de administración que se utiliza para proveer acceso al router fuera de banda. Se usa para la configuración inicial de router, el monitoreo y los procedimientos de recuperación de desastres. ¹

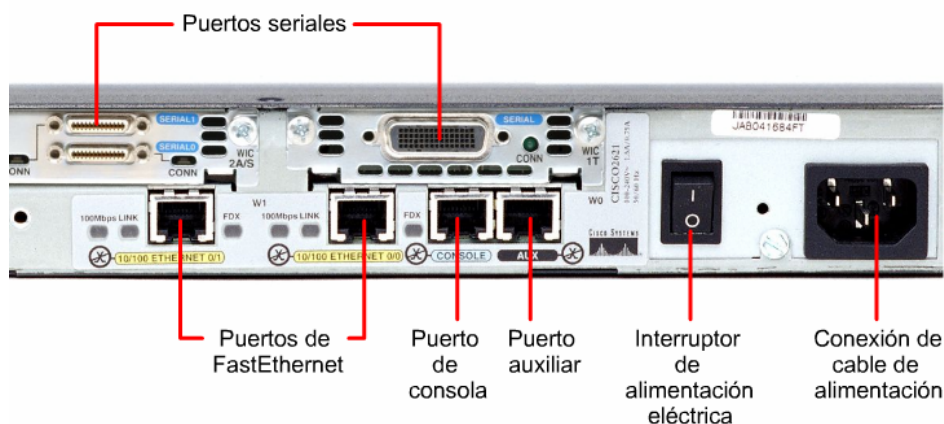


Figura 1

Para realizar la conexión al puerto de consola, se usa un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al PC. Cisco provee el adaptador necesario para realizar la conexión al puerto de consola.

El PC o la terminal deben admitir la emulación de terminal VT100. Un software de emulación de terminal, como el HyperTerminal es el que generalmente se usa.

Para conectar un PC a un router:

1. Configure el software de emulación de terminal en el PC para:
 - El puerto com adecuado
 - 9600 baudios
 - 8 bits de datos
 - Sin paridad
 - 1 bit de parada
 - Sin control de flujo
2. Conecte el conector RJ-45 del cable transpuesto al puerto de consola del router.

3. Conecte el otro extremo del cable transpuesto al adaptador RJ-45 a DB-9.
4. Conecte el adaptador DB-9 hembra al PC.

1.2.6 Conexión de las interfaces LAN

En la mayoría de los entornos LAN, el router se conecta a la red LAN a través de una interfaz de Ethernet o Fast Ethernet. El router es un host que se comunica con la LAN por medio de un hub o de un switch. Se usa un cable de conexión directa para efectuar esta conexión. Una interfaz de router 10/100BaseTX router requiere cable de par trenzado no blindado Categoría 5 o superior (UTP) no obstante el tipo de router. ¹

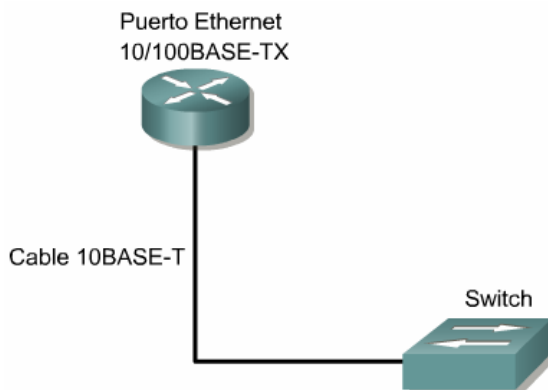


Figura 1

En algunos casos, la conexión Ethernet del router se realiza directamente al computador o a otro router. Para este tipo de conexión, se requiere un cable de conexión cruzada.

Es necesario usar la interfaz correcta. Si se conecta la interfaz incorrecta, es posible que se produzcan daños en el router o en otros dispositivos de networking. Varios tipos de conexiones usan el mismo estilo de conector. Por ejemplo, las interfaces CSU/DSU integradas, AUX, consola, BRI RDSI, Ethernet y Token Ring usan el mismo conector de ocho pins, RJ-45, RJ-48 o RJ-49.

Para ayudar a diferenciar las conexiones del router, Cisco utiliza un esquema de códigos de color para identificar el uso del conector. La Figura ² muestra algunos de los que se usan en un router 2600.

Puerto o conexión	Tipo de puerto	Color	Conectado a	Cable
Ethernet	RJ-45	amarillo	Hub o switch de Ethernet	de conexión directa
WAN T1/E1	RJ-48C/CA81A	verde claro	Red T1 o E1	RJ-48 T1
Consola	8 pins	azul claro	Puerto com del computador	transpuesto
AUX	8 pins	negro	Módem	transpuesto
BRI S/T	RJ-48C/CA81A	anaranjado	Dispositivo NT1 o de intercambio de red integrada privada (PINX)	RJ-48
WAN BRI U	RJ-49C/CA11A	anaranjado	Red RDSI	RJ-49
Token	UTP, STP	violeta	Dispositivo Token Ring	cable RJ-45 Token Ring

Figura 2

1.2.7 Conexión de interfaces WAN

Las conexiones WAN pueden tener un sinnúmero de formas. Una WAN realiza conexiones de datos a través de una amplia área geográfica usando distintos tipos de tecnologías. Generalmente, los proveedores arriendan estos servicios WAN. Entre los tipos de conexión WAN se encuentra los de línea arrendada, de conmutación de circuitos y de conmutación de paquetes. ¹

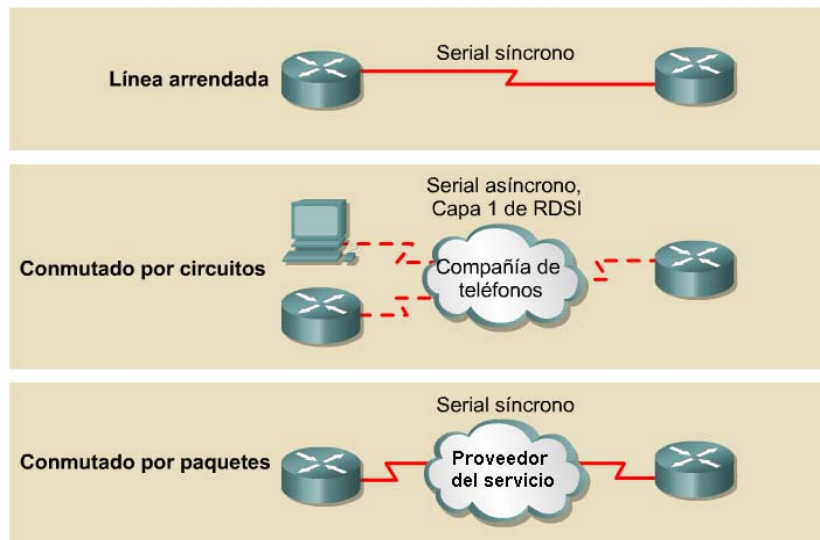


Figura 1

Para cada tipo de servicio WAN, el equipo terminal del abonado (CPE), a menudo un router, es el equipo terminal de datos (DTE). Este se conecta al proveedor del servicio por medio de un dispositivo del equipo de transmisión de datos (DCE), en general, un módem o una unidad de servicio de canal/unidad de servicio de datos (CSU/DSU). Este dispositivo se usa para convertir los datos del DTE a una forma aceptable para el proveedor del servicio WAN.

Tal vez, las interfaces de router que más se usan en los servicios WAN son las interfaces seriales. Seleccionar el cable serial adecuado es tan sencillo como conocer las respuestas a las cuatro siguientes preguntas:

- ¿Qué clase de conexión se hace al dispositivo Cisco? Los routers Cisco pueden usar diferentes conectores para las interfaces seriales. 2 La interfaz de la izquierda es una interfaz serial inteligente. La interfaz de la derecha es una conexión DB-60. Esto hace que la selección del cable serial que conecta el sistema de la red a los dispositivos seriales sea una parte fundamental de la configuración de una WAN.



Figura 2

- ¿Se conecta el sistema de red a un dispositivo de DTE o DCE? El DTE y el DCE son dos tipos de interfaces seriales que los dispositivos usan para comunicarse. La diferencia clave entre los dos es que el dispositivo DCE proporciona la señal reloj para las comunicaciones en el bus. La documentación del dispositivo debe especificar si es DTE o DCE.
- ¿Qué tipo de estándar de señalización requiere el dispositivo? 3 Cada dispositivo podría requerir un estándar serial diferente. Cada estándar define las señales del cable y especifica el conector del extremo del cable. Siempre se debe consultar la documentación del dispositivo para obtener información sobre el estándar de señalización.

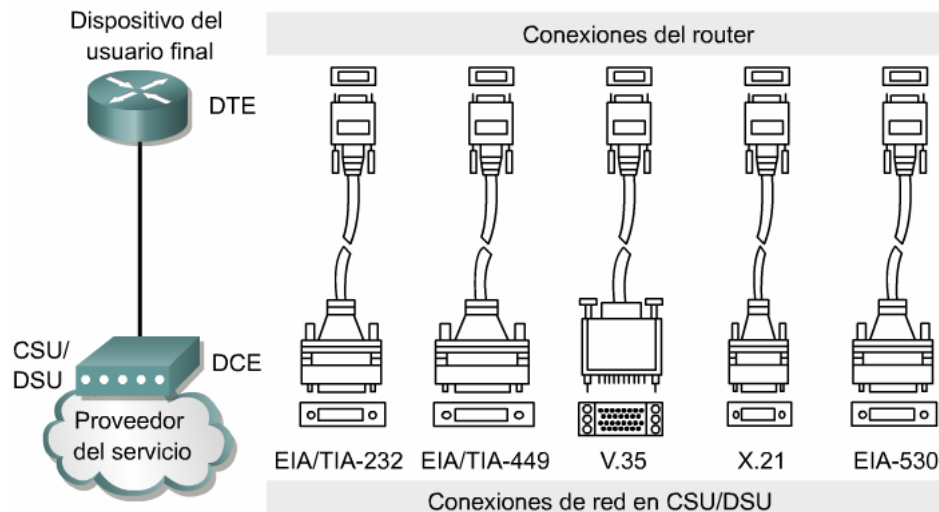


Figura 3

- ¿El cable requiere un conector macho o hembra? Si el conector tiene pins salientes visibles, es macho. Si el conector tiene tomas para los pins salientes, es hembra.

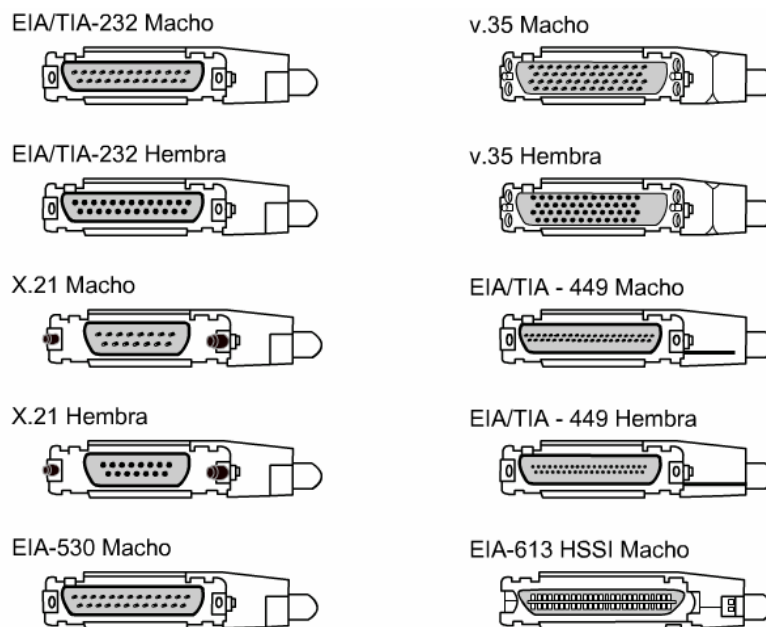


Figura 4

Resumen

Se debe haber logrado una comprensión de los siguientes puntos clave:

- Conceptos de las redes WAN y LAN
- La función de un router en las redes WAN y LAN
- Los protocolos de redes WAN
- La configuración del encapsulamiento
- La identificación y descripción de los componentes internos de un router
- Las características físicas de un router
- Los puertos comunes de un router
- Cómo hacer una conexión en los puertos WAN, LAN y de consola de un router

Módulo 2: Introducción a los routers

Descripción general

La tecnología de Cisco se basa en el sistema operativo de internetworking de Cisco (IOS), que es el software que controla las funciones de enrutamiento y conmutación de los dispositivos de red. Es esencial que el administrador de red cuente con una sólida comprensión acerca del IOS. Este módulo presenta una introducción de los fundamentos del IOS y provee ejercicios de familiarización con las características resaltantes del IOS. Todas las tareas de configuración de red, desde las más básicas hasta las más complejas, requieren un conocimiento sólido de los fundamentos básicos de la configuración del router. Este módulo brinda las herramientas y las técnicas para la configuración básica del router, las cuales se usarán a lo largo de todo el curso.

Los estudiantes que completen este módulo deberán ser capaces de:

- Describir las funciones del IOS
- Describir el funcionamiento básico del IOS
- Identificar algunas características resaltantes del IOS
- Identificar los métodos para establecer una sesión de interfaz de línea de comando (CLI) con el router.
- Pasar del modo de usuario ejecutivo (EXEC) al EXEC privilegiado y viceversa.
- Establecer una sesión de HyperTerminal con un router
- Iniciar una sesión con un router
- Usar la función de ayuda en la interfaz de línea de comando
- Diagnosticar errores de comando

2.1 Operación del software Cisco IOS

2.1.1 Funciones del software Cisco IOS

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

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

2.1.2 Interfaz de usuario del router

El software Cisco IOS usa una interfaz de línea de comando (CLI) como entorno de consola tradicional. El IOS es tecnología modular de Cisco, y está presente en casi todos sus productos. Sus detalles de operación pueden variar según los distintos dispositivos de red.

Se puede acceder a este entorno a través de varios métodos. Una de las formas de acceder a la CLI es a través de una sesión de consola. La consola usa una conexión serial directa, de baja velocidad, desde un computador o terminal a la conexión de consola del router. Otra manera de iniciar una sesión de CLI es mediante una conexión de acceso telefónico, con un módem o módem nulo conectado al puerto AUX del router. Ninguno de estos métodos requiere que el router tenga configurado algún servicio de red. Otro de los métodos para iniciar una sesión de CLI es establecer una conexión Telnet con el router. Para establecer una sesión Telnet al router, se debe configurar por lo menos una interfaz con una dirección IP, y configurar las conexiones y contraseñas de las sesiones de terminal virtual.

2.1.3 Modos de interfaz de usuario

La interfaz de línea de comando (CLI) de Cisco usa una estructura jerárquica. Esta estructura requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice, tendrá efecto únicamente en esa interfaz en particular. Al ingresar a cada uno de estos modos específicos, la petición de entrada del router cambia para señalar el modo de configuración en uso y sólo acepta los comandos que son adecuados para ese modo.

El IOS suministra un servicio de intérprete de comandos, denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y ejecuta.

Modo EXEC	Símbolo	Usos típicos
Usuario	GAD>	verificar el estado del router
Privilegiado	GAD#	acceso al router modos de configuración

Figura 1

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso. Estos niveles son el modo EXEC usuario y el modo EXEC privilegiado. El modo EXEC privilegiado también se denomina el modo enable. Las siguientes son las características resaltantes del modo EXEC usuario y del modo EXEC privilegiado:

- El modo EXEC usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo "de visualización solamente". El nivel EXEC usuario no permite ningún comando que pueda cambiar la configuración del router. El modo EXEC usuario se puede reconocer por la petición de entrada: ">". ¹
- El modo EXEC privilegiado da acceso a todos los comandos del router. Se puede configurar este modo para que solicite una contraseña del usuario antes de dar acceso. Para mayor protección, también se puede configurar para que solicite una ID de usuario. Esto permite que sólo los usuarios autorizados puedan ingresar al router. Los comandos de configuración y administración requieren que el administrador de red se encuentre en el nivel EXEC privilegiado. Para ingresar al modo de configuración global y a todos los demás modos específicos, es necesario encontrarse en el modo EXEC privilegiado. El modo EXEC privilegiado se puede reconocer por la petición de entrada "#".

Para ingresar al nivel EXEC privilegiado desde el nivel EXEC usuario, ejecute el comando **enable** con la petición de entrada ">" en pantalla. ² Si se ha configurado una contraseña, el router solicitará la contraseña. Por razones de seguridad, los dispositivos de red de Cisco no muestran la contraseña al ser introducida. Una vez que se ha introducido la contraseña correcta, la petición de entrada del router cambia a "#", lo que indica que el usuario se encuentra ahora en el nivel EXEC privilegiado. Si se introduce un signo de interrogación (?) en el nivel EXEC privilegiado, se mostrarán muchas opciones de comando, adicionales a las disponibles en el nivel EXEC usuario.

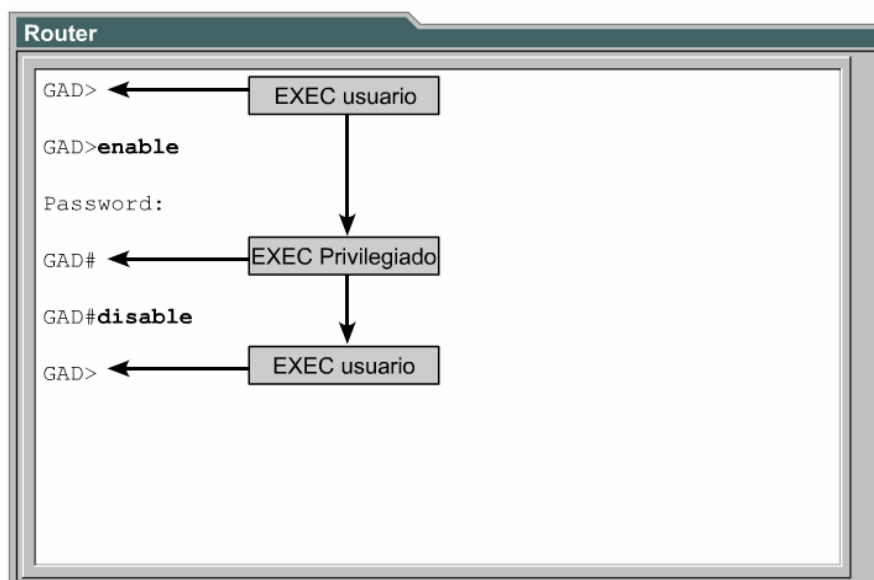


Figura 2

2.1.4 Características resaltantes del software Cisco IOS

Cisco suministra imágenes de su IOS para muchos dispositivos, que abarcan una amplia gama de plataformas de productos de red.

Para adecuar óptimamente el software Cisco IOS que requieren dichas plataformas, Cisco trabaja en el desarrollo de muchas y variadas imágenes del software Cisco IOS. Cada imagen provee una funcionalidad distinta, adecuada a las diversas plataformas de dispositivos, los recursos de memoria disponibles y las necesidades de los clientes.

Aunque existen diversas imágenes del IOS para cada modelo y funcionalidad de los dispositivos de Cisco, la estructura básica de los comandos de configuración es la misma. Las destrezas de configuración y diagnóstico de fallas que se adquieren en cualquiera de los dispositivos, son útiles en una amplia gama de productos.

El nombre tiene tres partes, separadas por guiones: Por ej.: xxxx-yyyy-ww:

- xxxx = Plataforma
- yyyy = Características
- ww = Formato: desde donde se ejecuta si está comprimido

Figura 1

El esquema de denominación de las distintas versiones del software Cisco IOS consta de tres partes: **1**

- La plataforma en la que se ejecuta la imagen.
- Las características especiales que permite la imagen.
- El lugar donde se ejecuta la imagen y si la imagen ha sido comprimida en formato zip.

Las características específicas del IOS se pueden seleccionar mediante el Cisco Software Advisor. El Cisco Software Advisor es una herramienta interactiva que suministra la información más actualizada y permite la selección de opciones que satisfagan los requisitos de la red.

Una de las consideraciones principales al momento de seleccionar una nueva imagen del IOS, es la compatibilidad con las memorias flash y RAM del router. En general, cuanto más reciente sea la versión y cuantas más características brinde, mayor será la cantidad de memoria que se requiera. Utilice el comando **show version** del dispositivo de Cisco para verificar cuál es la imagen en uso y la memoria flash disponible. Las páginas WWW de apoyo técnico de Cisco ofrecen herramientas para ayudar a determinar la cantidad de memoria flash y de memoria RAM que se requiere para cada imagen.

Antes de instalar una nueva imagen del software Cisco IOS en el router, verifique si el router cumple con los requisitos de memoria de dicha imagen. Para ver la cantidad de memoria RAM, ejecute el comando **show version**:

...<resultado omitido>...

cisco 1721 (68380) processor (revision C) with 3584K/512K bytes of memory.

Esta línea indica la cantidad de memoria principal y compartida instalada en el router. Algunas plataformas usan una parte de la DRAM como memoria compartida. Los requisitos de memoria toman esto en cuenta, de modo que ambos números deben sumarse para conocer la cantidad de DRAM instalada en el router.

Para conocer la cantidad de memoria flash, ejecute el comando **show flash**:

GAD#**show flash**

...<resultado omitido>...

15998976 bytes total (10889728 bytes free)

2.1.5 Operación del software Cisco IOS

Entorno operativo	Símbolo	Uso
Monitor de la ROM	> or ROMMON>	Falla o recuperación de contraseña
ROM de arranque	Router (boot) >	Actualización de la imagen de Flash
Cisco IOS	Router>	Operación normal

Figura 1

Los dispositivos que usan el Cisco IOS tienen tres entornos o modos de operación distintos: **1**

- Monitor de la ROM
- ROM de arranque
- Cisco IOS

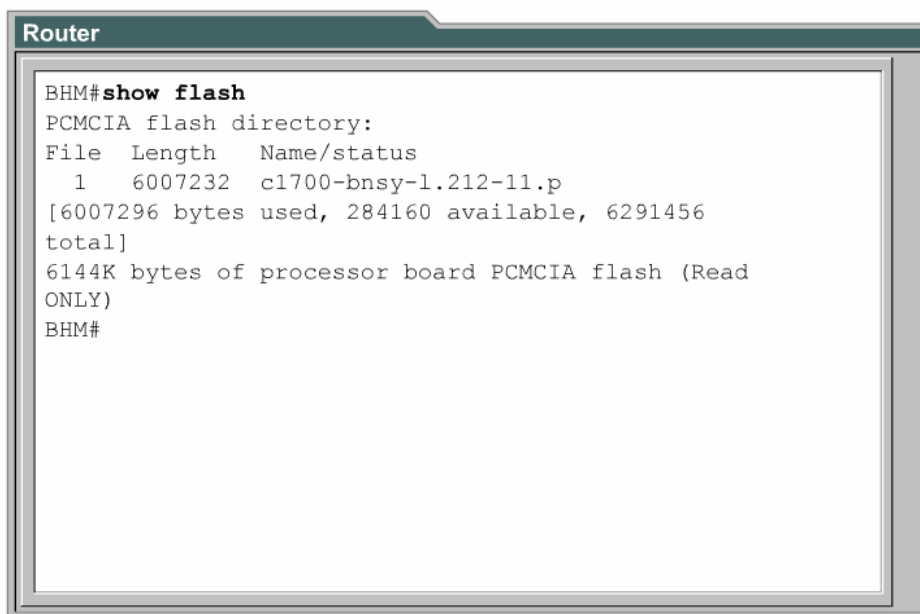
Los comandos de inicio del router generalmente se cargan en la RAM y ellos activan uno de estos entornos de operación. El registro de configuración puede ser utilizado por el administrador del sistema para controlar el modo de inicio por defecto del router.

El monitor de la ROM ejecuta el proceso de bootstrap y provee funcionalidad y diagnósticos de bajo nivel. Se usa para la reactivación luego de una falla del sistema y para recuperar una contraseña perdida. No es posible ingresar al monitor de la ROM mediante alguna de las interfaces de red. Sólo se puede ingresar a él mediante una conexión física directa en el puerto de la consola.

Cuando el router opera en modo ROM de arranque, sólo está disponible un subconjunto limitado de la funcionalidad del Cisco IOS. La ROM de arranque permite las operaciones de escritura en la memoria flash y se usa principalmente para reemplazar la imagen del software Cisco IOS que se guarda en la memoria flash. La imagen del software Cisco IOS se puede modificar en la ROM de arranque mediante el comando **copy tftp flash**, el cual copia una imagen del Cisco IOS almacenada en un servidor TFTP, en la memoria flash del router.

El funcionamiento normal de un router requiere el uso de la imagen completa del software Cisco IOS tal como se guarda en la memoria flash. En algunos dispositivos, el IOS se ejecuta directamente desde la memoria flash. Sin embargo, la mayoría de los routers Cisco requieren que se cargue una copia del IOS en la RAM, y también se ejecuta desde la RAM. Algunas imágenes del IOS se guardan en la memoria flash en un formato comprimido y se deben expandir al cargarse en la RAM.

Para ver la imagen y la versión del IOS en uso, use el comando **show version**, el cual muestra también el registro de configuración. El comando **show flash** se usa para verificar si el sistema tiene la memoria suficiente para cargar una nueva imagen del software Cisco IOS. [2](#)



```
BHM#show flash
PCMCIA flash directory:
File Length Name/status
  1  6007232 c1700-bnsy-1.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

Figura 2

2.2 Activación de un router

2.2.1 Puesta en marcha inicial de los routers Cisco

Un router se activa con la ejecución de tres elementos: el bootstrap, el sistema operativo y un archivo de configuración. Si el router no puede encontrar un archivo de configuración, entra en el modo de configuración inicial (setup). Una vez que el modo de configuración inicial se ha completado, se puede guardar una copia de respaldo del archivo de configuración en la RAM no volátil (NVRAM).

El objetivo de las rutinas de inicio del software Cisco IOS es iniciar la operación del router. Para ello, las rutinas de inicio deben:

- Asegurarse de que el hardware del router esté en perfectas condiciones y funcional.
- Encontrar y cargar el software Cisco IOS.
- Encontrar y aplicar el archivo de configuración inicial o entrar al modo de configuración inicial (setup).

Cuando se activa un router Cisco, éste realiza una autocomprobación de encendido (POST). Durante esta comprobación, el router ejecuta diagnósticos desde la ROM a todos los módulos de hardware. Estos diagnósticos verifican la operación básica de la CPU, la memoria y los puertos de interfaz de red. Después de verificar las funciones de hardware, el router procede a inicializar el software.

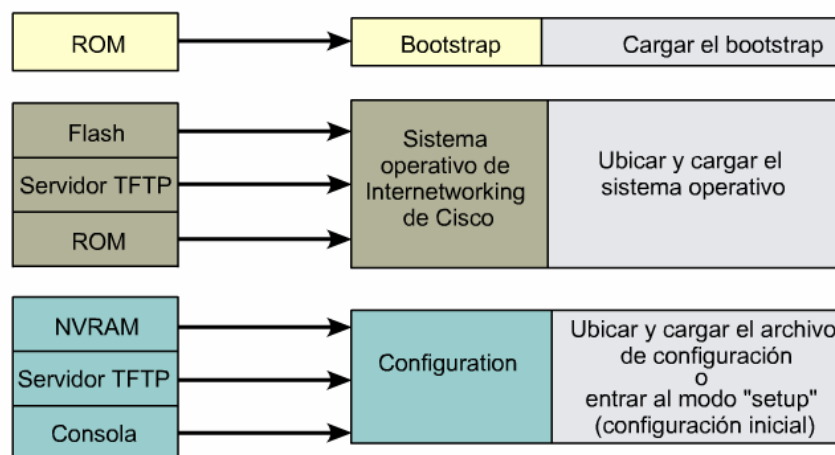


Figura 1

Después de la POST, se producen los siguientes eventos a medida que se inicializa el router: **1**

Paso 1 Se ejecuta el cargador genérico de bootstrap, que se encuentra en la ROM. Un bootstrap es un conjunto de instrucciones sencillo que comprueba el hardware e inicializa el IOS para el funcionamiento.

Paso 2 El IOS puede estar en diversos lugares. El registro de arranque de la configuración indica la ubicación que se debe utilizar para cargar el IOS. Si el registro de arranque indica que se debe cargar de una flash, o de la red, los comandos del sistema de arranque en el archivo de configuración señalan el nombre y la ubicación exacta de la imagen.

Paso 3 Se carga la imagen del sistema operativo. Cuando el IOS está cargado y funcionando, se muestra en pantalla del terminal de consola una lista de los componentes de hardware y software disponibles.

Paso 4 El archivo de configuración guardado en la NVRAM se carga en la memoria principal y se ejecuta línea por línea. Los comandos de configuración inician los procesos de enrutamiento, proporcionan las direcciones para las interfaces y definen otras características operativas del router.

Paso 5 Si no existe ningún archivo de configuración válido en la NVRAM, el sistema operativo busca un servidor TFTP disponible. Si no se encuentra ningún servidor TFTP, se inicia el diálogo de configuración inicial (setup).

El modo de configuración inicial no debe ser el utilizado para configurar funciones complejas de protocolo en el router. El propósito del modo de configuración inicial es permitir que el administrador instale una configuración mínima en un router que no pueda ubicar una configuración de otra fuente.

En el modo de configuración inicial, las respuestas por defecto aparecen entre corchetes **[]** a continuación de la pregunta. **2** Presione la tecla **Intro** para usar esos valores por defecto. Durante el proceso de configuración inicial, se puede presionar **Control-C** en cualquier momento para interrumpir el proceso. Al interrumpir la configuración inicial mediante **Control-C**, todas las interfaces quedan administrativamente inhabilitadas (shutdown).

```

Router
#setup

--System Configuration Dialog--
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Continue with configuration dialog? [yes].

First, would you like to see the current interface summary?
[yes]

Interface    IP-Address    OK?    Method    Status    Protocol
TokenRing0   unassigned    NO     not set   down      down
Ethernet0    unassigned    NO     not set   down      down
Serial0      unassigned    NO     not set   down      down
Fddi0       unassigned    NO     not set   down      down

```

Figura 2

Una vez que se ha completado el proceso de configuración en modo de configuración inicial, se muestran las siguientes opciones:

[0] Go to the IOS command prompt without saving this config. (Regresar a la petición de entrada de comandos del IOS sin guardar esta configuración).

[1] Return back to the setup without saving this config. (Regresar a la configuración inicial y no guardar esta configuración).

[2] Save this configuration to nvram and exit. (Guardar esta configuración en la NVRAM y salir).

Enter your selection [2] (Indique su selección):

2.2.2 Indicadores LED del router

Los routers Cisco usan indicadores LED para proporcionar información de estado. Los indicadores LED varían según el modelo del router Cisco.

Un LED de interfaz indica la actividad de la interfaz correspondiente. Si un LED está apagado cuando la interfaz está activa y la interfaz está conectada correctamente, puede ser señal de un problema. Si la interfaz está en gran actividad, el LED estará continuamente encendido. El LED OK verde a la derecha del puerto AUX se enciende luego de que el sistema se ha inicializado correctamente. **1**

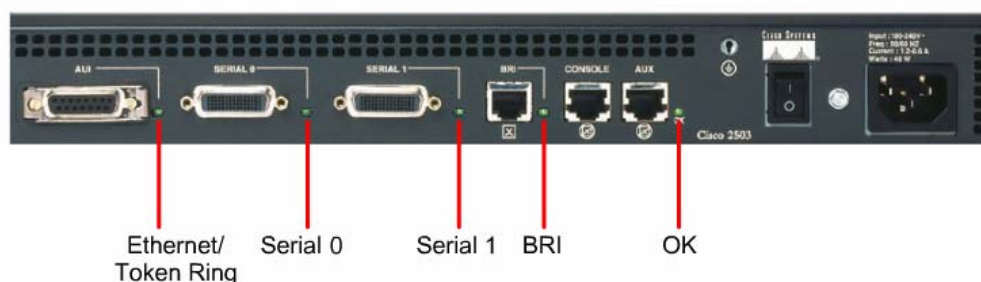


Figura 1

2.2.3 Examen del arranque inicial del router

Los ejemplos de las Figuras **1**– **3** muestran la información y los mensajes que se muestran durante el arranque inicial. Esta información varía, según las interfaces del router y la versión del software Cisco IOS. Las pantallas que se muestran en este gráfico son sólo de referencia y podrían no reflejar exactamente lo que la pantalla muestra en la consola.

En la Figura **1**, la frase "NVRAM invalid, possibly due to write erase" (NVRAM no válida, posiblemente por haber sido borrada), le indica al usuario que este router todavía no se ha configurado o que la NVRAM ha sido borrada. El router se debe configurar, el archivo de configuración se debe guardar en la NVRAM y

luego se le debe configurar para que use el archivo de configuración en la NVRAM. El valor preconfigurado de fábrica del registro de inicio es 0x2102, el cual indica que el router debe intentar cargar una imagen del software Cisco IOS desde la memoria flash.

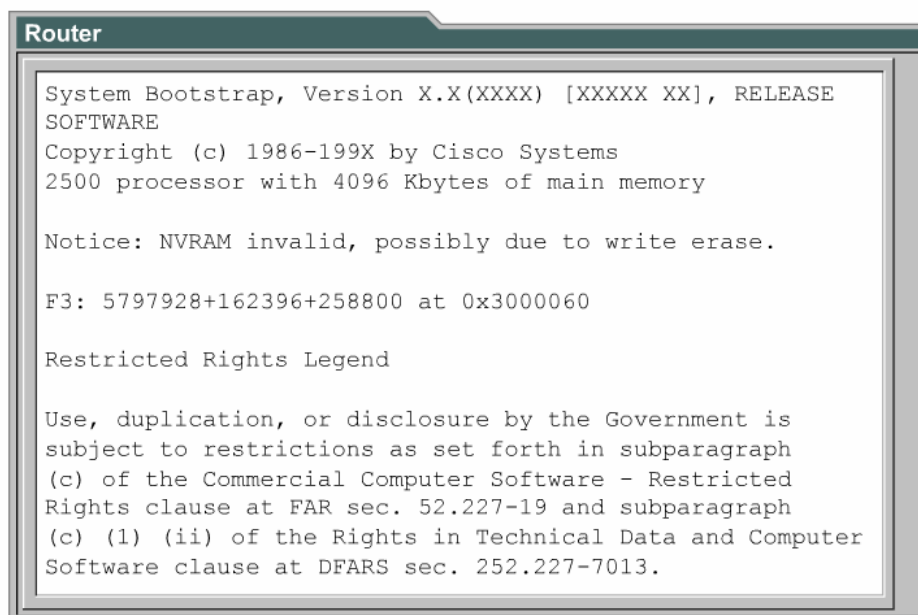


Figura 1

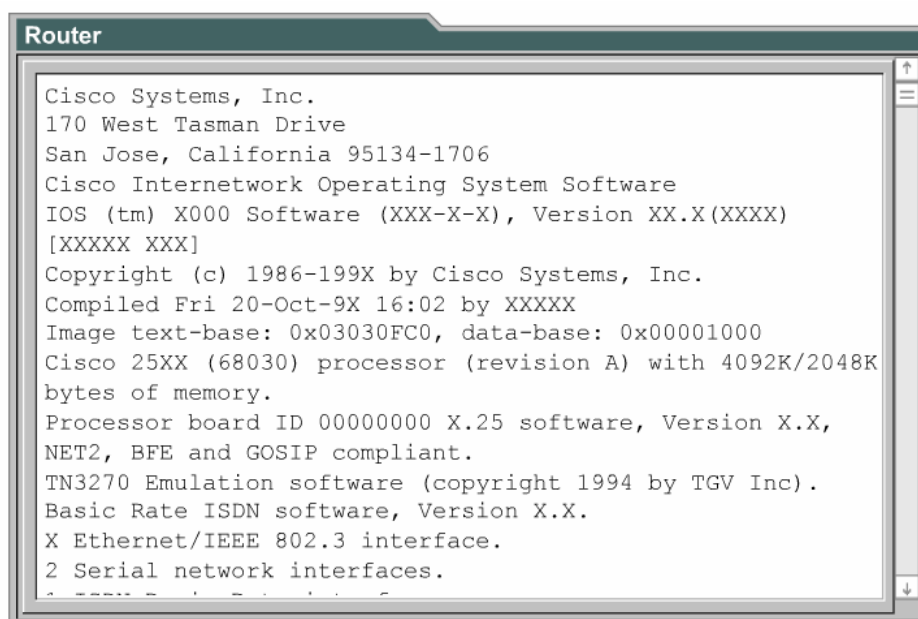


Figura 2

En la Figura 2, el usuario puede determinar la versión del bootstrap y la versión del IOS en uso en el router, así como también el modelo, el procesador y la cantidad de memoria que contiene el router. Otra información suministrada en este gráfico incluye:

- El número de interfaces
- Los tipos de interfaces
- La cantidad de NVRAM
- La cantidad de memoria flash

En la Figura 3, el usuario se le presenta la opción de ingresar al modo de configuración inicial. Recuerde que el propósito primordial del modo de configuración inicial es permitir que el administrador instale una configuración mínima en un router que no pueda ubicar una configuración de otra fuente.

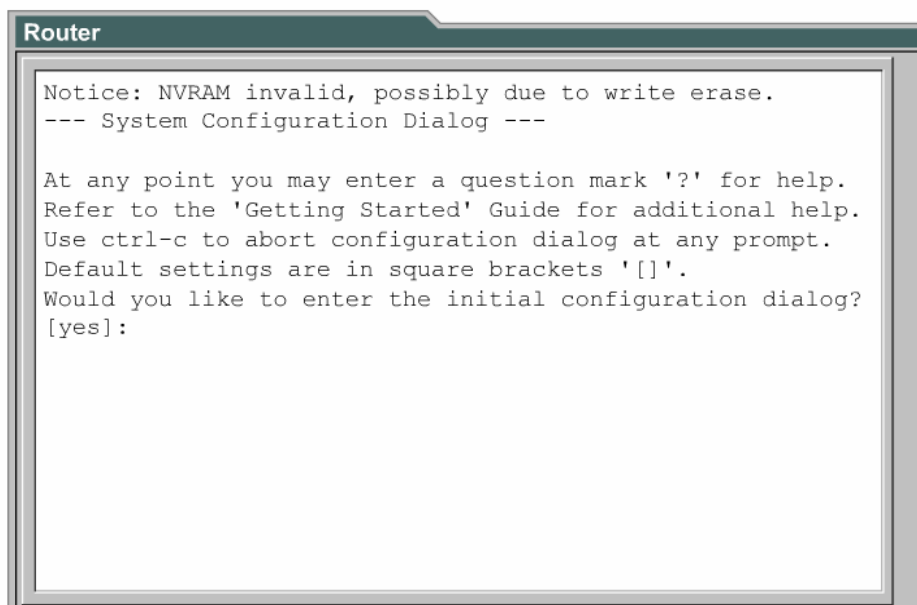


Figura 3

2.2.4 Establecimiento de una sesión de HyperTerminal

Todos los routers Cisco incluyen un puerto de consola serial asíncrono TIA/EIA-232 (RJ-45). Se requiere cables y adaptadores para conectar una terminal de consola al puerto de consola. Una terminal de consola es una terminal ASCII o un PC que ejecuta un software de emulación de terminal como, por ejemplo, HyperTerminal. Para conectar un PC que ejecuta un software de emulación de terminal al puerto de consola, use un cable transpuesto RJ-45 a RJ-45 con un adaptador hembra RJ-45 a DB-9.

Los parámetros por defecto para el puerto de consola son 9600 baudios, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo en hardware. El puerto de consola no permite control de flujo en hardware.

Siga los pasos a continuación para conectar una terminal al puerto de consola del router:

Paso 1 Conecte la terminal mediante un cable transpuesto RJ-45 a RJ-45 y un adaptador RJ-45 a DB-9 o RJ-45 a DB-25. **1**

Adaptador de
RJ-45 a DB-9

Figura 1

Paso 2 Configure la terminal o el software de emulación de terminal del PC para 9600 baudios, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo en hardware.

La Figura **2** muestra una lista de los sistemas operativos y los softwares de emulación de terminal que se pueden utilizar.

Sistema operativo del PC	Software
Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me	HyperTerminal (incluido con el software de Windows), ProComm Plus
Windows 3.1	Terminal (incluido con el software de Windows)
Macintosh	ProComm, VersaTerm, ZTerm (suministrados aparte)
Unix/Linux	Minicom

Figura 2

2.2.5 Inicio de sesión en el router

Para configurar los routers Cisco, se debe ingresar a la interfaz de usuario del router mediante una terminal o un acceso remoto. Al ingresar a un router, el usuario debe iniciar una sesión antes de ejecutar cualquier otro comando.

Por razones de seguridad, el router tiene dos niveles de acceso a los comandos:

- **Modo EXEC usuario:** Las tareas típicas incluyen la verificación del estado del router. En este modo no se permiten cambios en la configuración del router.
- **Modo EXEC privilegiado:** Las tareas típicas incluyen cambios a la configuración del router.

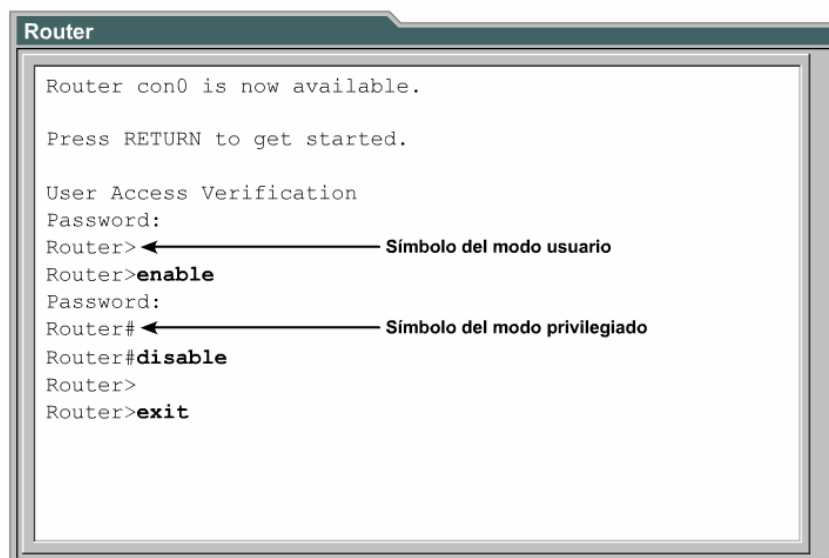


Figura 1

La petición de entrada de modo EXEC usuario se muestra al iniciar la sesión con el router. ¹ Los comandos disponibles en este nivel de usuario son un subconjunto de los comandos disponibles en el nivel EXEC privilegiado. En su mayor parte, estos comandos permiten que el usuario vea la información, sin cambiar la configuración del router.

Para acceder al conjunto completo de comandos, se debe ingresar al modo EXEC privilegiado. En la petición de entrada ">" escriba **enable** (Habilitar). En la petición de entrada **password:** (contraseña), escriba la contraseña que se ha establecido con el comando **enable secret**. Se puede usar dos comandos para establecer una contraseña de acceso al modo EXEC privilegiado: **enable password** y **enable secret**. Si se usan ambos comandos, el comando **enable secret** tiene precedencia. Una vez que se han completado los pasos para iniciar la sesión, la petición de entrada cambia a "#", para señalar que se ha ingresado al modo EXEC privilegiado. Sólo se puede ingresar al modo de configuración global desde el modo EXEC privilegiado. Los siguientes son modos específicos a los que también se puede ingresar desde el modo de configuración global:

- Interfaces
- Subinterfaces
- Línea
- Router
- Mapas de enrutamiento

Para regresar al modo EXEC usuario desde el modo EXEC privilegiado, se pueden ejecutar los comandos **disable** o **exit**. Para regresar al modo EXEC privilegiado desde el modo de configuración global, ejecute **exit** o **Control-Z**. Control-Z también se puede usar para regresar directamente al modo EXEC privilegiado desde cualquier modo de configuración global secundario.

2.2.6 Ayuda mediante el teclado en la interfaz de línea de comando

Al escribir un signo de interrogación (?) en la petición de entrada del modo usuario o del modo privilegiado, aparece una útil lista de los comandos disponibles. ¹Observe el "--More--" (Más) que aparece en la parte inferior de la pantalla de muestra. La pantalla muestra varias líneas a la vez. La petición de entrada "--More--" que aparece en la parte inferior de la pantalla indica que hay más pantallas disponibles. Siempre que aparezca una petición de entrada "--More--", la siguiente pantalla disponible se puede visualizar presionando la barra espaciadora. Para visualizar sólo la siguiente línea, presione la tecla **Return** o **Intro**. Presione cualquier tecla para regresar a la petición de entrada. ¹

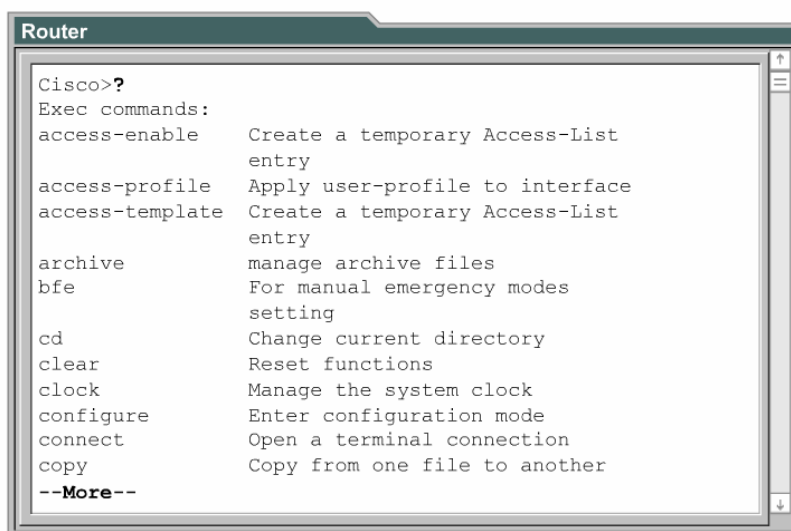


Figura 1

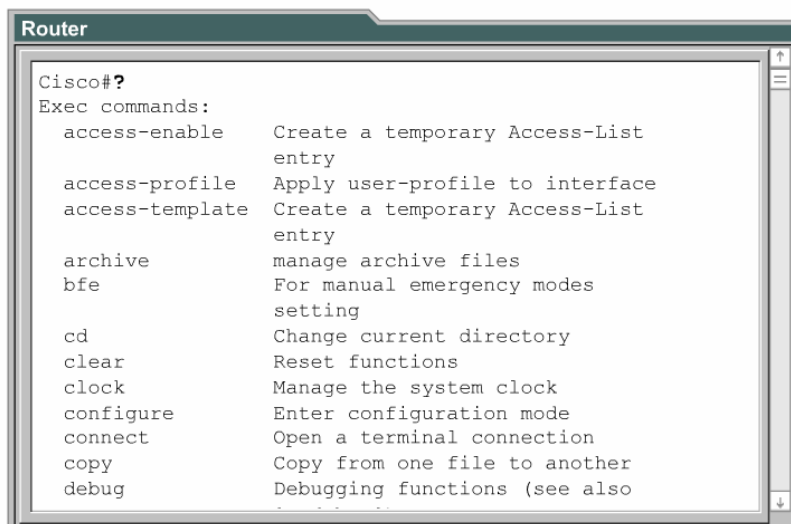
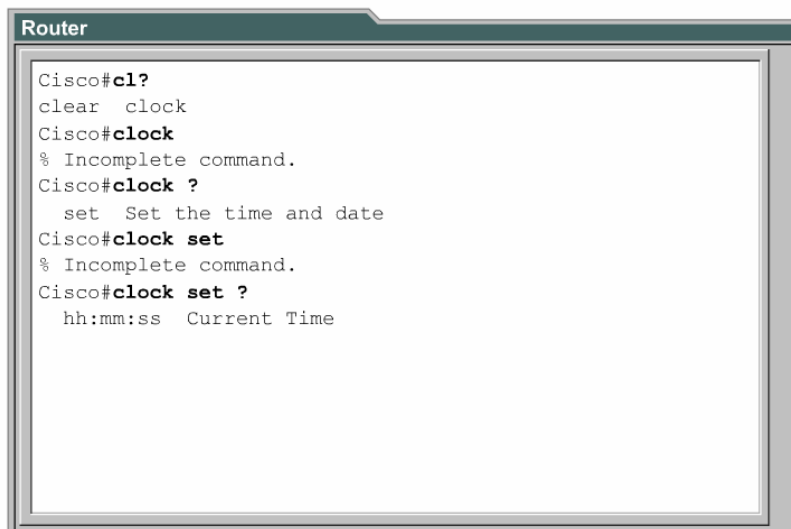


Figura 2

Para ingresar al modo EXEC privilegiado, escriba **enable** o su abreviatura **ena**. Esto puede hacer que el router pida al usuario una contraseña, que se haya fijado con anterioridad. Si se escribe un "?" (signo de interrogación) cuando se muestra la petición de entrada del modo EXEC privilegiado, la pantalla mostrará una lista de comandos más larga que la se obtiene cuando se muestra la petición de entrada del modo EXEC usuario. ²

El resultado que aparece en pantalla varía, según el nivel del software Cisco IOS y la configuración del router.

Si un usuario desea configurar el reloj del router pero no sabe cuál es el comando adecuado, puede usar la función de ayuda para conocer cuál es el comando correcto. ³El ejercicio siguiente ilustra uno de los muchos usos de la función de ayuda.



```
Router
Cisco#cl?
clear clock
Cisco#clock
% Incomplete command.
Cisco#clock ?
    set Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
    hh:mm:ss Current Time
```

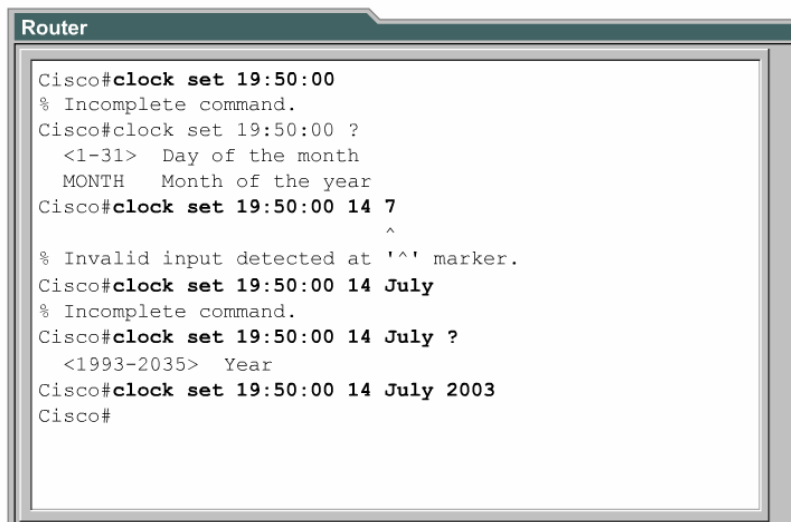
Figura 3

La tarea es configurar el reloj del router. Considere que no conoce el comando correspondiente, y efectúe lo siguiente:

Paso 1 Use ? para encontrar el comando adecuado para configurar el reloj. El resultado de la ayuda indica que se requiere el comando **clock** (reloj).

Paso 2 Verifique la sintaxis para hacer cambios en la hora.

Paso 3 Introduzca la hora actual en horas, minutos y segundos, tal como se muestra en la Figura ⁴. El sistema indica que se debe suministrar información adicional para completar el comando.



```
Router
Cisco#clock set 19:50:00
% Incomplete command.
Cisco#clock set 19:50:00 ?
    <1-31> Day of the month
    MONTH Month of the year
Cisco#clock set 19:50:00 14 7
    ^
% Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 14 July
% Incomplete command.
Cisco#clock set 19:50:00 14 July ?
    <1993-2035> Year
Cisco#clock set 19:50:00 14 July 2003
Cisco#
```

Figura 4

Paso 4 Presione **Control-P** (o la tecla flecha-arriba) para repetir el comando anterior automáticamente. Luego agregue un espacio y un signo de interrogación (?) para mostrar argumentos adicionales. Ahora se puede completar el comando.

Paso 5 El acento circunflejo (^) y la respuesta de la ayuda indican un error. La ubicación del acento ^ le muestra el lugar donde está ubicado el posible problema. Para reingresar con la sintaxis correcta, vuelva a introducir el comando hasta el lugar donde se encuentra el acento circunflejo, y escriba luego un signo de pregunta (?).

Paso 6 Introduzca el año, siguiendo la sintaxis correcta, y presione **Retorno** o **Intro** para ejecutar el comando.

2.2.7 Comandos ampliados de edición

La interfaz de usuario incluye un modo de edición ampliado que suministra un conjunto de funciones de teclas de edición que permiten que el usuario edite una línea de comando a medida que se la escribe. Las secuencias clave que se indican en la Figura 1 se pueden usar para mover el cursor sobre la línea de comando a efectos de realizar correcciones o cambios. Aunque el modo de edición ampliado se habilita automáticamente en la versión actual del software, se puede desactivar si interfiere con la interacción de guiones escritos. Para desactivar el modo de edición ampliado, escriba **terminal no editing** en la petición de entrada del modo EXEC privilegiado.

Comando	Descripción
Ctrl-A	Desplazarse al principio de la línea de comandos
Esc-B	Desplazarse una palabra hacia atrás
Ctrl-B (o flecha izquierda)	Desplazarse un carácter hacia atrás
Ctrl-E	Desplazarse hasta el final de la línea de comandos
Ctrl-F (o flecha derecha)	Desplazarse un carácter hacia adelante
Esc-F	Desplazarse una palabra hacia adelante

Figura 1

El conjunto de comandos de edición incluye una función de desplazamiento horizontal para comandos que ocupen más de una línea en la pantalla. Cuando el cursor alcanza el margen derecho, la línea de comando se desplaza diez espacios hacia la izquierda. Los primeros diez caracteres de la línea se ocultan, pero el usuario puede desplazar la línea hacia atrás para verificar la sintaxis al principio del comando. Para desplazarse hacia atrás, presione **Control-B** o la tecla flecha-izquierda reiteradamente hasta llegar al principio del comando. **Control-A** hará que el usuario vuelva directamente al principio de la línea.

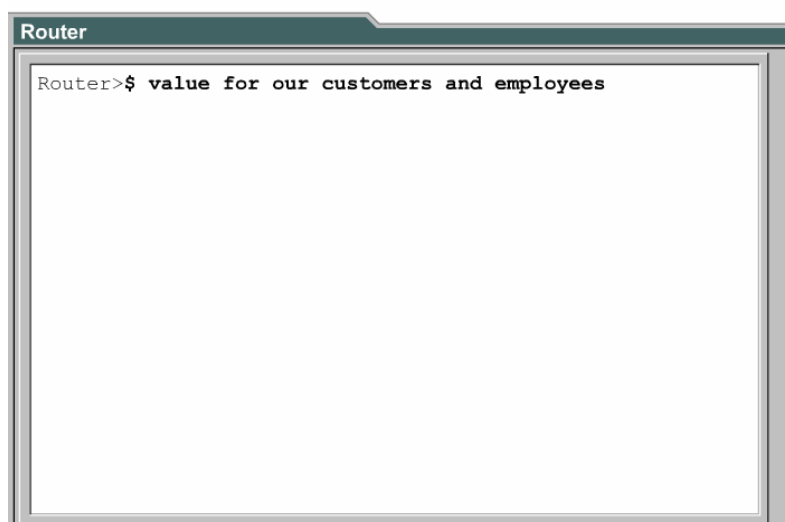


Figura 2

En el ejemplo que aparece en la Figura 2, el comando ocupa más de una línea. Cuando el cursor alcanza por primera vez el final de una línea, la línea se desplaza diez espacios hacia la izquierda. El signo pesos (\$) indica que la línea se ha desplazado hacia la izquierda. Cada vez que el cursor alcanza el final de la línea, la línea vuelve a desplazarse diez espacios hacia la izquierda.

El resultado que aparece en pantalla varía, según el nivel del software Cisco IOS y la configuración del router.

Control-Z es un comando que se usa para salir del modo de configuración. Hace que el usuario regrese a la petición de entrada del modo EXEC privilegiado.

2.2.8 Historial de comandos del router

La interfaz de usuario proporciona un historial o registro de los comandos que se han introducido. Esta función es particularmente útil para reintroducir comandos largos o complejos. Mediante la función de historial de comandos, se puede completar las siguientes tareas:

- Establecer el tamaño del buffer de historial de comandos
- Reintroducir comandos
- Desactivar la función de historial de comandos

El historial de comandos se activa por defecto y el sistema recuerda diez líneas de comandos en el buffer del historial. Para cambiar la cantidad de líneas de comando que el sistema recuerda durante una sesión de terminal, utilice el comando **terminal history size** (tamaño del historial de terminal) o el comando **history size**. ¹La cantidad máxima de comandos es 256.

Comando	Descripción
Ctrl-P o tecla flecha arriba	Hace aparecer nuevamente el último comando (comando anterior)
Ctrl-N o tecla flecha abajo	Hace aparecer nuevamente el comando más reciente
Router> show history	Muestra el buffer de comando
Router> terminal history size <i>number-of-lines</i>	Establece el tamaño del buffer de historial de comandos*
Router> terminal no editing	Deshabilita las funciones de edición avanzada
Router> terminal editing	Re-enable advanced editing
<Tab>	Completa la entrada

Figura 1

Para reintroducir comandos que se encuentran en el buffer del historial, a partir del comando más reciente, presione **Control-P** o la tecla flecha-arriba repetidas veces para reintroducir comandos sucesivamente más antiguos. Para regresar a los comandos más recientes en el buffer del historial, luego de introducir nuevamente los comandos con **Control-P** o la tecla flecha-arriba, presione **Control-N** o la tecla flecha-abajo repetidas veces para reintroducir comandos sucesivamente más recientes.

Para mayor rapidez al escribir comandos, se puede escribir los caracteres exclusivos del comando. Presione la tecla **Tab**, y la interfaz completará la entrada. Si las letras distintivas identifican el comando, la tecla **Tab** simplemente señala que el router ha comprendido el comando específico que se desea introducir.

En la mayoría de los computadores hay funciones adicionales de selección y copia disponibles. Se puede copiar y luego pegar o insertar una cadena anterior de comandos como el comando actual.

2.2.9 Diagnóstico de fallas de los errores de línea de comandos

Los errores de línea de comandos se producen principalmente debido a errores de tecleo. Si un comando es escrito de forma incorrecta, la interfaz del usuario muestra el error mediante un indicador de error (^). El símbolo "^" aparece en el punto de la cadena del comando donde se introdujo el comando, palabra clave o argumento incorrecto. El indicador de ubicación del error y el sistema de ayuda interactiva permiten al usuario localizar y corregir fácilmente los errores de sintaxis.

```
Router#clock set 13:32:00 23 February 99
```

^

Invalid input detected at "^" marker.

El acento circunflejo (^) y la respuesta de ayuda indican que se ha producido un error en 99. Para que se muestre la sintaxis correcta, escriba el comando hasta el punto donde se ha producido el error y luego escriba un signo de interrogación (?):

```
Router#clock set 13:32:00 23 February ?
```

```
<1993-2035> Year
```

```
Router#clock set 13:32:00 23 February
```

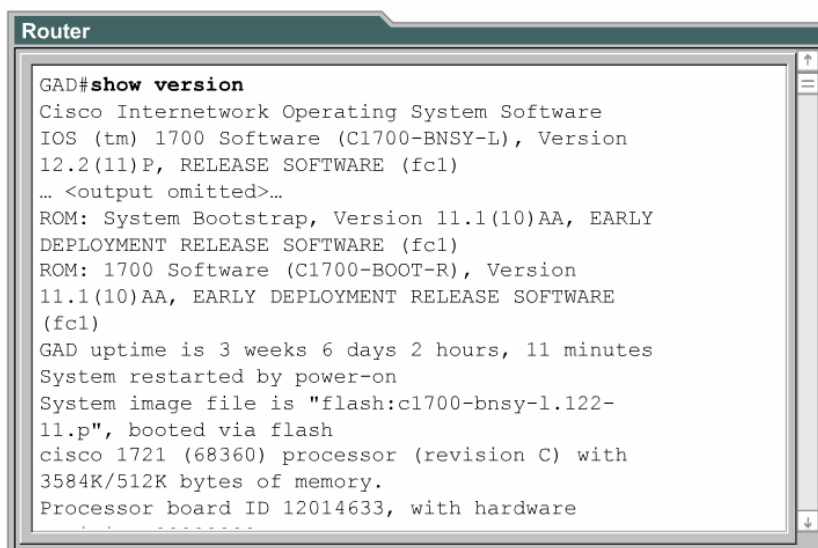
Introduzca el año, siguiendo la sintaxis correcta, y presione **Retorno** para ejecutar el comando.

Router#**clock set 13:32:00 23 February 1999**

Si una línea de comando es escrita de forma incorrecta y se presiona la tecla Intro, se puede presionar la tecla flecha-arriba para reescribir el último comando. Use las teclas flecha-derecha e izquierda para mover el cursor hasta el lugar donde se cometió el error. Luego escriba la corrección necesaria. Si es necesario eliminar algo, use la tecla retroceso.

2.2.10 El comando show version

El comando **show version** muestra información acerca de la versión del software Cisco IOS en uso en el router. Esto incluye el registro de configuración y el registro de arranque.



```
Router
GAD#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
... <output omitted>...
ROM: System Bootstrap, Version 11.1(10)AA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 1700 Software (C1700-BOOT-R), Version
11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
GAD uptime is 3 weeks 6 days 2 hours, 11 minutes
System restarted by power-on
System image file is "flash:c1700-bnsy-1.122-
11.p", booted via flash
cisco 1721 (68360) processor (revision C) with
3584K/512K bytes of memory.
Processor board ID 12014633, with hardware
```

Figura 1

La Figura 1 muestra la siguiente información acerca del comando **show version**:

- Versión e información descriptiva del IOS
- Versión de la ROM de bootstrap
- Versión de la ROM de arranque
- Tiempo de actividad del router
- Último método de reinicio
- Ubicación y nombre del archivo de imagen del sistema
- Plataforma del router
- Valores del registro de configuración

Use el comando **show version** para identificar la imagen del IOS del router y la fuente de arranque.

Resumen

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

- Las funciones del IOS
- El funcionamiento básico del IOS
- La identificación de las diversas funciones del IOS
- La identificación de los métodos para establecer una sesión CLI con el router
- Las diferencias entre los modos EXEC usuario y EXEC privilegiado
- Cómo establecer una sesión de HyperTerminal
- Iniciar una sesión en el router
- Uso de la función de ayuda en la interfaz de línea de comando
- Uso de los comandos de edición ampliados
- Uso del historial de comandos
- Diagnóstico de errores de línea de comandos
- Uso del comando **show version**

Módulo 3: Configuración del router

Descripción general

Configurar un router para que realice las complejas tareas de redes y telecomunicaciones puede resultar un desafío. No obstante, los procedimientos iniciales para configurar el router no son difíciles en absoluto. Si se ejercitan estos procedimientos y los pasos para cambiar de un modo a otro, las configuraciones más complejas no serán tan abrumadoras. Este módulo introduce los modos básicos de configuración del router y brinda oportunidades para practicar configuraciones sencillas.

La meta de todo administrador de red debe ser la de disponer de configuraciones claras y fáciles de entender, y que las mismas sean respaldadas periódicamente. El Cisco IOS brinda al administrador una gama de herramientas que permiten agregar comentarios al archivo de configuración, para efectos de documentación. De la misma manera que un programador competente documenta cada paso de su programación, un administrador de red debe documentar cuanta información le sea posible, en caso de que otra persona deba asumir la responsabilidad de la red.

Luego de completar este módulo, los estudiantes deben ser capaces de:

- Dar nombre a un router
- Fijar contraseñas
- Examinar los comandos show
- Configurar una interfaz serial
- Configurar una interfaz Ethernet
- Realizar cambios a un router
- Guardar los cambios realizados a un router
- Configurar una descripción de interfaz
- Configurar un mensaje del día
- Configurar tablas de host
- Comprender la importancia de hacer copias de respaldo y de documentar

3.1 Configuración del router

3.1.1 Modos de comando CLI

Todos los cambios de configuración hechos mediante la interfaz de línea de comando (CLI) en un router Cisco, se realizan desde el modo de configuración global. Se ingresa a otros modos de operación más específicos según sea el cambio de configuración requerido, pero dichos modos específicos son todos subconjuntos del modo de configuración global. ¹

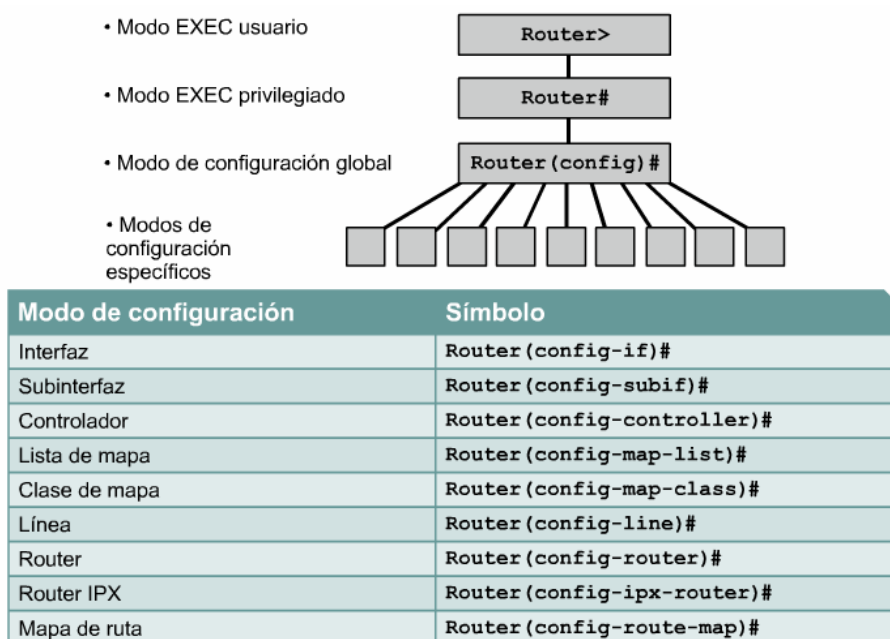


Figura 1

Los comandos del modo de configuración global se utilizan en un router para ejecutar comandos de configuración que afectan al sistema como un todo. El siguiente comando lleva al router al modo de configuración global y permite ingresar comandos desde la terminal:

NOTA:

La petición de entrada cambia para indicar que el router se encuentra ahora en modo de configuración global.

```
Router#configure terminal
```

```
Router(config)#
```

El modo de configuración global, a menudo abreviado como 'global config', es el modo de configuración principal. Estos son algunos de los modos de operación a los que se puede ingresar desde el modo de configuración global:

- Modo de interfaz
- Modo de línea
- Modo router
- Modo de subinterfaz
- Modo de controlador

Al ingresar a estos modos específicos, la petición de entrada del router cambia para señalar el modo de configuración en uso. Todo cambio de configuración que se realice, tendrá efecto únicamente en las interfaces o procesos relativos a ese modo particular.

Al escribir **exit** desde alguno de estos modos de configuración específicos, el router regresa al modo de configuración global. Al presionar **Control-Z**, se sale por completo del modo de configuración y el router vuelve al modo EXEC privilegiado.

3.1.2 Configuración del nombre de router

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Router(config)#hostname Tokyo
```

```
Tokyo(config)#
```

Al presionar la tecla **Enter**, la petición de entrada ya no mostrará el nombre de host por defecto ('Router'), sino el nombre de host que se acaba de configurar, 'Tokio', en el ejemplo anterior.

3.1.3 Configuración de contraseñas de router

Las contraseñas restringen el acceso a los routers. Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas también se usan para controlar el acceso al modo EXEC privilegiado, a fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.

Contraseña de la consola

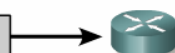
```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

**Contraseña de la terminal virtual**

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

**Permita la palabra de acceso**

```
Router(config)#enable password san-fran
```

**Ejecutar cifrado de la contraseña**

```
Router(config)#service password-encryption
Router(config)#enable secret <password>
```

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

```
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login
```

Se debe fijar contraseñas en una o más de las líneas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY. Se suele usar la misma contraseña para todas las líneas, pero a veces se reserva una línea mediante una contraseña exclusiva, para que sea posible el acceso al router aunque haya demanda de más de cuatro conexiones. Los siguientes comandos se utilizan para establecer contraseñas en las líneas de VTY:

```
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login
```

Los comandos **enable password** y **enable secret** se utilizan para restringir el acceso al modo EXEC privilegiado. El comando **enable password** se utiliza sólo si no se ha configurado previamente **enable secret**. Se recomienda habilitar siempre **enable secret**, ya que a diferencia de **enable password**, la contraseña estará siempre cifrada. Estos son los comandos que se utilizan para configurar las contraseñas:

```
Router(config)#enable password <password>
Router(config)#enable secret <password>
```

En ocasiones es deseable evitar que las contraseñas se muestren en texto sin cifrar al ejecutar los comandos **show running-config** o **show startup-config**. El siguiente comando se utiliza para cifrar las contraseñas al mostrar los datos de configuración:

```
Router(config)#service password-encryption
```

El comando **service password-encryption** aplica un cifrado débil a todas las contraseñas sin cifrar. El comando **enable secret <password>** usa un fuerte algoritmo MD5 para cifrar.

3.1.4 Uso de los comandos show

Los numerosos comandos **show** se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo EXEC privilegiado como en el modo EXEC de usuario, el comando **show ?** muestra una lista de los comandos **show** disponibles. La lista en el modo EXEC privilegiado es considerablemente más larga que en el modo EXEC de usuario.

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando **show interfaces** seguido de la interfaz específica y el número de puerto. Por ejemplo:
Router#**show interfaces serial 0/1**
- **show controllers serial:** muestra información específica de la interface de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz. Por ejemplo:
Router#**show controllers serial 0/1**
- **show clock:** Muestra la hora fijada en el router
- **show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones
- **show users:** Muestra todos los usuarios conectados al router
- **show history:** Muestra un historial de los comandos ingresados
- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí
- **show version:** Despliega la información acerca del routery de la imagen de IOS que esté corriendo en al RAM. Este comando también muestra el valor del registro de configuración del router
- **show ARP:** Muestra la tabla ARP del router
- **show protocols:** Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado
- **show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM

- **show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class

3.1.5 Configuración de una interfaz serial

Es posible configurar una interfaz serial desde la consola o a través de una línea de terminal virtual. Siga estos pasos para configurar una interfaz serial:

1. Ingrese al modo de configuración global
2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
5. Active la interfaz.

En los siguientes comandos, el argumento "tipo" incluye serial, ethernet, fastethernet, token ring y otros:

```
Router(config)#interface type port  
Router(config)#interface type slot/port
```

El siguiente comando se utiliza para desactivar la interfaz de forma administrativa:

```
Router(config-if)#shutdown
```

El siguiente comando se utiliza para activar una interfaz que se ha desactivado:

```
Router(config-if)#no shutdown
```

El siguiente comando se utiliza para salir del modo de configuración de interfaz actual:

```
Router(config-if)#exit
```

A cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

```
Router(config)#interface serial 0/0  
Router(config-if)#ip address <ip address> <netmask>
```

Las interfaces seriales necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE, por ejemplo un CSU, proporciona dicha señal. Por defecto, los routers Cisco son dispositivos DTE, pero se pueden configurar como dispositivos DCE.

En los enlaces seriales interconectados directamente, como en un entorno de laboratorio, un extremo debe considerarse como un DCE y debe proporcionar la señal de sincronización. Se activa la sincronización y se fija la velocidad mediante el comando **clock rate**. Las velocidades de sincronización disponibles (en bits por segundo) son: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, ó 4000000. No obstante, es posible que algunas de estas velocidades no estén disponibles en algunas interfaces seriales, según su capacidad.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o de diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

En el entorno del laboratorio, se utilizará una velocidad de sincronización de 56000. Los comandos para fijar la velocidad de sincronización y activar una interfaz serial son los siguientes:

```
Router(config)#interface serial 0/0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

3.1.6 Cambios en la Configuración

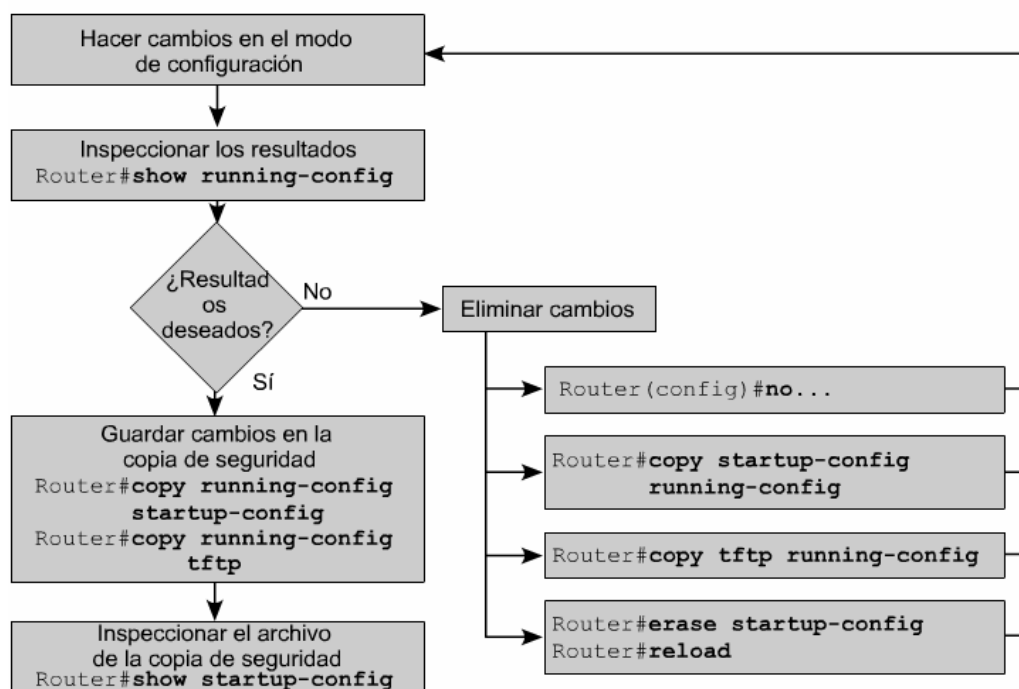
Si es necesario modificar una configuración, se debe ir al modo de operación apropiado e ingresar el comando correspondiente. Por ejemplo, para activar una interfaz, ingrese al modo de configuración global, luego al modo de configuración de interfaces, y ejecute el comando **no shutdown**.

Para comprobar los cambios, use el comando **show running-config**. Este comando mostrará la configuración en uso. Si las variables que se muestran no son las esperadas, es posible corregir el entorno efectuando uno o más de los siguientes pasos:

- Ejecute la forma **no** de un comando de configuración.
- Vuelva a cargar el sistema para regresar a la configuración original de configuración almacenada en la NVRAM.
- Copie un archivo de configuración desde un servidor TFTP.
- Elimine el archivo de configuración de inicio con **erase startup-config**, luego reinicie el router e ingrese al modo de configuración inicial (setup).

Para guardar las variables en la configuración de inicio en NVRAM, ejecute el siguiente comando al estar en EXEC privilegiado:

```
Router#copy running-config startup-config
```



3.1.7 Configuración de una interfaz Ethernet

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual.

A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

Para configurar una interfaz Ethernet, siga estos pasos:

1. Ingrese al modo de configuración global
2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. Active la interfaz

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

3.2 Pasos finales de la configuración

3.2.1 Importancia de los estándares de configuración

Dentro de las organizaciones, es importante el desarrollo de estándares para los archivos de configuración. Eso permite controlar el número de archivos de configuración que se deben mantener, y también el mecanismo y el lugar donde se almacenan. ¹

- Un estándar es un conjunto de reglas o procedimientos de uso generalizado o de carácter oficial
- Un requisito de estándares de configuración ordena la topología y las funciones de la red

Figura 1

Un estándar es un conjunto de reglas o procedimientos, de uso generalizado o de carácter oficial. Si una organización carece de estándares, una interrupción del servicio podría causar el caos en la red.

Para poder administrar una red, es necesario disponer de estándares de apoyo técnico centralizado. Se debe resolver adecuadamente asuntos como configuraciones, seguridad, rendimiento y otros, para que la red funcione sin tropiezos. La creación de estándares para la solidez de una red contribuye a reducir su complejidad, las paradas no planificadas, y el riesgo ante sucesos que pudieran tener un impacto negativo sobre su rendimiento.

3.2.2 Descripción de interfaces

La descripción de las interfaces se emplea para indicar información importante, como puede ser la relativa a un router distante, el número de un circuito, o un segmento de red específico. La descripción de la interfaz puede ayudar a un usuario de red a recordar información específica de la interfaz, como por ejemplo, a cuál red atiende dicha interfaz. ¹



```
Tokyo(config)#interface e 0  
Tokyo(config-if)#description Engineering LAN, Bldg. 18
```

Figura 1

La descripción es sólo un comentario escrito acerca de la interfaz. Aunque la descripción se encuentra en los archivos de configuración en la memoria del router, no tiene efectos sobre su operación. Las descripciones se crean siguiendo un formato estándar de acuerdo al tipo de interfaz. La descripción puede incluir el propósito y la ubicación de la interfaz, otros dispositivos o localidades geográficas conectadas a la interfaz, y también identificadores de circuitos. Las descripciones permiten que el personal de apoyo comprenda mejor el alcance de los problemas relacionados con una interfaz, y permite resolver los problemas con mayor celeridad.

3.2.3 Configuración de la descripción de interfaces

Para configurar una descripción de interfaz, ingrese al modo de configuración global. Desde el modo de configuración global, ingrese al modo de configuración de interfaz. Use el comando **description** seguido de la información.

Pasos a seguir:

Ingresa al modo de configuración global, mediante el comando **configure terminal**.

Ingresa al modo de interfaz específica (por ejemplo interfaz Ethernet 0) **interface ethernet 0**.

Introduzca el comando **description**, seguido de la información que se deberá mostrar. Por ejemplo, Red XYZ, Edificio 18.

Salga del modo de interfaz y regrese al modo EXEC privilegiado mediante el comando **ctrl-z**.

Guarde los cambios de configuración en la NVRAM mediante el comando **copy running-config startup-config**.

A continuación se da dos ejemplos de descripciones de interfaz:

```
interface Ethernet 0
description LAN Engineering, Bldg.2
interface serial 0
description ABC network 1, Circuit 1
```

3.2.4 Mensajes de inicio de sesión

El mensaje de inicio de sesión se muestra al usuario al momento de hacer login en el router, y se usa para comunicar información de interés a todos los usuarios de la red, tales como avisos de próximas interrupciones del sistema.

Todos pueden ver los mensajes de inicio de sesión. Por lo tanto, se debe poner especial atención a la redacción de dichos mensajes. "Bienvenido" es una invitación a entrar al router, y probablemente no sea un mensaje apropiado. ¹

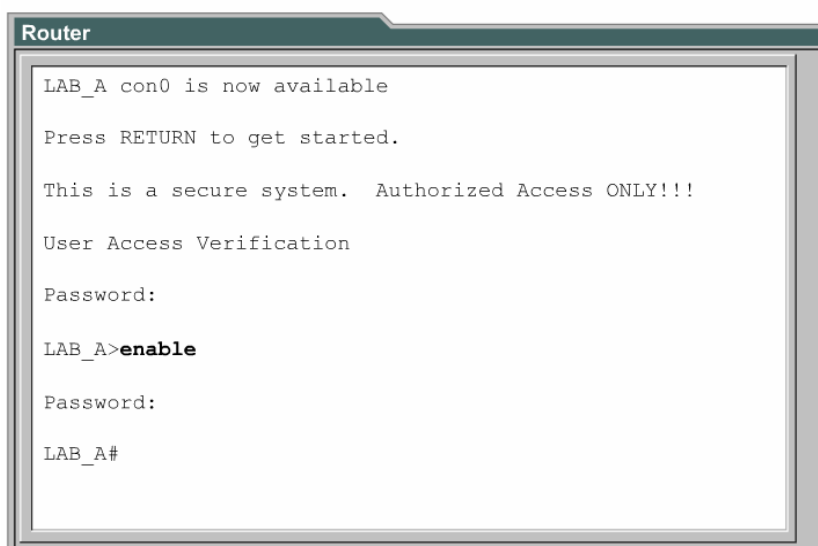


Figura 1

Un mensaje de inicio de sesión debe advertir que sólo los usuarios autorizados deben intentar el acceso. Un mensaje del estilo "¡Este es un sistema protegido, ingrese únicamente si está autorizado!" advierte a los visitantes que el ir más allá está prohibido y es ilegal.

3.2.5 Configuración del mensaje del día (MOTD)

Se puede configurar un mensaje del día (MOTD), para que sea mostrado en todas las terminales conectadas.

Ingresa al modo de configuración global para configurar un texto como mensaje del día (MOTD). Use el comando **banner motd**, seguido de un espacio y un delimitador, como por ejemplo el signo numeral (#). Escriba el mensaje del día (MOTD) seguido de un espacio y de nuevo el delimitador. 1

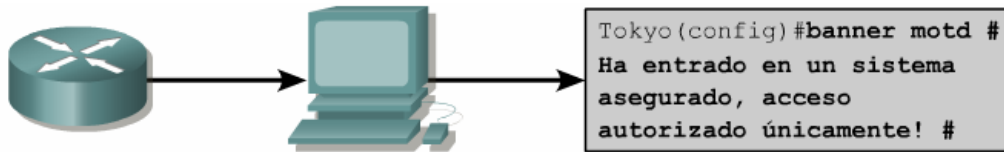


Figura 1

Siga estos pasos para crear y mostrar un mensaje del día:

1. Ingresa al modo de configuración global, mediante el comando **configure terminal**.
2. Escriba el comando **banner motd # Escriba aquí el mensaje del día #**.
3. Guarde los cambios mediante el comando **copy running-config startup-config**.

3.2.6 Resolución de nombres de host

La resolución de nombres de host es el mecanismo que utiliza un computador para relacionar un nombre de host con una dirección de IP.

Para poder usar nombres de host para comunicarse con otros dispositivos de IP, los dispositivos de red, como los routers, deben poder vincular los nombres de host con las direcciones de IP. Una lista de nombres de host y sus direcciones de IP asignadas se denomina tabla de host. 1

Lo siguiente es un ejemplo de la configuración de una tabla de host en un router:

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Figura 1

Una tabla de host puede incluir todos los dispositivos de una red. Cada dirección de IP individual puede estar vinculada a un nombre de host. El software Cisco IOS mantiene un archivo de vínculos entre los nombres de host y las direcciones de IP, el cual es utilizado por los comandos EXEC. Este caché agiliza el proceso de conversión de nombres a direcciones.

Los nombres de host, a diferencia de los nombres DNS, sólo tienen vigencia en el router en el que están configurados. La tabla de host permite que el administrador de red pueda escribir tanto el nombre del host, como puede ser Auckland, como la dirección de IP, para conectarse por Telnet a un host remoto. 1

3.2.7 Configuración de tablas de host

Para asignar nombres de host a direcciones, primero ingrese al modo de configuración global. Ejecute el comando **ip host** seguido del nombre de destino y todas las direcciones de IP con las que se puede llegar al dispositivo. Esto asigna el nombre del host a cada una de sus direcciones IP. Para llegar al host, use un comando **telnet** o **ping** con el nombre del router o una dirección de IP que esté vinculada al nombre del router.

El procedimiento para configurar la tabla de host es:

1. Ingresa al modo de configuración global en el router.
2. Ejecute el comando **ip host** seguido del nombre del router y todas las direcciones de IP asociadas con las interfaces en cada router.
3. Repita el proceso, hasta que todos los routers de la red hayan sido configurados.
4. Guarde la configuración en la NVRAM.

3.2.8 Hacer copias de respaldo y documentar la configuración

La configuración de los dispositivos de la red determina el comportamiento de la red. La administración de las configuraciones de los dispositivos incluye las siguientes tareas:

- Confeccionar una lista y comparar los archivos de configuración de los dispositivos activos
- Almacenar los archivos de configuración en servidores de red
- Instalar y actualizar software

Se deben guardar copias de respaldo de los archivos de configuración, en caso de que surja algún problema. Dichas copias se pueden guardarse en un servidor de red, un un servidor TFTP, o en un disco que se conserve en un lugar seguro. ¹Se debe documentar la información, y la misma debe también guardarse fuera de línea.

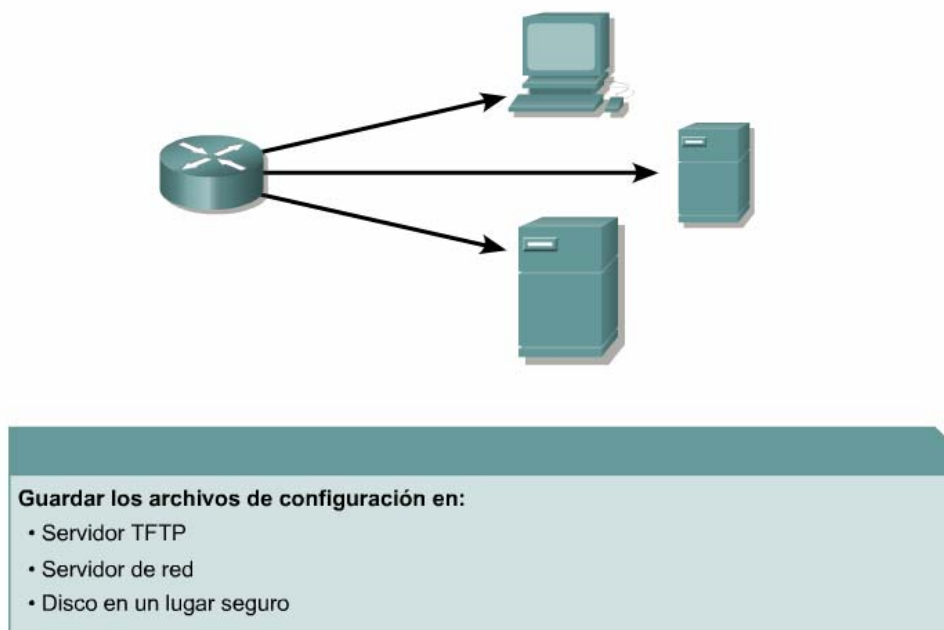


Figura 1

3.2.9 Copiar, modificar y pegar configuraciones

Se puede almacenar una copia de la configuración en uso, en un servidor TFTP. Se puede usar el comando **copy running-config tftp**, como se muestra en la Figura ¹, para almacenar la configuración en uso del router en un servidor TFTP. Para ello, realice las siguientes tareas:

```
Router
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!! [OK]
```

Figura 1

Paso 1 Ejecute el comando **copy running-config tftp**.

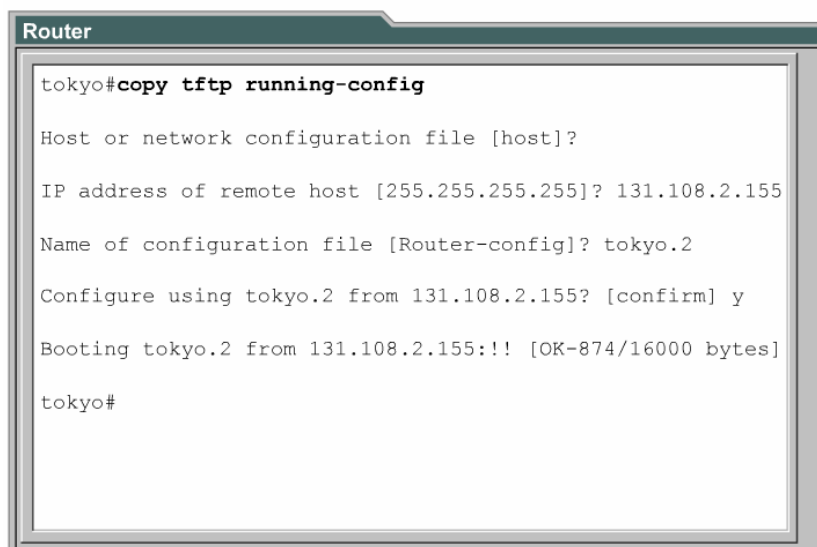
Paso 2 Introduzca la dirección de IP del host en el cual se almacenará la configuración.

Paso 3 Introduzca el nombre a ser asignado al archivo de configuración.

Paso 4 Confirme sus selecciones respondiendo yes (sí) cada vez que se le solicite que lo haga.

Se puede usar un archivo de configuración ubicado en alguno de los servidores para configurar un router. Para ello, realice las siguientes tareas:

1. Ingrese al modo de configuración, mediante el comando **copy tftp running-config**, como se muestra en la Figura 2.
2. Con la petición de entrada del sistema en pantalla, seleccione un archivo de configuración de host o de red. El archivo de configuración de red contiene comandos relacionados con todos los routers y servidores de terminales de la red. El archivo de configuración de host contiene comandos relativos a un router en particular. Con la petición de entrada en pantalla, introduzca la dirección de IP opcional del host remoto en el cual se encuentra el archivo de configuración. En la línea de comandos del sistema, escriba la dirección IP del host remoto donde se encuentra el servidor TFTP. En este ejemplo, el router se configura desde el servidor TFTP con la dirección IP 131.108.2.155.
3. Con la petición de entrada en pantalla, introduzca el nombre del archivo de configuración o acepte el nombre preconfigurado. La convención de nombres para los archivos se basa en UNIX. Los nombres preconfigurados de los archivos son **hostname-config** para el archivo de host y **network-config** para el archivo de configuración de red. En el entorno DOS, los nombres están limitados a ocho caracteres, más una extensión de tres caracteres (por ejemplo, **router.cfg**). Confirme el nombre del archivo de configuración y la dirección del servidor TFTP que suministra el sistema. Observe que, en la Figura 2, la petición de entrada del router cambia a **tokyo** de forma inmediata. Esto comprueba que la reconfiguración ocurre tan pronto como se descarga el nuevo archivo.



```
Router
tokyo#copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

Figura 2

La configuración del router también se puede guardar en un disco. Para ello se efectúa una captura de texto en el router, para luego guardar dicho texto en el disco o en el disco duro. Cuando sea necesario copiar el archivo nuevamente al router, use las funciones estándar de edición de un programa emulador de terminal para pegar (paste) el archivo de comandos en el router.

Resumen

Esta sección resume los puntos clave de la configuración de un router.

El router tiene varios modos de operación:

- Modo EXEC usuario
- Modo EXEC privilegiado
- Modo de configuración global
- Otros modos de configuración

La interfaz de línea de comando se puede usar para hacer cambios a la configuración:

- Fijar el nombre de host
- Fijar contraseñas
- Configurar interfaces
- Modificar configuraciones
- Mostrar configuraciones

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

- Los estándares de configuración son elementos fundamentales para el éxito de toda organización que mantenga una red eficiente.
- Las descripciones de las interfaces pueden incluir información que ayude a los administradores a entender y a diagnosticar problemas en sus redes.
- Los mensajes de inicio de sesión y los mensajes del día proporcionan información a los usuarios cuando se conectan al router.
- La resolución de nombres de host traduce nombres a direcciones de IP, lo que permite al router convertir rápidamente dichos nombres en direcciones.
- Es en extremo importante hacer copias de respaldo y también documentar las configuraciones, para un funcionamiento sin tropiezos de la red.

Módulo 4: Aprender sobre otros dispositivos

Descripción general

A veces los administradores de red se enfrentan a situaciones en las que la documentación de la red se encuentra incompleta o es imprecisa. El Protocolo de descubrimiento de Cisco (CDP) puede resultar una herramienta útil para estas situaciones ya que ayuda a crear un panorama de la red. El CDP es un protocolo propietario de Cisco, destinado al descubrimiento de vecinos y es independiente de los medios y el protocolo. Aunque el CDP solamente mostrará información sobre los vecinos conectados de forma directa, este constituye una herramienta de gran utilidad.

En muchos casos, después de configurar un router por primera vez, el administrador de red descubre que resulta difícil o inconveniente conectarse directamente al router para efectuar cambios de configuración u otras tareas. Telnet es una aplicación basada en TCP/IP que permite la conexión remota con la interfaz de línea de comando del router (CLI) con el propósito de efectuar tareas de configuración, monitoreo y diagnóstico de fallas. Constituye una herramienta esencial para el profesional de redes.

Los estudiantes que completen este módulo deberán poder:

- Activar y desactivar el CDP
- Utilizar el comando **show cdp neighbors**
- Determinar cuáles dispositivos vecinos están conectados a cuáles interfaces locales
- Usar el CDP para recaudar información de las direcciones de red de los dispositivos vecinos
- Establecer una conexión Telnet
- Verificar una conexión Telnet
- Desconectarse de la sesión Telnet
- Suspender una sesión Telnet
- Realizar pruebas de conectividad alternativas
- Diagnosticar las fallas de las conexiones de terminales remotas

4.1 Detección y conexión con vecinos

4.1.1 Introducción al CDP

El Protocolo de descubrimiento de Cisco (CDP) es un protocolo de Capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores, como lo indica la Figura 1. El CDP se utiliza para obtener información sobre los dispositivos vecinos, tal como los tipos de dispositivos conectados, las interfaces de router a las que están conectados, las interfaces empleadas para realizar las conexiones, y los números de modelo de los dispositivos. El CDP es independiente de los medios y los protocolos, y es ejecutable en todos los equipos Cisco sobre el Protocolo de acceso de subred (SNAP).

Direcciones de entrada de la capa superior	TCP/IP	Novell IPX	AppleTalk	Otros
Protocolo de enlace de datos propietario de Cisco	CDP detecta y muestra información acerca de los dispositivos de Cisco directamente conectados			
Soporte de medios SNAP	LANS	Frame Relay	ATM	Otros

Figura 1

La versión 2 del CDP (CDPv2) es la versión más reciente del protocolo. El Cisco IOS (Versión 12.0(3) o posteriores) admiten el CDPv2. En las versiones de Cisco IOS 10.3 a 12.0(3)T, la función de CDPv1 está activada de manera predeterminada.

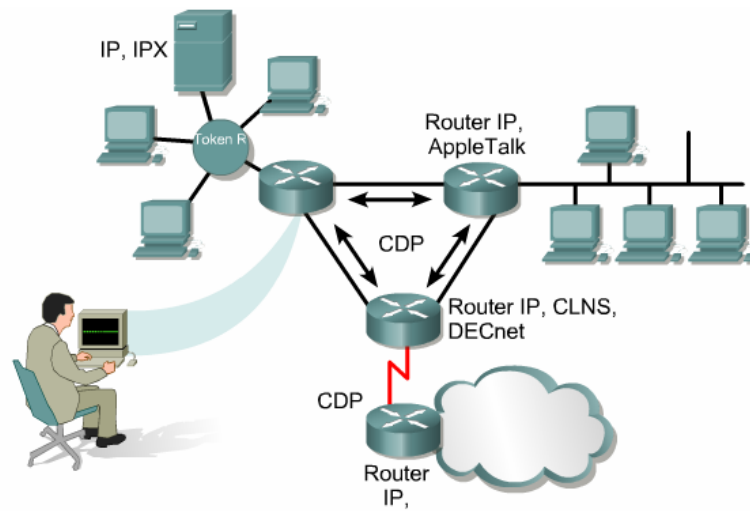
Cuando arranca un dispositivo Cisco, el CDP se inicia de forma automática y permite que el dispositivo detecte los dispositivos vecinos que también están ejecutando el CDP. Este protocolo de Cisco se ejecuta en la capa de enlace de datos y permite que dos sistemas obtengan información entre sí, incluso si estos sistemas están utilizando protocolos de capa de red diferentes.

Cada dispositivo configurado para el CDP envía mensajes periódicos, conocidos como publicaciones, a varios routers. Cada dispositivo publica al menos una dirección en la cual puede recibir mensajes del Protocolo de administración de red simple (SNMP). Las publicaciones también contienen información sobre el "tiempo de existencia" o tiempo de espera, que indica la cantidad de tiempo que los dispositivos de recepción deben mantener la información CDP antes de descartarla. Además, cada dispositivo escucha los mensajes periódicos CDP enviados por otros con el fin de obtener información de los dispositivos vecinos.

4.1.2 La información obtenida con CDP

El CDP se usa básicamente para detectar todos los dispositivos Cisco que se encuentran conectados directamente a un dispositivo local. Use el comando **show cdp neighbors** para visualizar las actualizaciones CDP en el dispositivo local.

La Figura 1 muestra un ejemplo de cómo el CDP presenta la información reunida a un administrador de red. Cada router que ejecuta el CDP intercambia información de protocolo con sus vecinos. El administrador de red puede mostrar los resultados de este intercambio de información CDP en una consola conectada al router local.



Comando único resume protocolos y direcciones en el objetivo (por ejemplo, un router Cisco vecino)

Figura 1

El administrador de red utiliza el comando **show cdp neighbors** para mostrar la información sobre las redes conectadas de forma directa al router. CDP provee información sobre cada dispositivo vecino CDP al transmitir los valores de longitud y tipo (TLVs), que constan de bloques de información incorporados en las publicaciones CDP.

Los TLV del dispositivo que muestra el comando **show cdp neighbors** incluyen los siguientes:

- Identificador del dispositivo
- Interfaz local
- Tiempo de espera
- Capacidad
- Plataforma
- Identificador del puerto

Los siguientes TLVs se incluyen sólo en CDPv2:

- Administración de nombres de dominio VTP
- VLAN Nativas

- Full o half-duplex

Observe que el router inferior de la figura no está conectado directamente al router de la consola del administrador. Para obtener información CDP acerca de este dispositivo, el administrador necesitaría iniciar una sesión Telnet a un router conectado directamente al dispositivo.

4.1.3 Implementación, monitoreo y mantenimiento del CDP

Los siguientes comandos se utilizan para implementar, monitorear y mantener la información CDP:

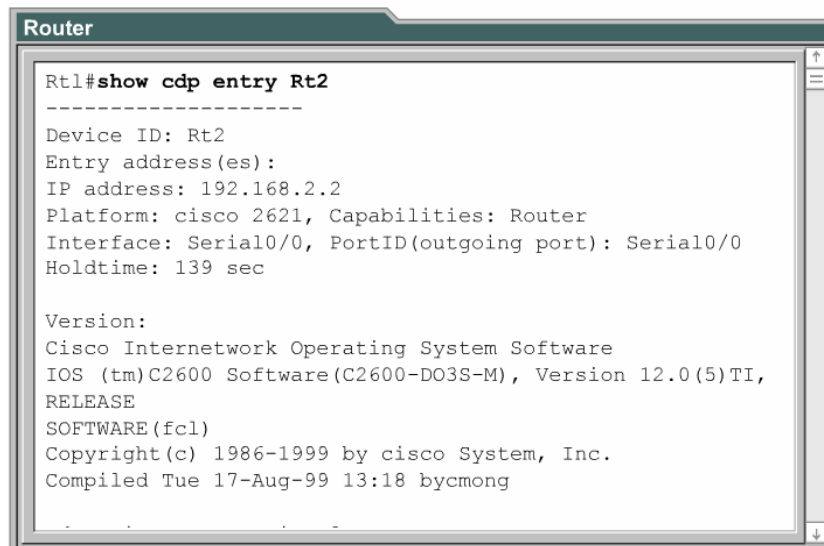
- **cdp run**
- **cdp enable**
- **show cdp traffic**
- **clear cdp counters** ¹
- **show cdp** ²
- **show cdp entry** {**|nombre-dispositivo[*]*}[*protocolo | versión*]} ³
- **show cdp interface** [número de tipo] ⁴
- **show cdp neighbors** [número de tipo] [detalle] ⁵

```
Router
Rt1#show cdp traffic
CDP counters:
  Total packets output: 6, Input:6
  Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
  No memory: 0, Invalid packet: 0, Fragmented:0
  CDP version1 advertisements output: 0, Input:0
  CDP version2 advertisements output: 6, Input:6
Rt1#clear cdp counters
Rt1#show cdp traffic
CDP counters:
  Total packets output: 0, Input:0
  Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
  No memory: 0, Invalid packet: 0, Fragmented:0
  CDP version1 advertisements output: 0, Input:0
  CDP version2 advertisements output: 0, Input:0
Rt1#
```

Figura 1

```
Router
CDP Version 1
Rt3#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
Rt3#
CDP Version 2
Rt1#show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rt1#
```

Figura 2



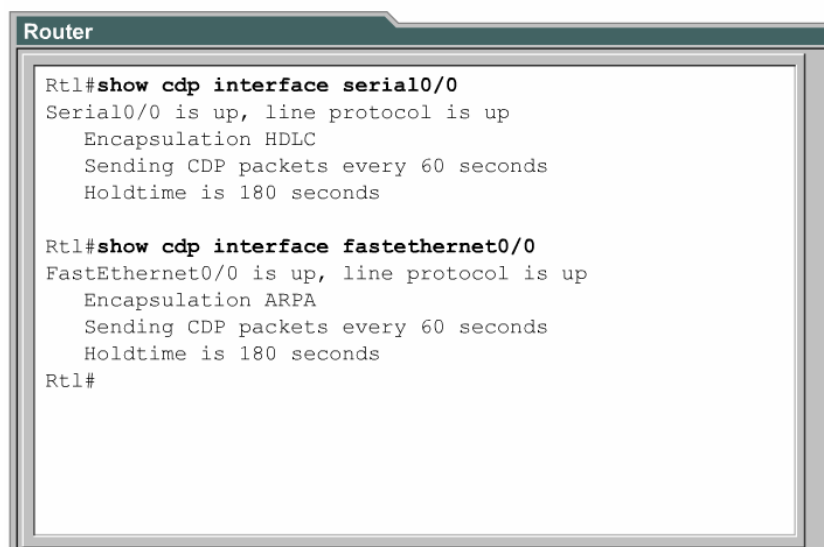
```

Router
Rt1#show cdp entry Rt2
-----
Device ID: Rt2
Entry address(es):
IP address: 192.168.2.2
Platform: cisco 2621, Capabilities: Router
Interface: Serial0/0, PortID(outgoing port): Serial0/0
Holdtime: 139 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DO3S-M), Version 12.0(5)TI,
RELEASE
SOFTWARE(fcl)
Copyright(c) 1986-1999 by cisco System, Inc.
Compiled Tue 17-Aug-99 13:18 bycmong

```

Figura 3



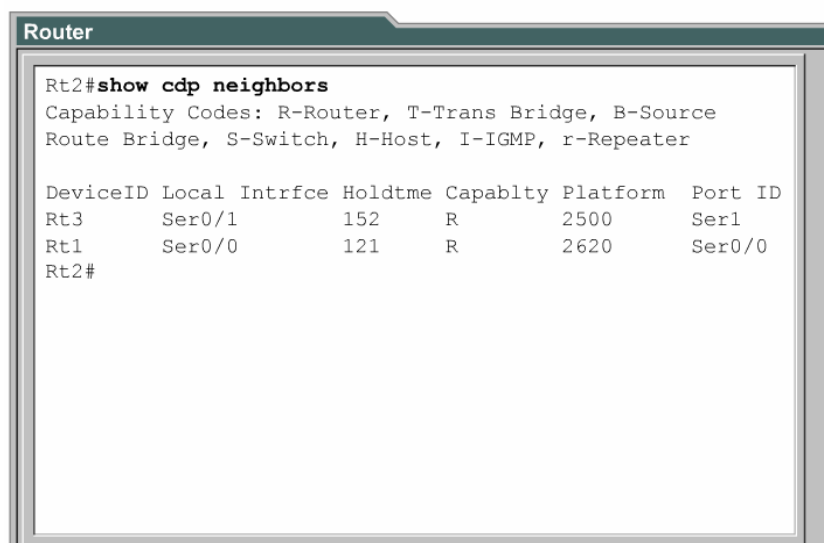
```

Router
Rt1#show cdp interface serial0/0
Serial0/0 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Rt1#show cdp interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Rt1#

```

Figura 4



```

Router
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capabltty Platform Port ID
Rt3      Ser0/1      152    R      2500      Ser1
Rt1      Ser0/0      121    R      2620      Ser0/0
Rt2#

```

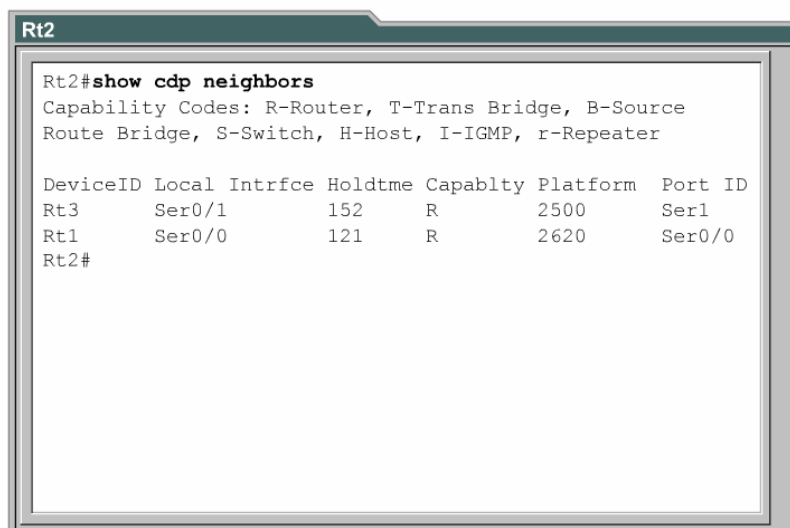
Figura 5

El comando **cdp run** se utiliza para activar el CDP de forma global en el router. El CDP se activa de forma global automáticamente. El comando **cdp enable** se utiliza para activar el CDP en una interfaz en particular.

En la versión 10.3 o superior del Cisco IOS, el CDP se activa de manera automática en todas las interfaces soportadas para enviar y recibir información de CDP. El CDP podría activarse en cada una de las interfaces de los dispositivos utilizando el comando **cdp enable**.

4.1.4 Creación de un mapa de red del entorno

El CDP se diseñó e implementó como un protocolo sencillo, de baja carga general. Aunque una trama CDP puede ser pequeña, puede recuperar una gran cantidad de información útil sobre los dispositivos Cisco vecinos conectados.



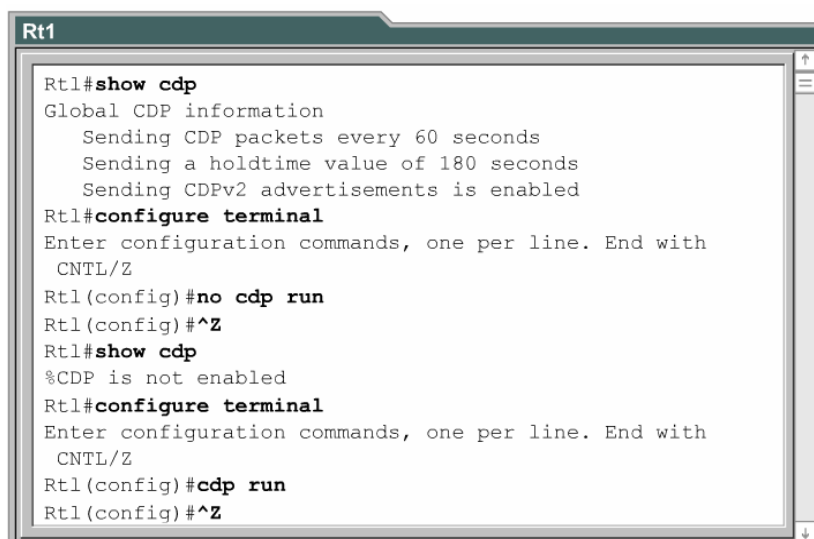
```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform Port ID
Rt3      Ser0/1      152    R      2500      Ser1
Rt1      Ser0/0      121    R      2620      Ser0/0
Rt2#
```

Esta información puede utilizarse para crear un mapa de red de los dispositivos conectados. Los dispositivos conectados a los dispositivos vecinos pueden detectarse al usar Telnet para conectarse con ellos, y con el comando **show cdp neighbors** para detectar cuáles dispositivos se encuentran conectados a esos vecinos.

4.1.5 Desactivación del CDP

Para desactivar el CDP a nivel global, utilice el comando **no CDP run** en el modo de configuración global. ¹ Si se desactiva el CDP de forma global, no es posible activar las interfaces individuales para CDP.



```
Rt1#show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rt1(config)#no cdp run
Rt1(config)#^Z
Rt1#show cdp
%CDP is not enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rt1(config)#cdp run
Rt1(config)#^Z
```

Figura 1

En la versión 10.3 o superior del Cisco IOS, el CDP se activa automáticamente en todas las interfaces soportadas para enviar y recibir información CDP. Sin embargo, en algunas interfaces, tales como las asíncronas, el CDP se desactiva de forma automática. Si el CDP se encuentra desactivado utilice el comando **CDP enable** en el modo de configuración de interfaz. Para desactivar el CDP en una interfaz

específica después de haberlo activado, utilice el comando **no CDP enable** en el modo de configuración de interfaz.

4.1.6 Diagnóstico de fallas en el CDP

Los siguientes comandos pueden utilizarse para mostrar la versión, la información de actualización, las tablas y el tráfico: 1

Comando	Descripción
<code>clear cdp table</code>	Elimina la tabla CDP de información de los vecinos.
<code>clear cdp counters</code>	Restaura los contadores de tráfico a cero.
<code>show cdp traffic</code>	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos y los errores de checksum.
<code>show debugging</code>	Muestra información acerca de los tipos de debugging que están habilitados
<code>debug cdp adjacency</code>	Información de vecinos CDP
<code>debug cdp events</code>	Eventos CDP
<code>debug cdp ip</code>	Información CDP IP
<code>debug cdp packets</code>	CDP packet-related information
<code>cdp timer</code>	Especifica la frecuencia con que el software Cisco IOS envía actualizaciones CDP.
<code>cdp holdtime</code>	Especifica el tiempo de espera que se enviará en el paquete de actualización CDP.
<code>show cdp</code>	Muestra información global de CDP, incluyendo la información de temporizador y tiempo de espera.

Figura 1

- `clear cdp table`
- `clear cdp counters`
- `show cdp traffic` 2
- `show debugging`
- `debug cdp adjacency`
- `debug cdp events`
- `debug cdp ip`
- `debug cdp packets`
- `cdp timer`
- `cdp holdtime`
- `show cdp`

```

Rt2
Rt2#show cdp traffic
CDP counters:
  Total packets output: 526, Input: 323
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 168, Input: 153
  CDP version 2 advertisements output: 358, Input: 170
  
```

Figura 2

4.2 Información sobre los dispositivos remotos

4.2.1 Telnet

Telnet es un protocolo de terminal virtual que forma parte del conjunto de protocolos TCP/IP. Permite realizar conexiones a los hosts remotos. Telnet brinda la capacidad de una terminal de red o una conexión remota. Telnet es un comando IOS EXEC que se utiliza para verificar el software de capa de aplicación entre el origen y destino. Constituye el mecanismo de prueba más completo disponible.

Telnet funciona en la capa de aplicación del modelo OSI. ¹Telnet depende de TCP para garantizar la entrega correcta y ordenada de datos entre el cliente y el servidor.

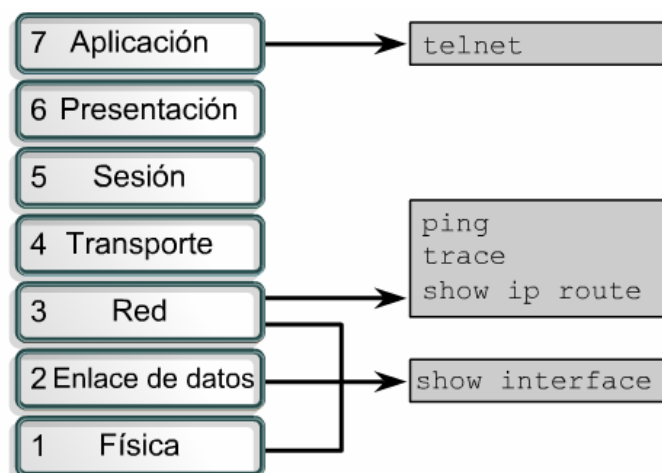


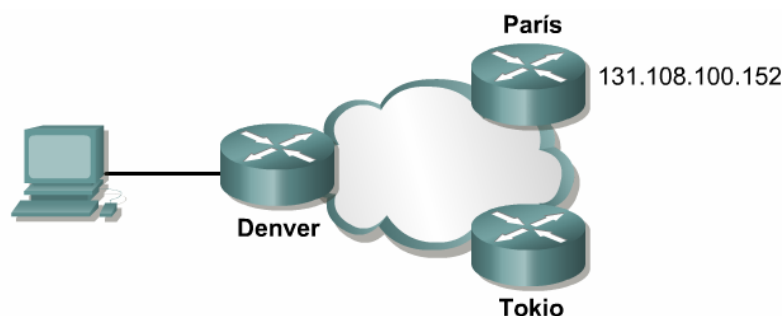
Figura 1

Un router puede tener varias sesiones Telnet entrantes de forma simultánea. Se utiliza el rango cero a cuatro para especificar cinco líneas VTY o de Telnet. Estas cinco sesiones Telnet entrantes pueden ocurrir a la vez.

Cabe destacar que verificar la conectividad de la capa de aplicación es un subproducto de Telnet. El uso principal de Telnet consiste en la conexión remota a dispositivos de red. Telnet es un programa de aplicación universal y simple.

4.2.2 Establecer y verificar una conexión Telnet

El comando Telnet IOS EXEC le permite al usuario establecer una sesión Telnet de un dispositivo Cisco a otro. Con la implementación de TCP/IP de Cisco, no es necesario ingresar el comando **connect** o **telnet** para establecer una conexión Telnet. Puede ingresarse el nombre del host o la dirección IP del router remoto. Para finalizar una sesión Telnet, use los comandos EXEC **exit** o **logout**. ¹



```
Initiate a session:
Denver>telnet paris

Exit a session:
Paris>exit
```

Figura 1

Para iniciar una sesión Telnet es posible utilizar cualquiera de las siguientes alternativas:

```
Denver>connect paris
Denver>paris
Denver>131.108.100.152
Denver>telnet paris
```

Para que un nombre funcione, debe haber una tabla de nombre de host o acceso a DNS. De otra forma, se debe ingresar la dirección IP del router remoto.

Es posible usar Telnet para realizar una prueba para determinar si se puede o no acceder a un router remoto. Como lo indica la Figura 2, si se puede establecer una sesión Telnet de forma exitosa para conectar el router York al París, entonces una prueba básica de la conexión en red se ha realizado con éxito. Esta operación puede realizarse en los niveles EXEC usuario o privilegiado.

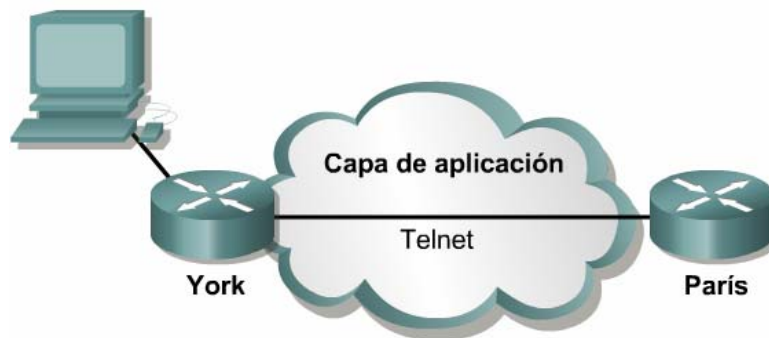


Figura 2

Si el acceso remoto puede lograrse por medio de otro router, entonces al menos una aplicación TCP/IP puede llegar al router remoto. Una conexión Telnet exitosa indica que la aplicación de las capas superiores funciona correctamente.

Si es posible establecer una sesión Telnet a un router, pero no es posible establecerla a otro router, es probable que existan problemas en el direccionamiento, denominación o permiso de acceso específicos que han causado la falla de Telnet. Es posible que el problema exista en ese router o en el router que falló como objetivo de Telnet. En este caso, el próximo paso es intentar **ping**, como se estudiará más adelante en esta lección. El uso de **ping** permite la prueba de conexiones de extremo a extremo en la capa de la red.

Una vez completado el Telnet, termine la sesión en el host. La conexión Telnet finalizará por defecto después de diez minutos de inactividad o cuando se ingrese el comando **exit** en la petición de entrada EXEC.

4.2.3 Desconexión y suspensión de las sesiones Telnet

Una función importante del comando Telnet es la capacidad de suspenderlo. Sin embargo, un problema potencial surge cuando una sesión Telnet queda suspendida y se presiona la tecla **Intro**. Esta tecla le indica al software Cisco IOS que reanude la conexión a la última conexión Telnet suspendida. Se utiliza con frecuencia la tecla **Intro**. Por lo tanto, cuando una sesión Telnet queda suspendida, es posible reconectarse a otro router inadvertidamente. Esto implica ciertos riesgos a la hora de realizar cambios a la configuración o utilizar comandos EXEC. Siempre ponga atención especial en qué router se está utilizando al suspender una sesión Telnet.

Una sesión queda suspendida por un tiempo limitado; para reanudar la sesión Telnet que se encuentra suspendida, sólo hay que presionar **Intro**. El comando **show sessions** mostrará las sesiones Telnet que están activas.

El procedimiento para desconectar una sesión Telnet es el siguiente:

- Introduzca el comando **disconnect**
- Siga el comando con el nombre o dirección IP del router. Ejemplo:

```
Denver>disconnect paris
```

El procedimiento para suspender una sesión Telnet es el siguiente:

- Presione **Ctrl-Shift-6**, luego **x**
- Introduzca el nombre del router o la dirección IP

Iniciar una sesión

```
Denver>telnet paris
```

Finalizar una sesión

```
Paris>exit
```

Suspender una sesión

```
Paris><Ctrl><Shift><6><x>
Denver>
```

Reanudar una sesión

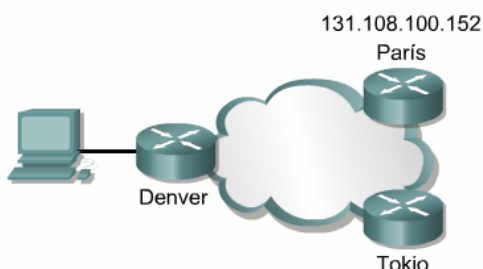
```
Denver><Return>
```

Desconectar una sesión

```
Denver>disconnect paris
```

Ver sesión

```
Denver#show sessions
Conn  Host      Address          Idle  Conn Name
 1      Paris    131.108.100.152   0      Paris
 2      Tokyo    126.102.57.63    0      Tokyo
```



4.2.4 Operaciones Telnet avanzadas

Puede haber varias sesiones Telnet abiertas de forma simultánea. El usuario puede alternar entre estas sesiones. El número de sesiones abiertas que se permiten a la vez se define con el comando **session limit**. Para alternar entre sesiones al abandonar una sesión y reanudar una abierta previamente, utilice los comandos indicados en la Figura 1.

Comando	Propósito
Ctrl-Shift-6 then x	Abandona la conexión actual y vuelve al símbolo EXEC
Resume	Realiza la conexión

Figura 1

Una nueva conexión puede iniciarse desde la petición de entrada EXEC. Los routers de la serie 2500 tienen un límite de 5 sesiones. Los routers series 2600 y 1700 tiene un límite predeterminado de 5 sesiones.

```
Router
Denver>telnet Paris
Trying Paris (131.108.100.152)...Open
User Access Verification
Password: xxxxx
Paris> (User pressed Ctrl-Shift- 6, then x)
Denver>telnet Tokyo
Trying Tokyo (127.102.57.63)...Open
User Access Verification
Password: xxxxx
Tokyo> (User pressed Ctrl-Shift-6, then x)
Denver>show sessions
Conn Host Address          Idle  Conn Name
 1  131.108.100.152    0      Paris
 2  127.102.57.63     0      Tokyo
```

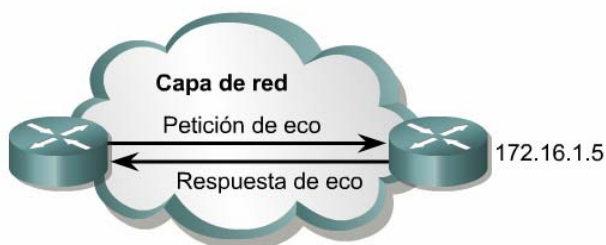
Figura 2

Varias sesiones Telnet pueden utilizarse y suspenderse por medio de la secuencia de teclas **Ctrl-Shift-6**, y luego **x**. La sesión puede reanudarse presionando la tecla **Intro**. Si se utiliza la tecla **Intro**, el software Cisco IOS reanuda la conexión a la última conexión Telnet suspendida. Si se utiliza el comando **resume**, se requiere una identificación de conexión. La identificación de conexión se muestra al utilizar el comando **show sessions**. ²

4.2.5 Pruebas alternativas de conectividad

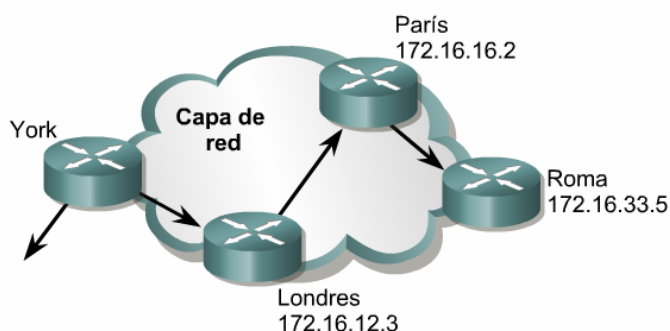
Como ayuda para diagnosticar la conectividad básica de red, muchos protocolos de red admiten un protocolo de eco. Los protocolos de eco se utilizan para verificar el enrutamiento de los paquetes de protocolo. El comando **ping** envía un paquete al host destino y luego espera un paquete de respuesta de ese host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de ruta a host, las demoras en la ruta y si se puede acceder al host, o si éste está funcionando. Este es un mecanismo de prueba básico. Esta operación puede realizarse en los niveles EXEC usuario o privilegiado.

El objetivo de ping 172.16.1.5 de la Figura 1 responde de forma exitosa a los cinco datagramas enviados. Los signos de exclamación (!) indican cada eco exitoso. Si se visualizan uno o más puntos (.) en lugar de signos de exclamación, significa que se venció el tiempo de espera de la aplicación en el router mientras esperaba un eco de paquete proveniente del objetivo de ping. El comando EXEC de usuario **ping** puede utilizarse para diagnosticar la conectividad básica de la red. El comando **ping** usa ICMP (Protocolo de mensajes de control en Internet).



```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Figura 1



```
York#traceroute ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
 1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
 2 PARIS (172.16.16.2) 8 msec 8msec 8msec
 3 ROME (172.16.33.5) 8msec 8msec 4msec
York#
```

Figura 2

El comando **tracert** es la herramienta ideal para descubrir dónde se envían los datos en una red. El comando **tracert** es similar al comando **ping**, salvo que en lugar de probar la conectividad de extremo a extremo, **tracert** verifica cada paso en el proceso. Esta operación puede realizarse en los niveles EXEC usuario o privilegiado.

En este ejemplo, se rastrea la ruta de York a Roma. La ruta también debe pasar por Londres y París. Si no es posible llegar a alguno de estos routers, se devolverán tres asteriscos (*) en lugar del nombre del router. El comando **tracert** seguirá intentando alcanzar el siguiente paso hasta que se utilice la secuencia de escape **Ctrl-Shift-6**. [2](#)

Una prueba básica de verificación también se concentra en la capa de red. Utilice el comando **show ip route** para determinar si existe una entrada en la tabla de enrutamiento para la red objetivo. Este comando se estudiará con mayor detalle en un módulo posterior de este curso.

El procedimiento para utilizar el comando **ping** es el siguiente:

- **ping** dirección IP o nombre del destino
- Presione la tecla **Intro**

El procedimiento para utilizar el comando **tracert** es el siguiente:

- **tracert** dirección IP o nombre del destino.
- Presione la tecla **Intro**

4.2.6 Diagnóstico de fallas en las cuestiones de direccionamiento IP

Los problemas de direccionamiento son los problemas más comunes que surgen en las redes IP. Los siguientes tres comandos se utilizan para realizar el diagnóstico de fallas relacionado con las direcciones:

- **ping** utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección IP de la capa de red. Este es un mecanismo de prueba básico.
- **telnet** verifica el software de capa de aplicación entre las estaciones origen y destino. Constituye el mecanismo de prueba más completo disponible.
- **tracert** permite la localización de fallas en la ruta desde el origen hasta el destino. **Trace** utiliza los valores de tiempo de existencia para generar mensajes desde cada router que se encuentra a lo largo de la ruta.

Resumen

Se debe haber logrado una comprensión de los siguientes puntos clave:

- Activación y desactivación del CDP
- Uso del comando **show cdp neighbors**
- Cómo determinar cuáles dispositivos vecinos están conectados a cuáles interfaces locales
- Uso del CDP para recaudar información de las direcciones de red de los dispositivos vecinos
- Cómo establecer una conexión Telnet
- Verificación de una conexión Telnet
- Desconexión de la sesión Telnet
- Suspensión de una sesión Telnet
- Realización de pruebas alternativas de conectividad
- Diagnóstico de fallas de las conexiones de terminales remotas

Módulo 5: Administración del software Cisco IOS

Descripción general

Un router Cisco no puede funcionar sin el sistema operativo de internetworking de Cisco (IOS). Cada router Cisco tiene una secuencia de arranque predeterminada, para ubicar y cargar el IOS. Este módulo describe las etapas y la importancia de dicha secuencia de arranque.

Los dispositivos de internetworking de Cisco requieren del uso de varios archivos para su funcionamiento. Estos incluyen las imágenes del sistema operativo de internetworking de Cisco (IOS) y los archivos de configuración. Un administrador que desee mantener una operación confiable y sin interrupciones de su red, debe poner mucha atención a estos archivos, para garantizar que se usen las versiones adecuadas y que se creen todas las copias de respaldo que sean necesarias. Este módulo también describe el sistema de archivos de Cisco y suministra herramientas para su administración eficiente.

Los estudiantes que completen este módulo deberán ser capaces de:

- Identificar las etapas de la secuencia de arranque del router
- Determinar cómo el dispositivo ubica y carga el software Cisco IOS
- Usar los comandos boot system
- Identificar los valores del registro de configuración
- Describir brevemente los archivos que usa el Cisco IOS y sus funciones
- Hacer una lista de la ubicación de los distintos tipos de archivos en el router
- Describir brevemente las partes del nombre del IOS
- Guardar y restaurar archivos de configuración mediante TFTP y mediante copiar y pegar
- Cargar una imagen del IOS mediante TFTP
- Cargar una imagen del IOS mediante XModem
- Verificar el sistema de archivos mediante los comandos show

5.1 Secuencia de arranque del router y su verificación

5.1.1 Etapas de la secuencia de arranque del router

El objetivo de las rutinas de arranque del software Cisco IOS es activar el funcionamiento del router. El router debe proveer un rendimiento confiable en lo que respecta a sus funciones de interconexión de redes. Para lograrlo, las rutinas de inicio deben efectuar lo siguiente:

- Comprobar el hardware del router.
- Encontrar y cargar el software Cisco IOS.
- Encontrar y ejecutar los comandos de configuración, que abarcan las funciones de protocolo y las direcciones de las interfaces.

La Figura 1 ilustra la secuencia y los servicios empleados para inicializar el router.

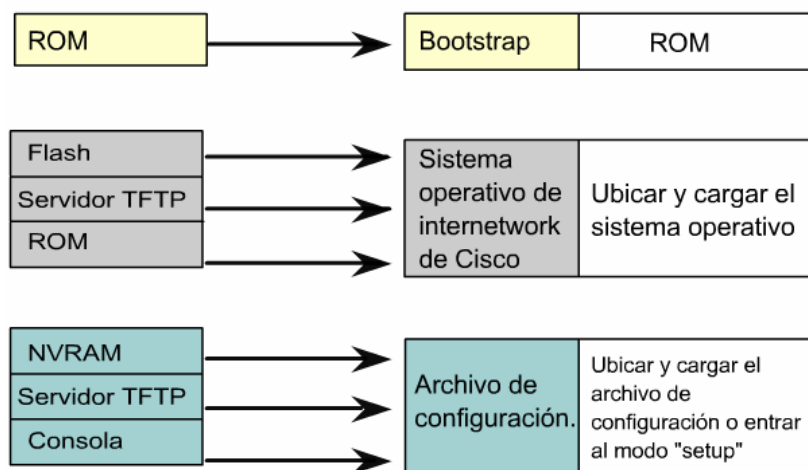


Figura 1

5.1.2 Mecanismo de ubicación y carga del software Cisco IOS

La fuente predefinida del Cisco IOS depende de la plataforma de hardware, pero por lo general el router busca los comandos boot system almacenados en la NVRAM. El Cisco IOS permite varias alternativas. Se puede especificar otras fuentes del software, o el router puede usar su propia secuencia de reserva o alterna para cargarlo. ¹

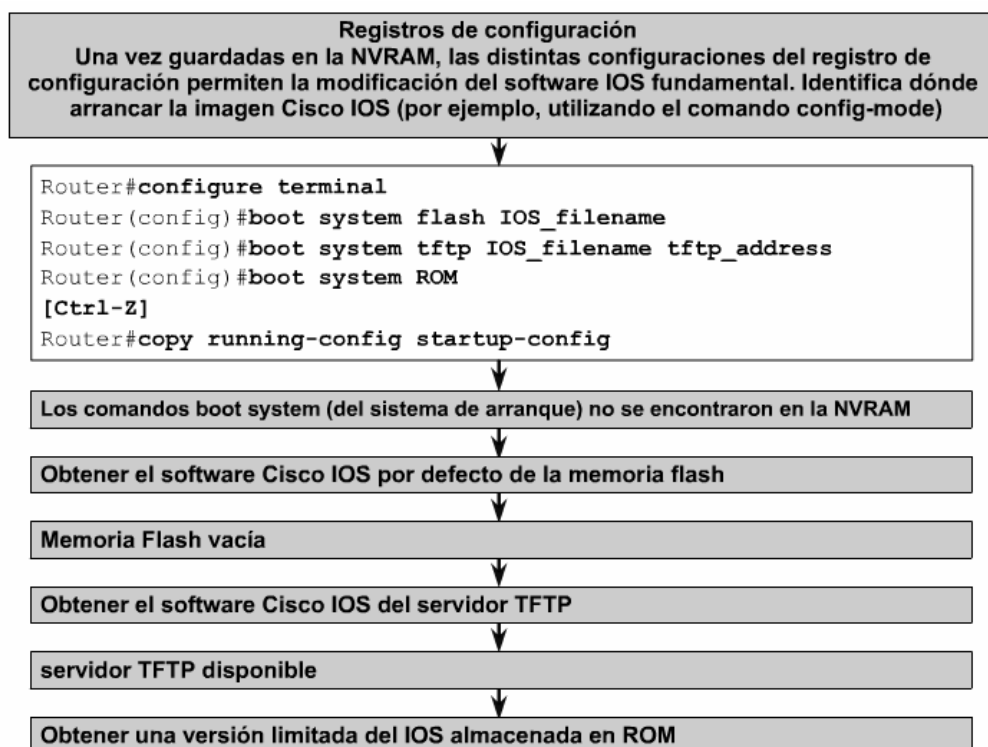


Figura 1

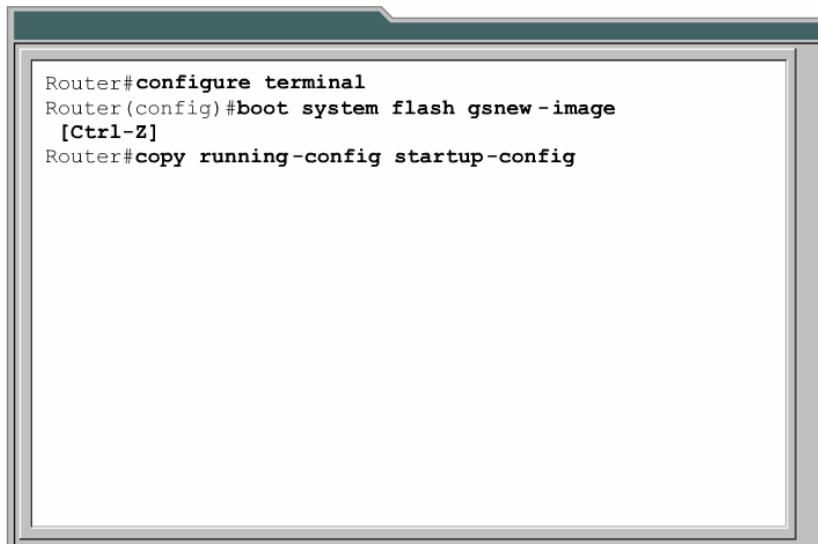
Los valores particulares del registro de configuración permiten las alternativas siguientes.

- Se puede especificar comandos boot system del modo de configuración global para introducir fuentes de reserva, a fin de que el router las utilice en forma secuencial. El router utiliza estos comandos según sea necesario, en forma secuencial, cuando arranca de nuevo.
- Si el router no encuentra comandos boot system en la NVRAM, el sistema, por defecto, usa el Cisco IOS que se encuentra en la memoria flash.
- Si no hay un servidor TFTP disponible, el router cargará una versión limitada del IOS almacenada en ROM.

5.1.3 Uso de los comandos boot system

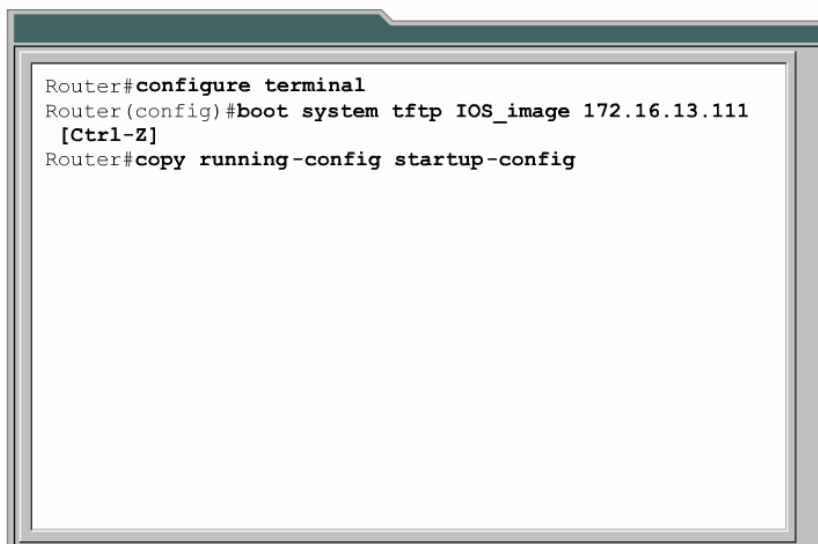
Los siguientes ejemplos muestran el uso de diversos comandos boot system, los cuales especifican la secuencia de reserva o alterna para el arranque del Cisco IOS. Los tres ejemplos muestran valores del boot system los cuales especifican que la imagen del Cisco IOS sea cargada en primer lugar desde la memoria flash, luego desde un servidor de red y, por último, desde la ROM:

- **Memoria flash:** Se puede cargar una imagen del sistema desde la memoria flash. Tiene la ventaja de que la información en la memoria flash no se ve afectada por fallas en la red, las cuales sí afectan la carga de imágenes del sistema desde servidores TFTP. ¹
- **Servidor de red:** En caso de que el contenido de la memoria flash esté dañado, se puede cargar una imagen del sistema desde un servidor TFTP. ²
- **ROM:** Si la memoria flash está dañada y tampoco se puede cargar la imagen desde un servidor, la opción final programada es arrancar desde la ROM. Sin embargo, es probable que la imagen del sistema en la ROM sea sólo una porción del software Cisco IOS, y que no incluya los protocolos, las funciones y las configuraciones del Cisco IOS completo. Además, si el software se ha actualizado desde que se adquirió el router, la versión en la ROM puede ser más antigua. ³

A terminal window with a dark green header bar. The text inside shows the configuration steps for booting from flash.

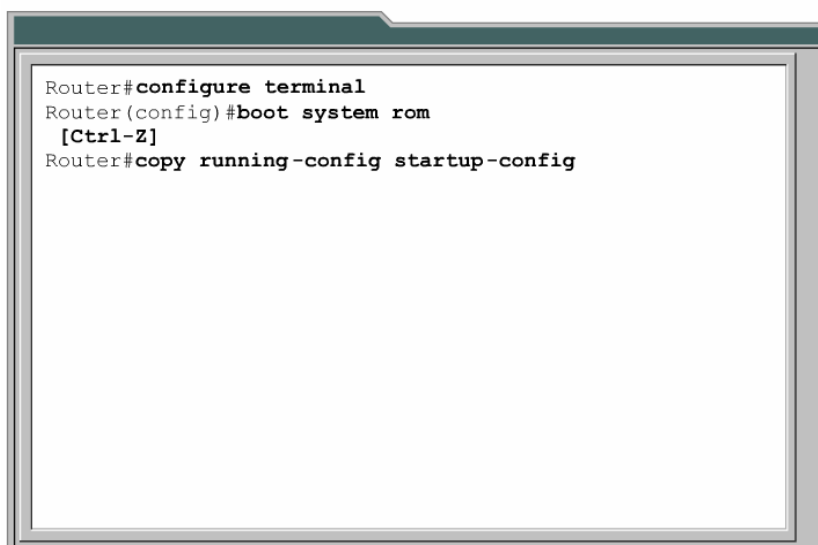
```
Router#configure terminal
Router(config)#boot system flash gsnew-image
[Ctrl-Z]
Router#copy running-config startup-config
```

Figura 1

A terminal window with a dark green header bar. The text inside shows the configuration steps for booting from a tftp server.

```
Router#configure terminal
Router(config)#boot system tftp IOS_image 172.16.13.111
[Ctrl-Z]
Router#copy running-config startup-config
```

Figura 2

A terminal window with a dark green header bar. The text inside shows the configuration steps for booting from ROM.

```
Router#configure terminal
Router(config)#boot system rom
[Ctrl-Z]
Router#copy running-config startup-config
```

Figura 3

El comando **copy running-config startup-config** guarda los comandos en la NVRAM. El router ejecutará los comandos boot system según lo requiera, en el orden en el que se introdujeron originalmente al hacer la configuración.

5.1.4 Registro de configuración

El valor del campo de arranque del registro de configuración determina el orden en el cual el router busca la información de arranque del sistema. Los valores por defecto del registro de configuración se pueden cambiar con el comando **config-register** del modo de configuración global. El argumento de este comando es un número hexadecimal.

El registro de configuración en la NVRAM es de 16 bits. Sus cuatro bits inferiores (un dígito hexadecimal) conforman el campo de arranque. Para garantizar que el valor de los 12 bits superiores se conserve, primero debe recuperarse el valor en uso del registro de configuración, mediante el comando **show version**. Luego ejecute el comando **config-register**, con las modificaciones del valor del último dígito hexadecimal.

Valor	Descripción
0xnnn0	Usar el modo de monitoreo de ROM (arranca manualmente utilizando el comando)
0xnnn1	Carga la primera imagen en Flash. Sin embargo, en plataformas previas cargará una versión limitada del IOS grabada en memoria ROM.
De 0xnnn2 a 0xnnnF	Examinar la NVRAM para los comandos del sistema de arranque (0xnnn2 es la opción por defecto si el router tiene Flash)

Figura 1

Para cambiar el campo de arranque del registro de configuración, siga estas pautas: ¹

- Para ingresar al modo de monitor de la ROM, fije 0xnnn0 como el valor del registro de configuración, donde *nnn* representa el valor anterior de los dígitos del campo diferentes al de arranque. Este valor fija los bits del campo de arranque en 0000 binario. Arranque el sistema operativo manualmente. Para ello ejecute el comando **b** al estar en pantalla el indicador del modo monitor de la ROM.
- Para arrancar usando la primera imagen en memoria Flash, o para arrancar usando el IOS en memoria ROM (dependiendo de la plataforma), fije el registro de configuración en 0xnnn1, donde *nnn* representa el valor anterior de los dígitos del campo diferentes al de arranque. Este valor fija los bits del campo de arranque en 0001 binario. Plataformas previas, como los routers Cisco 1600 y 2500, arrancan usando una versión limitada del IOS ubicada en ROM. Plataformas mas recientes, como los Cisco 1700, 2600 y enrutadores de alta capacidad arrancarán usando la primera imagen en memoria Flash.
- Para configurar el sistema de modo que arranque automáticamente desde la NVRAM, fije el registro de configuración en cualquier valor entre 0xnnn2 y 0xnnnF, donde *nnn* representa el valor anterior de los dígitos del campo diferentes al de arranque. Estos valores fijan los bits del campo de arranque en un valor comprendido entre 0010 y 1111 binario. El uso de los comandos boot system almacenados en la NVRAM es el esquema por defecto.

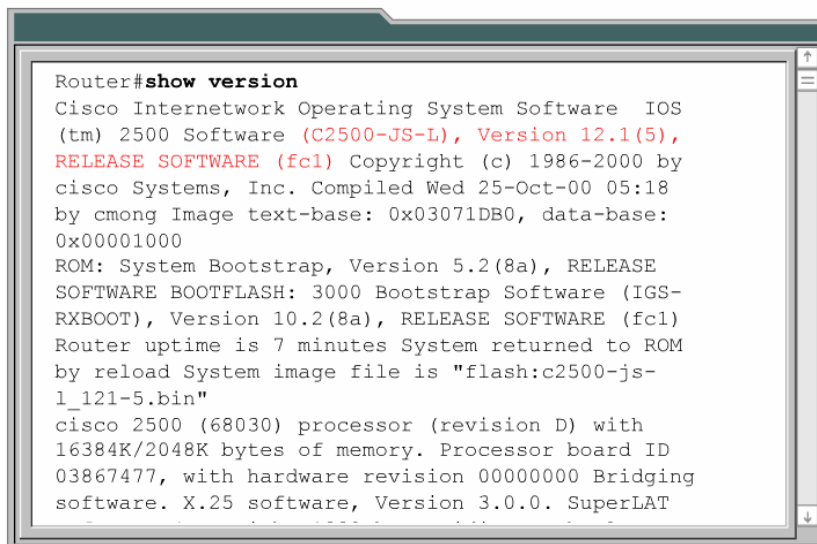
5.1.5 Diagnóstico de fallas en el arranque del Cisco IOS

Si el router no arranca correctamente, eso puede deberse a fallas en alguno de estos elementos:

- El archivo de configuración incluye comandos **boot system** incorrectos
- El valor del registro de configuración es erróneo
- La imagen en la flash está dañada
- Hay una falla de hardware

En el arranque, el router busca comandos **boot system** en el archivo de configuración. Los comandos **boot system** pueden forzar el arranque del router desde una imagen del IOS diferente a la que está en la flash.

Para identificar la fuente de la imagen de arranque, ejecute el comando **show version** y busque la línea que identifica la fuente. ¹



```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.1(5),
RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18
by cmong Image text-base: 0x03071DB0, data-base:
0x00001000
ROM: System Bootstrap, Version 5.2(8a), RELEASE
SOFTWARE BOOTFLASH: 3000 Bootstrap Software (IGS-
RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)
Router uptime is 7 minutes System returned to ROM
by reload System image file is "flash:c2500-js-
l_121-5.bin"
cisco 2500 (68030) processor (revision D) with
16384K/2048K bytes of memory. Processor board ID
03867477, with hardware revision 00000000 Bridging
software. X.25 software, Version 3.0.0. SuperLAT
```

Figura 1

Ejecute el comando **show running-config** y busque el comando **boot system** cerca de la parte superior de la configuración. Si el comando **boot system** señala una imagen del IOS incorrecta, elimine el comando mediante la versión "no" de dicho comando.

Un valor erróneo del registro de configuración evita que el IOS se cargue desde la flash. El valor del registro de configuración le indica al router la fuente del IOS. Esto se puede confirmar al ejecutar el comando **show version**. Busque en la última línea el registro de configuración. El valor correcto varía de una plataforma de hardware a otra. Una de las partes de la documentación de la red debe ser una copia impresa del resultado de **show version**. Si dicha documentación no está disponible, en el CD de documentación de Cisco o en el sitio Web de Cisco se proveen recursos para identificar el valor correcto del registro de configuración. Para hacer correcciones, se debe cambiar el registro de configuración en la configuración, para luego guardarla como la configuración de arranque.

Si la falla continua, es posible que el archivo de imagen en la flash esté dañado. Si ese es el caso, debe aparecer un mensaje de error durante el arranque. El mensaje puede tener diversas formas. A continuación se indican algunos ejemplos:

- open: read error...requested 0x4 bytes, got 0x0 (error de lectura)
- trouble reading device magic number (problemas al leer el número mágico del dispositivo)
- boot: cannot open "flash:" (no se puede abrir la "flash:")
- boot: cannot determine first file name on device "flash:" (no se puede determinar el nombre del primer archivo del dispositivo "flash:")

Si la imagen en la flash está dañada, se debe cargar un nuevo IOS en el router.

Si ninguno de los ejemplos anteriores parece ser el problema, es posible que se haya producido una falla de hardware en el router. Si este es el caso, debe comunicarse con el centro de asistencia técnica (TAC) de Cisco. Aunque las fallas de hardware son inusuales, a veces ocurren.

NOTA:

El valor del registro de configuración no se muestra mediante los comandos **show running-config** o **show startup-config**.

5.2 Administración del sistema de archivos de Cisco

5.2.1 Descripción general del sistema de archivos del IOS

Los routers y los switches dependen de software para su funcionamiento. Se requiere de dos tipos de software: los sistemas operativos y los archivos de configuración.

En la mayoría de los dispositivos de Cisco se usa el sistema operativo de internetworking (IOS) de Cisco. El Cisco IOS® es el software que permite que el hardware funcione como un router o un switch. El archivo del IOS es de varios megabytes.

El otro software utilizado por los routers o switches se denomina archivo de configuración o archivo config. La configuración contiene las "instrucciones" que determinan cómo el dispositivo debe enrutar o conmutar. El administrador de red crea una configuración que define la funcionalidad deseada para el dispositivo de Cisco. Las funciones que se pueden especificar en el archivo de configuración son las direcciones de IP de las interfaces, los protocolos de enrutamiento y las redes que serán publicadas. Generalmente, el archivo de configuración es de unos pocos cientos o miles de bytes.

Ambos componentes de software se guardan en la memoria como archivos individuales. Estos archivos también se guardan en distintos tipos de memoria. ¹

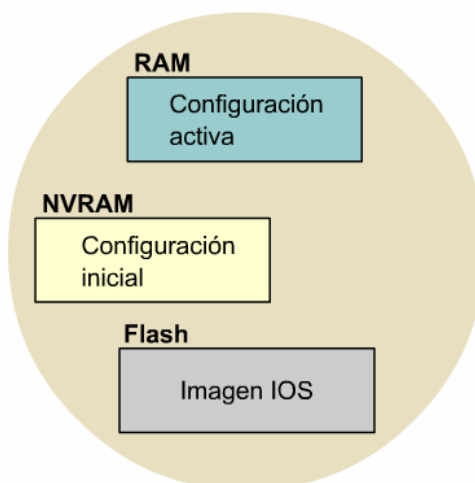


Figura 1

El IOS se guarda en un área denominada memoria flash. La memoria flash provee almacenamiento no volátil de una imagen del IOS, la cual se puede usar como sistema operativo en el arranque. El uso de memoria flash permite la actualización del IOS, y también guardar múltiples IOS. En muchas arquitecturas de router, el IOS es copiado a la memoria RAM y se ejecuta desde allí.

Una copia del archivo de configuración se guarda en la RAM no volátil (NVRAM), para ser utilizada como configuración en el arranque. A dicha copia se le denomina "startup config" o configuración de arranque. la configuración de arranque es copiada a la RAM durante el arranque. Una vez en la RAM, es la que se pone en uso para la operación del router. Se le denomina "running config" o configuración en uso.

Prefix	Descripción
bootflash:	Memoria Bootflash
flash:	Memoria flash. Este prefijo está disponible en todas las plataformas. Para plataformas que no tienen un dispositivo denominado flash, el prefijo flash: es referido como slot0:. Así, el prefijo flash: puede usarse para referir al área de almacenamiento de memoria principal flash en todas las plataformas.
flh:	Archivos de bitácora de ayuda de carga de Flash
ftp:	Servidor de red del Protocolo de Transferencia de Archivos (FTP)
nvrn:	NVRAM
rcp:	Servidor de red del Protocolo de Copia Remota (RCP)
Slot0:	Primera tarjeta de memoria flash de la Asociación Internacional de Tarjetas de Memoria de Computadora Personal (PCMCIA)
Slot1:	Servidor de red del Protocolo de Copia Remota (RCP)
system:	Contiene la memoria del sistema, incluyendo la configuración activa
Tftp:	Servidor de red TFTP

Figura 2

A partir de la versión 12, el IOS provee una interfaz única a todos los sistemas de archivos que utiliza el router. A dicha interfaz se le denomina sistema de archivos del Cisco IOS (IFS). El IFS provee un método unificado para administrar el sistema de archivos que utilizan los routers. Esto incluye los sistemas de

archivos de la memoria flash, los sistemas de archivos de red (TFTP, rcp y FTP) y la lectura o escritura de datos (de o a la NVRAM, de la configuración en uso, de la ROM). El IFS usa un conjunto común de prefijos para especificar los dispositivos del sistema de archivos. ²

El IFS usa la convención URL para especificar archivos en los dispositivos de red y la red. La convención URL identifica la ubicación de los archivos de configuración mediante el esquema [[[//location]/directory]/filename], luego de dos puntos. El IFS también permite la transferencia de archivos mediante FTP.

5.2.2 Convenciones de nombres del software IOS de escritorio

Cisco desarrolla numerosas versiones del IOS. El IOS ofrece diversas funciones y también corre sobre diversas plataformas de hardware. Cisco desarrolla y lanza nuevas versiones del IOS en forma continua.

Cisco ha establecido una convención para identificar por nombres a las distintas versiones, de los archivos del IOS. La convención de nombres del IOS utiliza varios campos. Entre ellos podemos mencionar el de identificación de la plataforma del hardware, el de identificación de la funcionalidad y el correspondiente a la secuencia numérica. ¹

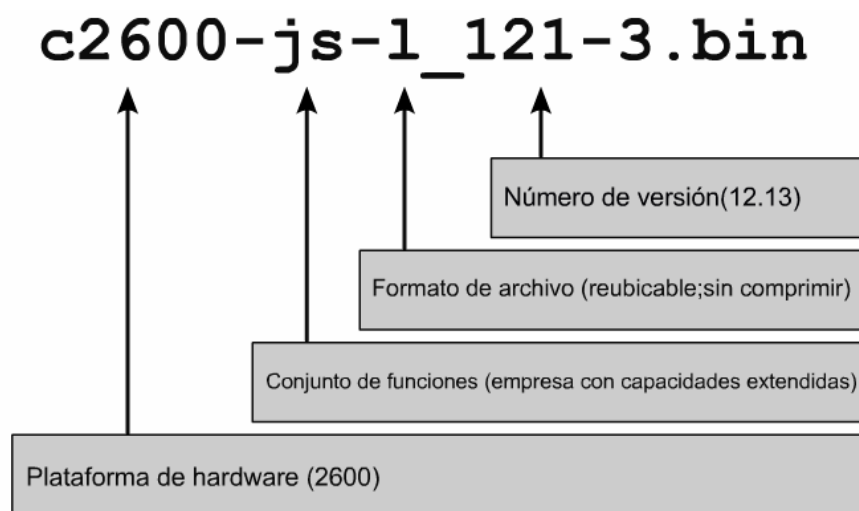


Figura 1

La primera parte del nombre del archivo del Cisco IOS identifica la plataforma de hardware para la cual ha sido desarrollado.

La segunda parte del nombre del archivo del IOS identifica las características funcionales que brinda dicho IOS. Existen numerosas características funcionales a elegir. Dichas características se agrupan en "imágenes de software". Cada grupo de funciones contiene un subconjunto específico de las funciones del software Cisco IOS. Los siguientes son ejemplos de categorías de funcionalidad:

- **Básica:** Un grupo de funciones básicas para una plataforma de hardware dada, por ejemplo, IP e IP/FW
- **Plus:** Un grupo de funciones básicas y otras funciones adicionales tales como IP Plus, IP/FW Plus y Enterprise Plus
- **Cifrado:** Añade la funcionalidad de cifrado de datos de 56 bits como la denominada Plus 56, a un conjunto de funciones Básicas o Plus. Unos ejemplos son IP/ATM PLUS IPSEC56 o Enterprise Plus 56. A partir de la Versión 12.2 de Cisco IOS en adelante, los identificadores de cifrado son k8 y k9:
- **k8:** cifrado de hasta 64 bits en la versión 12.2 del IOS y posteriores
- **k9:** cifrado de más de 64 bits, en la versión 12.2 y posteriores

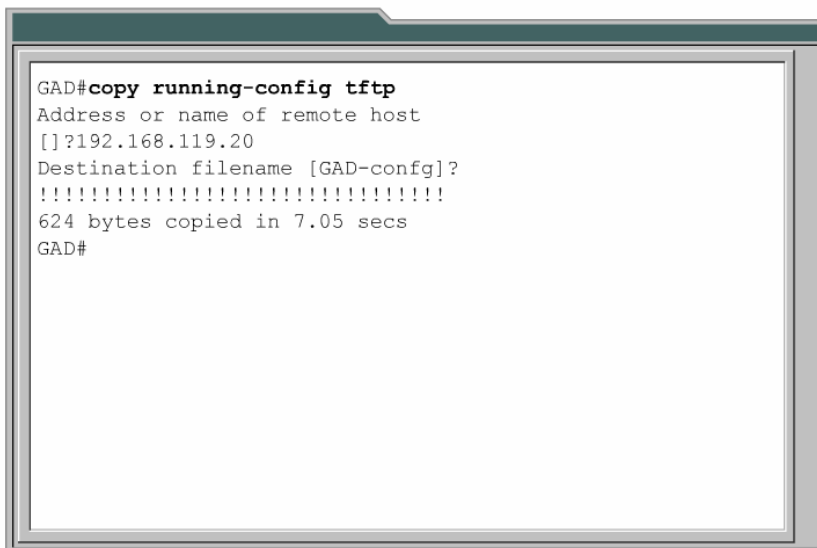
La tercera parte del nombre indica el formato del archivo. Indica si el IOS se almacena en la memoria flash en formato comprimido y si se puede reubicar. Si la imagen del IOS en la flash está comprimida, se debe descomprimir durante el arranque al copiarse en la RAM. Una imagen reubicable se puede copiar de la memoria flash a la RAM para ejecutarse desde allí. Una imagen no reubicable se ejecuta directamente desde la memoria flash.

La cuarta parte del nombre identifica numéricamente la versión del IOS. A medida que Cisco desarrolla versiones más recientes del IOS, el identificador numérico aumenta.

5.2.3 Administración de los archivos de configuración mediante TFTP

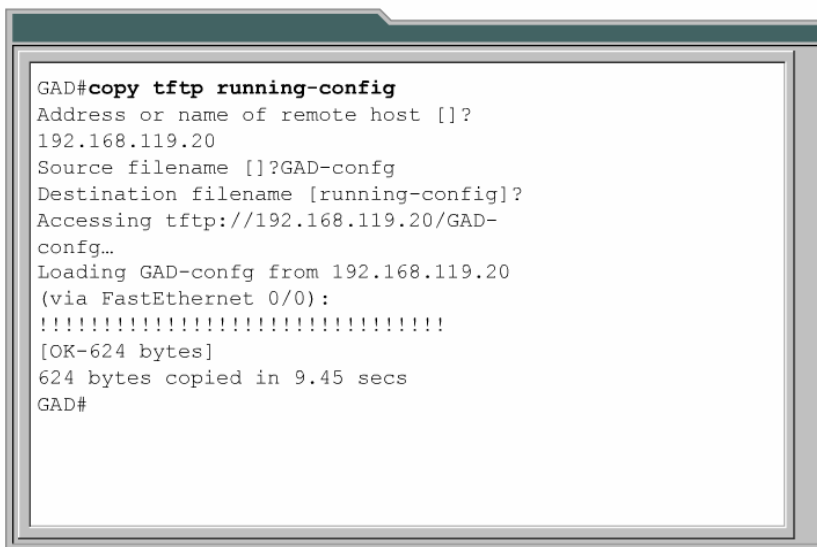
En un router o switch de Cisco, la configuración en uso se encuentra en la RAM y la ubicación por defecto de la configuración de arranque es la NVRAM. En caso de que la configuración se pierda, debe existir una copia de respaldo de la configuración de arranque. Se puede guardar una de estas copias de respaldo en un servidor TFTP. Para ello, se puede ejecutar el comando **copy running-config tftp**. ¹A continuación se da una lista de los pasos de este proceso:

- Ejecute el comando **copy running-config tftp**.
- Cuando aparezca el indicador, introduzca la dirección de IP del servidor TFTP en el cual se guardará el archivo de configuración.
- Introduzca el nombre a ser asignado al archivo de configuración o acepte el nombre por defecto.
- Confirme sus elecciones respondiendo 'yes' (sí) cada vez.



```
GAD#copy running-config tftp
Address or name of remote host
[]?192.168.119.20
Destination filename [GAD-config]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
624 bytes copied in 7.05 secs
GAD#
```

Figura 1



```
GAD#copy tftp running-config
Address or name of remote host []?
192.168.119.20
Source filename []?GAD-config
Destination filename [running-config]?
Accessing tftp://192.168.119.20/GAD-
config...
Loading GAD-config from 192.168.119.20
(via FastEthernet 0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK-624 bytes]
624 bytes copied in 9.45 secs
GAD#
```

Figura 2

Cargar el archivo de configuración de respaldo desde un servidor TFTP, puede servir para restaurar la configuración del router. ²Los pasos a continuación describen este proceso:

- Ejecute el comando **copy tftp running-config**.
- Cuando aparezca el indicador, seleccione un archivo de configuración de host o de red.
- Cuando aparezca el indicador del sistema, introduzca la dirección de IP del servidor TFTP en el que se encuentra el archivo de configuración.
- Cuando aparezca el indicador del sistema, introduzca el nombre del archivo de configuración o acepte el nombre por defecto.

- Confirme el nombre del archivo de configuración y la dirección del servidor que suministra el sistema.

5.2.4 Administración de los archivos de configuración mediante cortar y pegar

Otra forma de crear una copia de respaldo de la configuración es mediante la captura del resultado del comando **show running-config**. Esto puede hacerse desde una sesión de terminal, mediante la copia y pegado del resultado del comando en un archivo de texto, el cual se guarda luego. Será necesario editar este archivo antes de que se pueda usar para restaurar la configuración del router.

Ejecute los siguientes pasos para hacer un respaldo de la configuración mediante la captura del texto que se muestra en la pantalla de HyperTerminal:

1. Seleccione **Transfer** (Transferir).
2. Seleccione **Capture Text** (Captura de texto).
3. Indique el nombre del archivo de texto donde se hará la captura de la configuración.
4. Seleccione **Start** (Inicio) para empezar la captura del texto
5. Muestre en pantalla la configuración mediante **show running-config**
6. Presione la **barra espaciadora** cuando aparezca el indicador "-More -".
7. Una vez que se haya mostrado completamente la configuración, detenga la captura:
8. Seleccione **Transfer** (Transferir).
9. Seleccione **Capture Text** (Captura de texto).
10. Seleccione **Stop** (Detener).

Una vez que se haya completado la captura, se debe editar el archivo de configuración para eliminar textos superfluos. Para ello, elimine toda la información innecesaria de la configuración capturada, a fin de poder "pegarla" de vuelta en el router. Se puede agregar comentarios para explicar las diversas partes de la configuración. Una línea de comentario comienza con un signo de exclamación "!".

El archivo de configuración se puede editar con un editor de texto como, por ejemplo, el Notepad de Windows. Para editar el archivo con el Notepad, haga clic en **File > Open** (Archivo > Abrir). Busque el archivo de captura y selecciónelo. Haga clic en **Open** (Abrir).

Debe eliminarse las líneas que contienen:

- show running-config
- Building configuration...
- Current configuration:
- -More-
- Todas las líneas que aparecen después de la palabra "End".

Al final de cada una de las secciones relativas a las interfaces, agregue el comando **no shutdown**. Al ejecutar **File > Save** (Archivo > Guardar), se guardará la versión limpia de la configuración.

La copia de respaldo de la configuración se puede restaurar desde una sesión de HyperTerminal. Antes de restaurar la configuración, debe eliminarse toda configuración remanente en el router. Esto se hace mediante el comando **erase startup-config**, luego del indicador EXEC privilegiado, para luego arrancar el router mediante el comando **reload**.

Se puede usar HyperTerminal para restaurar la configuración. La versión limpia de la configuración puede copiarse de vuelta en el router.

- Ingrese al modo de configuración global del router.
- En HyperTerminal, haga clic en **Transfer > Send Text File** (Transferir>Enviar archivo de texto).
- Seleccione el nombre del archivo de la copia de respaldo de la configuración.
- Las líneas del archivo se introducirán en el router como si se estuviesen tecleando.
- Observe si ocurre algún error.
- Una vez que haya introducido la configuración, presione las teclas **Ctrl-Z** para salir del modo de configuración global.
- Restaure la configuración de arranque mediante **copy running-config startup-config**.

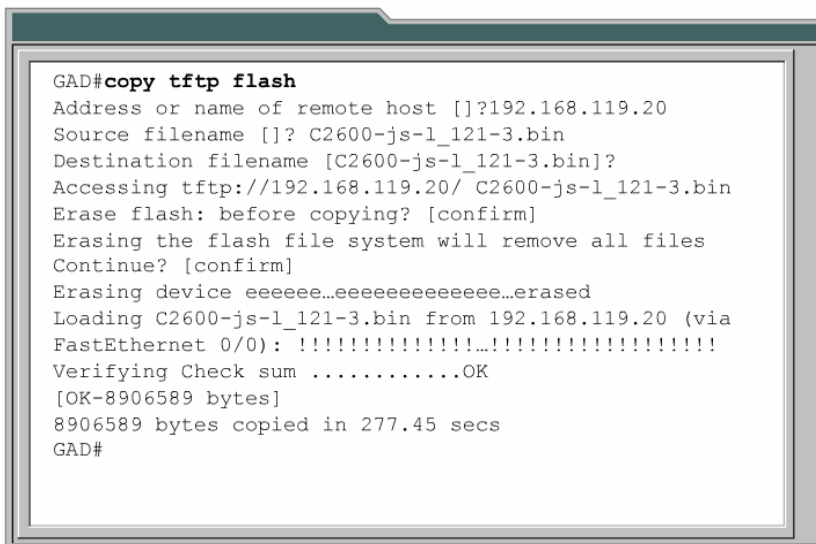
5.2.5 Administración de imágenes del IOS mediante TFTP

Ocasionalmente, es necesario actualizar o restaurar el IOS del router. Al recibir un router, se debe realizar una copia de respaldo del IOS. Esta imagen del IOS se puede guardar en un servidor central junto con otras

imágenes del IOS. Éstas se pueden usar para restaurar o actualizar el IOS de los routers y switches de la red.

Dicho servidor debe tener un servicio TFTP activo. El respaldo del IOS se puede iniciar desde el modo EXEC privilegiado, mediante el comando **copy flash tftp**.

Se puede recargar desde el servidor el IOS en su misma versión, o una superior, con el comando **copy tftp flash**. De nuevo, el router le solicitará al usuario que introduzca la dirección de IP del servidor TFTP. Cuando se le solicite el nombre de archivo de la imagen del IOS en el servidor, el router puede solicitar que se borre la memoria flash. Esto sucede a menudo cuando no hay suficiente memoria flash disponible para la nueva imagen. A medida que la imagen es borrada de la memoria flash, se mostrará una serie de "e's" que indican el avance del proceso. ¹



```
GAD#copy tftp flash
Address or name of remote host []?192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeeee.....erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying Check sum .....OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#
```

Figura 1

A medida que se descarga cada uno de los archivos de imagen del IOS, se mostrará un signo de exclamación "!". La imagen del IOS es de varios megabytes y su descarga puede tomar bastante tiempo. La nueva imagen en la flash se debe verificar luego de la descarga. Ahora el router está listo para ser cargado de nuevo, y para utilizar la nueva imagen del IOS.

5.2.6 Administración de imágenes del IOS mediante Xmodem

Si la imagen del IOS de la flash se ha borrado o dañado, es posible que se deba restaurar el IOS desde el modo de monitor de la ROM (ROMmon). En muchas de las arquitecturas de hardware de Cisco, el modo ROMmon se indica mediante el indicador rommon 1 >.

El primer paso de este proceso es determinar por qué la imagen del IOS no se cargó desde la flash. La causa puede ser una imagen dañada o ausente. La flash se debe examinar usando el comando **dir flash:**. Si la imagen que se ha ubicado parece ser válida, se debe intentar arrancar desde esa imagen. Esto se hace mediante el comando **boot flash:**. Por ejemplo, si el nombre de la imagen es "c2600-is-mz.121-5", el comando sería:

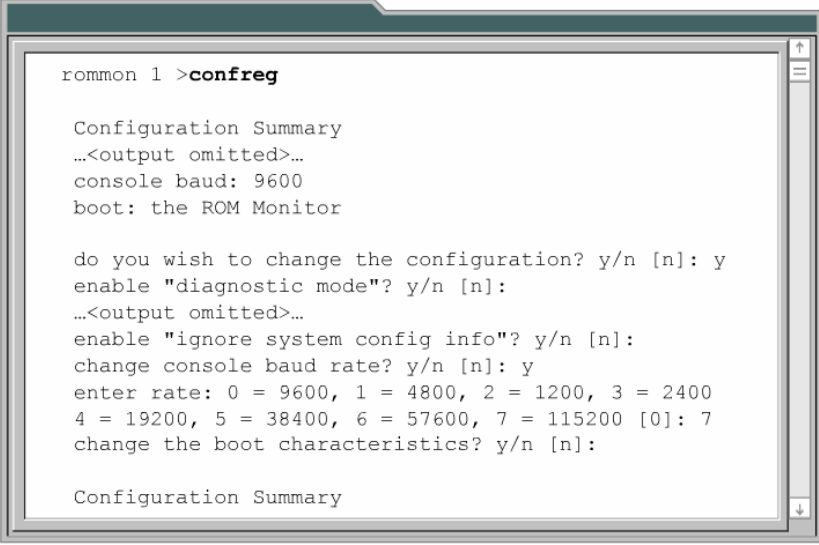
```
rommon 1>boot flash:c2600-is-mz.121-5
```

Si el router arranca correctamente, es necesario examinar varios elementos a fin de determinar por qué el router arrancó mediante ROMmon y no lo hizo automáticamente. En primer lugar, ejecute el comando **show version** para verificar el registro de configuración y asegurarse que esté configurado para la secuencia de arranque por defecto. Si el valor del registro de configuración es correcto, ejecute el comando **show startup-config** para ver si hay algún comando del sistema de arranque que le indique al router que debe usar el IOS del monitor de la ROM.

Si el router no arranca correctamente desde la imagen o si no existe ninguna imagen del IOS, es necesario descargar un nuevo IOS. El archivo del IOS se puede recuperar mediante Xmodem, para restaurar la imagen a través de la consola o mediante TFTP en el modo ROMmon.

Descarga mediante Xmodem en el modo ROMmon

Para restaurar el IOS a través de la consola, la PC local debe tener una copia del archivo del IOS a ser restaurado, y un programa de emulación de terminal como, por ejemplo, HyperTerminal. El IOS se puede restaurar a la velocidad por defecto de la consola, 9600 bps. Se puede cambiar a 115200 bps para agilizar la descarga. La velocidad de la consola se puede cambiar en el modo ROMmon, mediante el comando **confreg**. Al ejecutar el comando **confreg**, el router solicitará los diversos parámetros modificables. ¹



```
rommon 1 >confreg

Configuration Summary
...<output omitted>...
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
...<output omitted>...
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7
change the boot characteristics? y/n [n]:

Configuration Summary
```

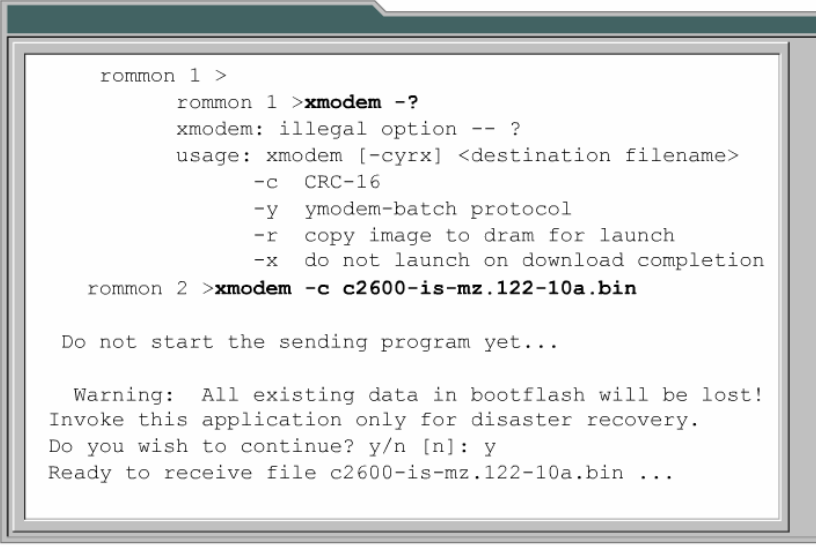
Figura 1

Cuando se le solicite "change console baud rate? y/n [n]:" si selecciona **y** aparecerá un indicador para seleccionar la nueva velocidad. Una vez que ha cambiado la velocidad de la consola y reiniciado el router en el modo ROMmon, se debe cerrar la vieja sesión (a 9600) e iniciar una nueva a 115200 bps, la nueva velocidad de la consola.

El comando Xmodem se puede ejecutar desde el modo ROMmon para restaurar la imagen del software IOS desde la PC. El formato del comando es **xmodem -nombre_del_archivo**. Por ejemplo, para restaurar un archivo de imagen del IOS de nombre "c2600-is-mz.122-10a.bin", ejecute el comando:

xmodem -c c2600-is-mz.122-10a.bin ²

La **-c** le indica al proceso Xmodem que debe usar Verificación de redundancia cíclica (CRC) para detectar errores durante la descarga.



```
rommon 1 >
rommon 1 >xmodem -?
xmodem: illegal option -- ?
usage: xmodem [-cyrx] <destination filename>
       -c CRC-16
       -y ymodem-batch protocol
       -r copy image to dram for launch
       -x do not launch on download completion
rommon 2 >xmodem -c c2600-is-mz.122-10a.bin

Do not start the sending program yet...

Warning: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y
Ready to receive file c2600-is-mz.122-10a.bin ...
```

Figura 2

El router no inicia la transferencia de inmediato, sino que le muestra un mensaje de advertencia. El mensaje le informa que la bootflash será borrada y le pregunta si desea continuar. Una vez que se acepta el continuar, el router le indica que puede iniciar la transferencia.

Ahora se requiere iniciar una transferencia Xmodem desde el emulador de terminal. En HyperTerminal, seleccione **Transfer > Send File** (Transferir > Enviar archivo). Luego, al aparecer la ventana **Send File** (Enviar archivo), indique el nombre y la ubicación de la imagen. Seleccione Xmodem como el protocolo e inicie la transferencia. Durante la transferencia, la ventana Sending File (Enviando archivo) mostrará el estado de la transferencia. **3**

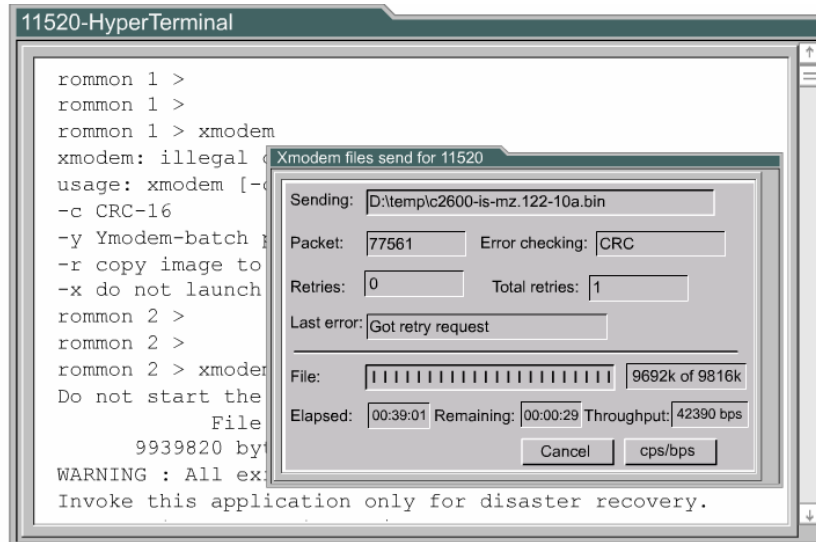


Figura 3

Al finalizar la transferencia, aparecerá un mensaje que indica que la flash ha sido borrada. Luego aparece el mensaje "Download Complete!" (¡Ha finalizado la descarga!). Antes de arrancar de nuevo el router, es necesario volver a fijar la velocidad de consola en 9600 y el config register a 0x2102. Ejecute el comando **config-register 0x2102** luego del indicador EXEC privilegiado.

Mientras el router arranca de nuevo, es necesario finalizar la sesión de terminal a 115200 bps e iniciar una nueva a 9600 bps.

5.2.7 Variables del entorno

El IOS también puede restaurarse desde una sesión TFTP. El descargar la imagen mediante TFTP desde ROMmon es la forma más rápida para restaurar una imagen del IOS en el router. Para ello se fijan variables de entorno y luego el comando **tftpdnld**.

Dado que el modo ROMmon tiene una funcionalidad muy limitada, no se carga ningún archivo de configuración durante el arranque. Por lo tanto, el router no dispone de ninguna configuración de interfaz o IP. Las variables de entorno suministran una configuración mínima para permitir el uso del TFTP. La transferencia TFTP de ROMmon sólo funciona en el primer puerto LAN, de modo que se fija un conjunto simple de parámetros IP para dicha interfaz. Para establecer una variable de entorno ROMmon, se escribe el nombre de la variable, luego el signo igual (=) y el valor de la variable (NOMBRE_DE_LA_VARIABLE=valor). Por ejemplo, para asignar la dirección de IP 10.0.0.1, ejecute **IP_ADDRESS=10.0.0.1** luego del indicador de ROMmon. **1**

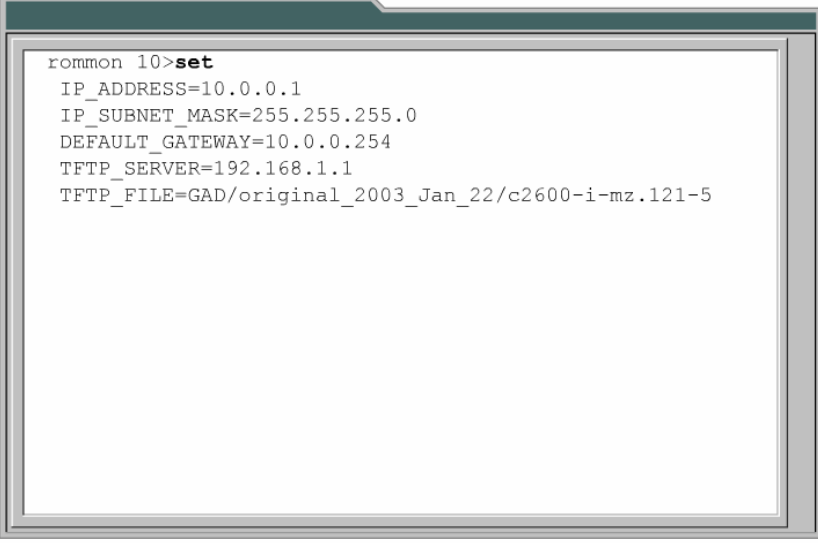
NOTA:

Todos los nombres de variables hacen distinción entre mayúsculas y minúsculas.

Las variables necesarias para usar **tftpdnld** son:

- **IP_ADDRESS**: la dirección de IP de la interfaz LAN
- **IP_SUBNET_MASK**: la máscara de subred de la interfaz LAN
- **DEFAULT_GATEWAY**: el gateway por defecto de la interfaz LAN
- **TFTP_SERVER**: la dirección de IP del servidor TFTP.
- **TFTP_FILE**: el nombre de la imagen del IOS en el servidor

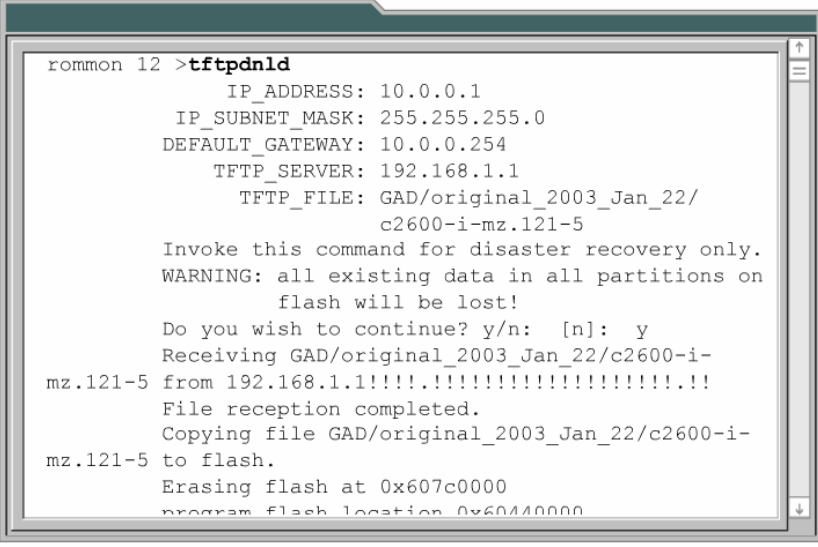
Para verificar las variables de entorno ROMmon, se puede usar el comando **set**. ¹



```
rommon 10>set
IP_ADDRESS=10.0.0.1
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=10.0.0.254
TFTP_SERVER=192.168.1.1
TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

Figura 1

Una vez que se han fijado las variables para la descarga del IOS, se ejecuta el comando **tftpdnld** sin ningún argumento. ROMmon mostrará un eco de las variables y luego un indicador de confirmación, con una advertencia que indica que esto borrará la flash. ²



```
rommon 12 >tftpdnld
IP_ADDRESS: 10.0.0.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 10.0.0.254
TFTP_SERVER: 192.168.1.1
TFTP_FILE: GAD/original_2003_Jan_22/
c2600-i-mz.121-5
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on
flash will be lost!
Do you wish to continue? y/n: [n]: y
Receiving GAD/original_2003_Jan_22/c2600-i-
mz.121-5 from 192.168.1.1!!!!!!
File reception completed.
Copying file GAD/original_2003_Jan_22/c2600-i-
mz.121-5 to flash.
Erasing flash at 0x607c0000
program flash location 0x60440000
```

Figura 2

A medida que se recibe cada uno de los datagramas del archivo del IOS, aparecerá un signo de exclamación "!". Una vez que se haya recibido todo el archivo de IOS, se procede a borrar la flash y escribir el nuevo archivo de imagen del IOS: Se mostrarán los mensajes correspondientes a medida que el proceso avanza.

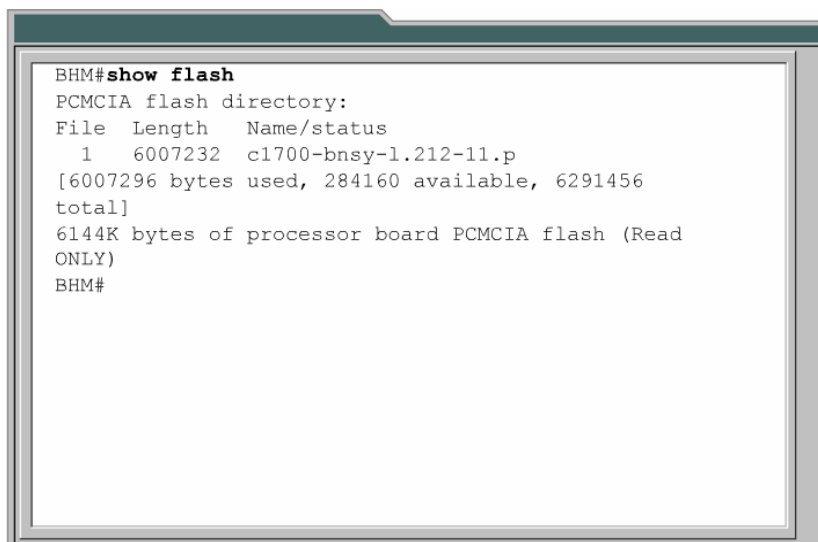
Cuando la nueva imagen ha sido escrita en la flash y reaparece el indicador de ROMmon, el router se puede arrancar mediante el comando **i**. Ahora, el router debe arrancar desde la nueva imagen del IOS en la flash.

5.2.8 Verificación del sistema de archivos

Se puede usar diversos comandos para verificar el sistema de archivos del router. Uno de ellos es el comando **show version**. El comando **show version** puede usarse para verificar la imagen en uso y la cantidad total de memoria flash. También verifica los otros dos elementos relativos a la carga del IOS. Identifica la fuente de la imagen del IOS que el router usa para arrancar y muestra el registro de configuración. Se puede examinar los valores del campo de arranque del registro de configuración para determinar desde dónde debe cargarse el IOS. Si no concuerdan, es posible que haya una imagen del IOS

dañada o ausente en la flash, o tal vez que haya comandos relativos al arranque en la configuración de arranque.

El comando **show flash** se puede usar también para verificar el sistema de archivos. ¹ Este comando se usa para identificar la o las imágenes del IOS en la flash, así como también la cantidad de memoria flash disponible. A menudo, este comando se usa para confirmar que haya espacio suficiente para guardar una nueva imagen del IOS.



```
BHM#show flash
PCMCIA flash directory:
File Length Name/status
 1 6007232 c1700-bnsy-1.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

Figura 1

Como se mencionara anteriormente, el archivo de configuración puede contener comandos boot system (del sistema de arranque). Estos comandos se pueden usar para identificar la fuente de la imagen de arranque del IOS deseada. Se pueden usar varios comandos boot system para crear una secuencia de reserva para encontrar y cargar el IOS. Estos comandos boot system se ejecutan en el orden en el que aparecen en el archivo de configuración.

Resumen

- Identificación de las etapas de la secuencia de arranque del router
- Identificación del esquema usado por el dispositivo de Cisco para ubicar y cargar el Cisco IOS
- Uso del comando **boot system**
- Identificación de los valores del registro de configuración.
- Diagnóstico de fallas
- Identificación de los archivos que usa el Cisco IOS y sus funciones
- Identificación de la ubicación de los distintos tipos de archivos en el router
- Identificación de las partes del nombre del IOS
- Administración de los archivos de configuración mediante TFTP
- Administración de los archivos de configuración mediante cortar y pegar
- Administración de las imágenes del IOS mediante TFTP
- Administración de las imágenes del IOS mediante XModem
- Verificación del sistema de archivos mediante comandos show

Módulo 6: Enrutamiento y protocolos de enrutamiento

Descripción general

El enrutamiento no es otra cosa que instrucciones para ir de una red a otra. Estas instrucciones, también conocidas como rutas, pueden ser dadas a un router por otro de forma dinámica, o pueden ser asignadas al router por el administrador de forma estática.

Este módulo introduce el concepto de protocolos de enrutamiento dinámico, describe sus distintas clases y brinda ejemplos de protocolos de cada clase.

Un administrador de redes toma en cuenta muchos aspectos al seleccionar un protocolo de enrutamiento dinámico. El tamaño de la red, el ancho de banda de los enlaces disponibles, la capacidad de procesamiento de los routers, las marcas y modelos de los routers de la red y los protocolos que ya se encuentran en uso en la red son todos factores a considerar a la hora de elegir un protocolo de enrutamiento. Este módulo proporcionará más detalles acerca de las diferencias entre los protocolos de enrutamiento, los cuales serán útiles a los administradores de redes para hacer su elección.

Los estudiantes que completen este módulo deberán ser capaces de:

- Explicar la importancia del enrutamiento estático.
- Configurar rutas estáticas y rutas por defecto.
- Verificar y diagnosticar fallas de las rutas estáticas y las rutas por defecto.
- Identificar las clases de protocolos de enrutamiento
- Identificar los protocolos de enrutamiento por vector-distancia.
- Identificar los protocolos de enrutamiento de estado del enlace.
- Describir las características básicas de los protocolos de enrutamiento más comunes.
- Identificar los protocolos de gateway interior.
- Identificar los protocolos de gateway exterior.
- Habilitar el Protocolo de información de enrutamiento (RIP) en un router.

6.1 Introducción al enrutamiento estático

6.1.1 Introducción al enrutamiento

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Estática	Utiliza una ruta programada que el administrador de la red introduce en el router
Dinámica	Utiliza una ruta que un protocolo de enrutamiento de red ajusta automáticamente ante los cambios de

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

6.1.2 Operación con rutas estáticas

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.
- Los paquetes se enrutan de acuerdo a la ruta estática.

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **ip route**. La sintaxis correcta del comando **ip route** se muestra en la Figura 1.

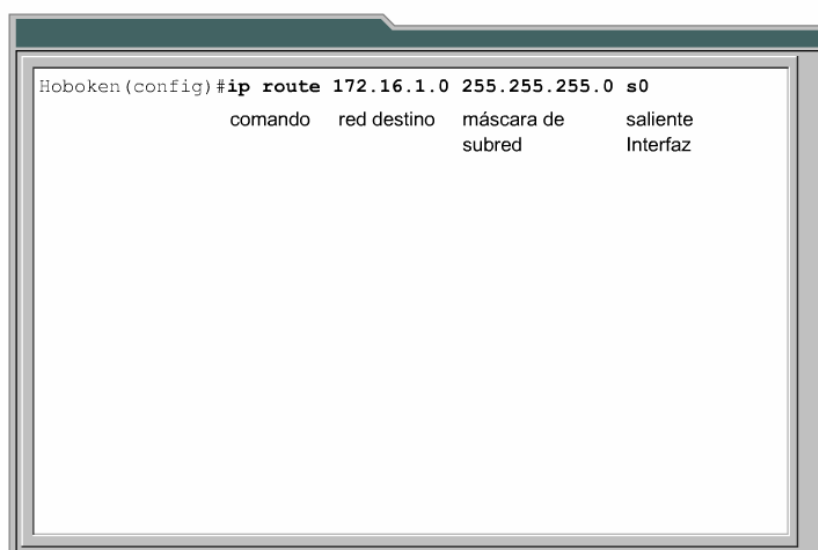


Figura 1

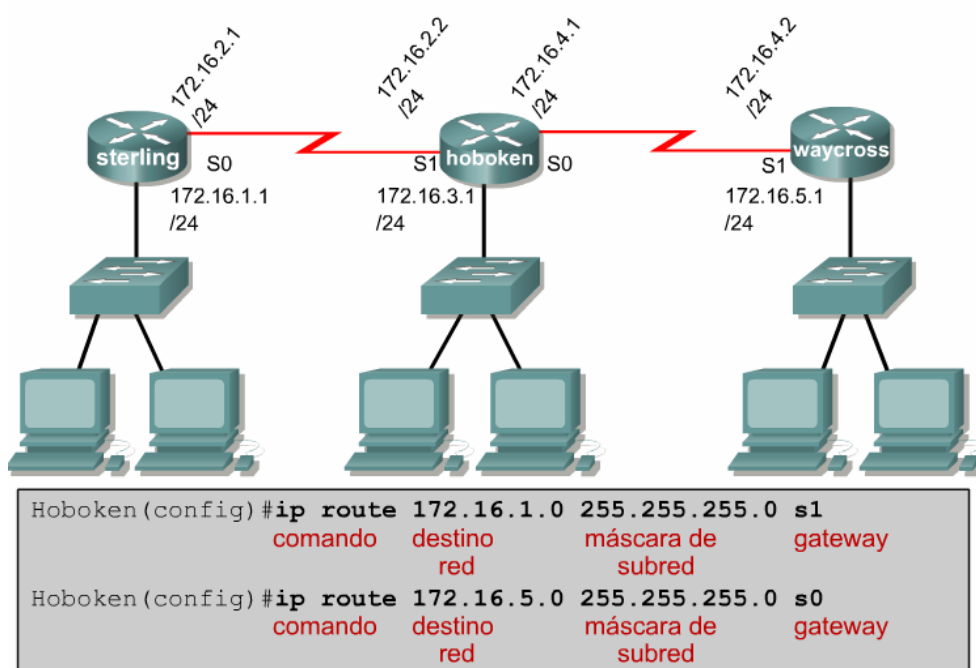


Figura 2

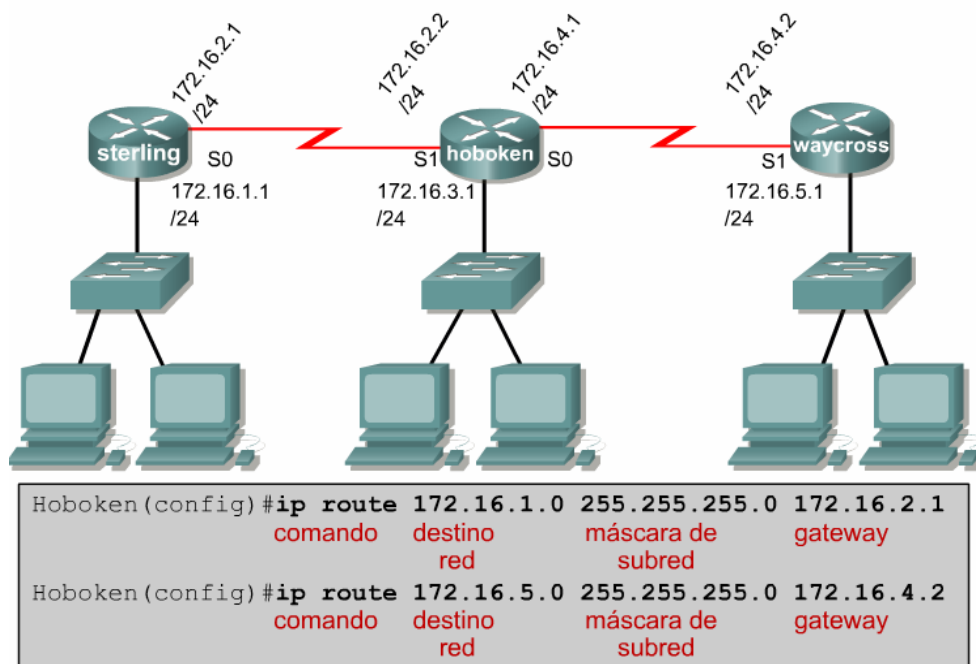


Figura 3

En las Figuras 2 y 3, el administrador del router Hoboken necesita configurar las rutas estáticas cuyo destino son las redes 172.16.1.0/24 y 172.16.5.0/24. El administrador puede ejecutar uno de dos comandos posibles para lograr su objetivo. El método de la Figura 2 especifica la interfaz de salida. El método de la Figura 3 especifica la dirección IP del siguiente salto (hop) del router adyacente. Cualquiera de los comandos instalará una ruta estática en la tabla de enrutamiento del router Hoboken.

La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. Por lo tanto, es preferible instalar rutas de distancia administrativa menor antes que una ruta idéntica de distancia administrativa mayor. La distancia administrativa por defecto cuando se usa una ruta estática es 1. En la tabla de enrutamiento se observará la ruta estática indicando la interface de salida, como si hubiera conexión directa. Esto a veces confunde, ya que la redes directamente conectadas tienen distancia 0. Para verificar la distancia administrativa de una ruta en particular use el comando **show ip route address**, donde la dirección ip de dicha ruta se inserta en la opción *address*. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida o el siguiente salto, como se muestra a continuación:

```
waycross(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1 130
```

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta.

A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

6.1.3 Configuración de rutas estáticas

Esta sección enumera los pasos a seguir para configurar rutas estáticas y da un ejemplo de una red sencilla en la que se podrían configurar rutas estáticas.

Siga estos pasos para configurar rutas estáticas.

1. Defina todas las redes de destino deseadas, sus máscaras de subred y sus gateways. Las direcciones pueden ser una interfaz local o la dirección del siguiente salto que conduce al destino deseado.
2. Ingrese al modo de configuración global.
3. Ejecute el comando **ip route** con una dirección de destino y máscara de subred, seguidos del gateway correspondiente del Paso 1. La inclusión de una distancia administrativa es opcional.

4. Repita el Paso 3 para todas las redes de destino definidas en el Paso 1.
5. Salga del modo de configuración global.
6. Guarde la configuración activa en la NVRAM mediante el comando **copy running-config startup-config**.

La red en el ejemplo tiene una sencilla configuración de tres routers. **1** Hoboken debe configurarse de manera tal que pueda llegar a la red 172.16.1.0 y a la red 172.16.5.0. Ambas tienen una máscara de subred de 255.255.255.0.

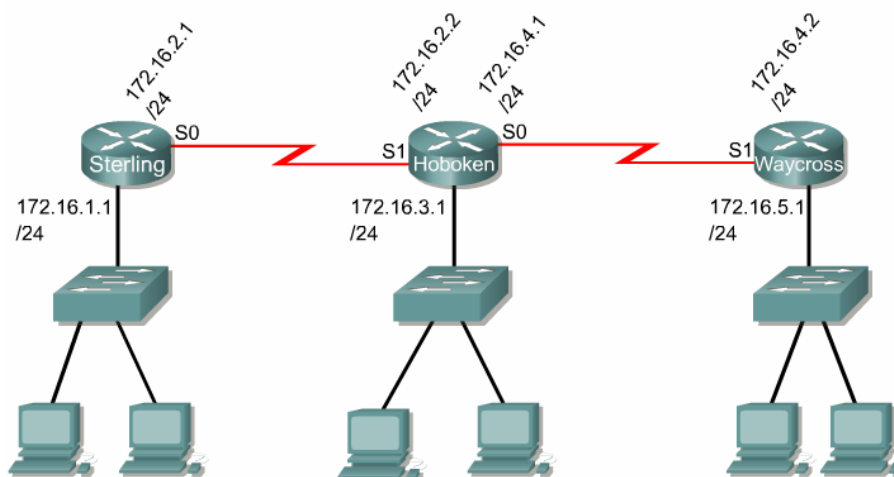


Figura 1

Los paquetes cuyo destino es la red 172.16.1.0 deben ser enrutados hacia Sterling y los paquetes que cuyo destino es la red 172.16.5.0 deben ser enrutados hacia Waycross. Esto se puede llevar a cabo mediante rutas estáticas.

Como primer paso, se configura ambas rutas estáticas para utilizar una interfaz local como gateway hacia las redes de destino. **2** Como no se especificaron distancias administrativas, estas tomarán el valor por defecto de 1 en la tabla de enrutamiento.

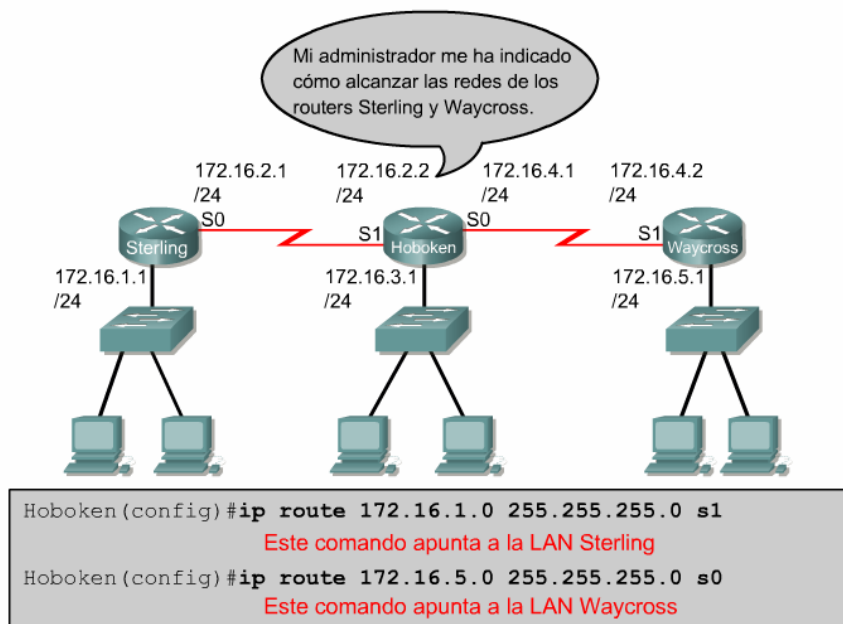


Figura 2

Esas mismas rutas estáticas también se pueden configurar utilizando como gateway la dirección del siguiente salto. **3** La primera ruta hacia la red 172.16.1.0 tendría como gateway 172.16.2.1. La segunda ruta hacia la red 172.16.5.0 tendría como gateway 172.16.4.2. Como no se especificaron distancias administrativas, toman el valor por defecto de 1.

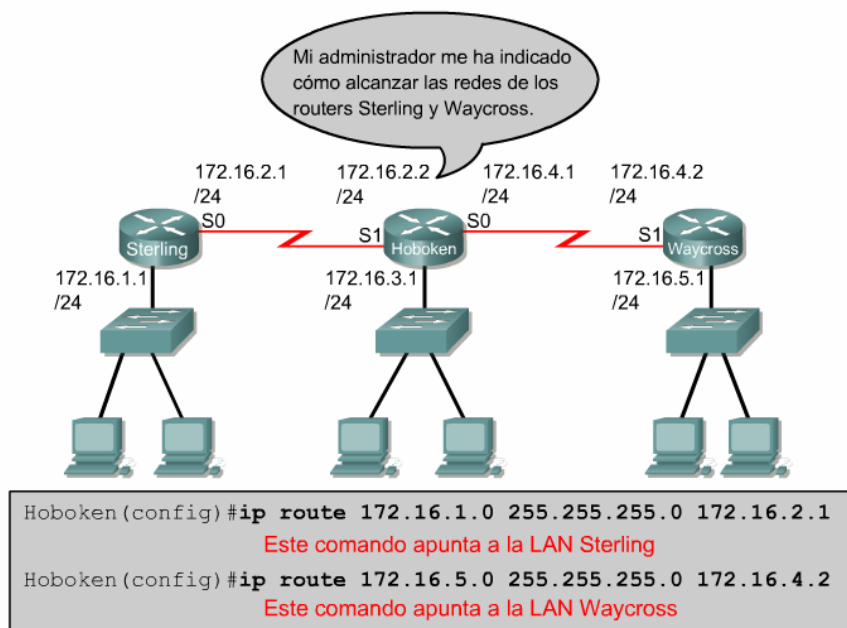


Figura 3

6.1.4 Configuración de enrutamiento por defecto

Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet. En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato:

ip route 0.0.0.0 0.0.0.0 [*dirección-del-siguiente-salto* | *interfaz de salida*]

La máscara 0.0.0.0, cuando se ejecuta el AND lógico hacia la dirección de IP de destino del paquete, siempre obtiene la red 0.0.0.0. Si el paquete no coincide con una ruta más específica en la tabla de enrutamiento, será enviado hacia la red 0.0.0.0.

Siga estos pasos para configurar rutas por defecto.

1. Ingrese al modo de configuración global.
2. Ejecute el comando **ip route** con 0.0.0.0 como la dirección de red de destino y 0.0.0.0 como máscara de subred. La opción address para la ruta por defecto puede ser la interfaz del router local que está conectado a las redes externas, o puede ser la dirección IP del router del siguiente salto. En la mayoría de los casos, es preferible especificar la dirección IP del router del siguiente salto.
3. Salga del modo de configuración global.
4. Guarde la configuración activa en la NVRAM mediante el comando **copy running-config startup-config**.

En la sección "Configuración de rutas estáticas", se crearon rutas estáticas en Hoboken para hacer posible el acceso a las redes 172.16.1.0 de Sterling y 172.16.5.0 de Waycross. Ahora debería ser posible el enrutamiento de paquetes hacia ambas redes desde Hoboken. Sin embargo, ni Sterling ni Waycross sabrán como enviar paquetes de vuelta hacia cualquier red conectada indirectamente. Se puede configurar una ruta estática en Sterling y en Waycross para cada una de las redes de destino conectadas indirectamente. Esta no sería una solución escalable en una red de mayor tamaño.

Sterling se conecta a todas las redes conectadas indirectamente mediante la interfaz Serial 0. Waycross tiene sólo una conexión con todas las redes conectadas indirectamente. Lo hace mediante la interfaz Serial 1. Una ruta por defecto tanto en Sterling como en Waycross proporcionará el enrutamiento para todos los paquetes cuyo destino sea las redes conectadas indirectamente. [1](#) [2](#)

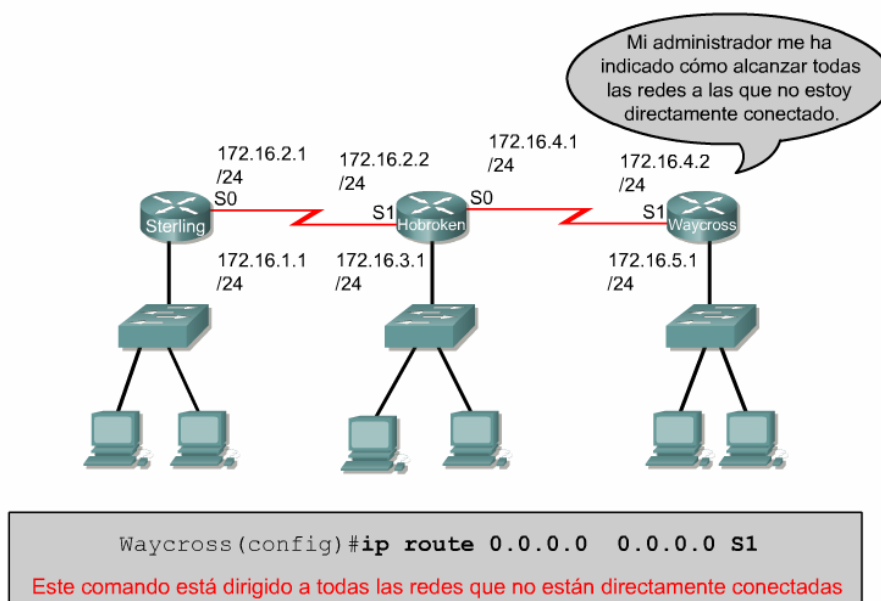


Figura 1

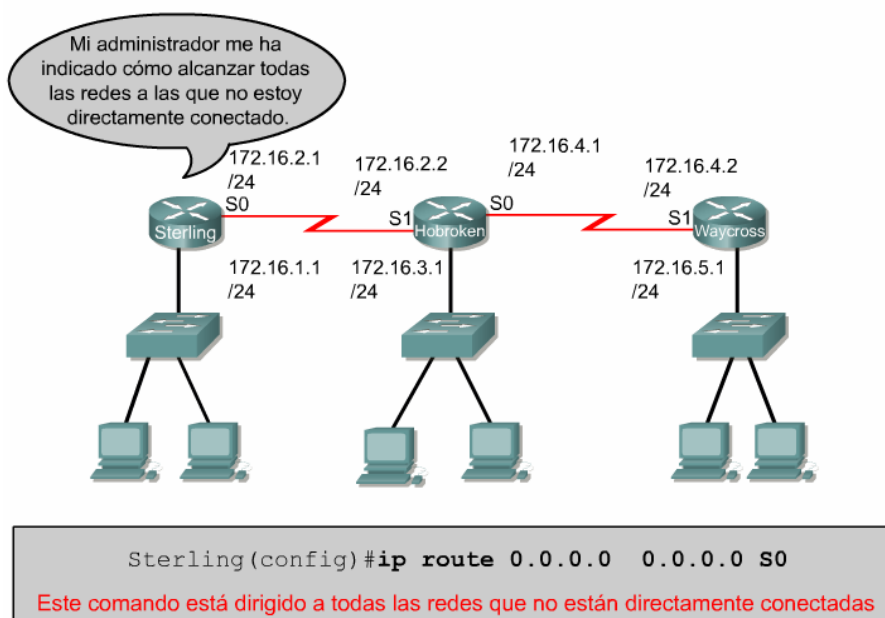


Figura 2

6.1.5 Verificación de las rutas estáticas

Una vez configuradas las rutas estáticas, es fundamental verificar que se muestren en la tabla de enrutamiento, y que el enrutamiento funcione tal como está previsto. El comando **show running-config** se utiliza para mostrar la configuración activa en la RAM, a fin de verificar que se haya ingresado correctamente la ruta estática. El comando **show ip route** se utiliza para comprobar que la ruta estática se encuentre en la tabla de enrutamiento.

Siga estos pasos para verificar la configuración de las rutas estáticas.

- En modo privilegiado, introduzca el comando **show running-config** para mostrar la configuración activa.
- Verifique que la ruta estática se haya ingresado correctamente. Si la ruta fuese incorrecta, será necesario volver al modo de configuración global para eliminar la ruta estática incorrecta e ingresar la ruta correcta.
- Ejecute el comando **show ip route**.
- Verifique que la ruta configurada se encuentre en la tabla de enrutamiento.

6.1.6 Diagnóstico de fallas en la configuración de rutas estáticas

En la sección "Configuración de rutas estáticas", se crearon rutas estáticas en el router Hoboken para hacer posible el acceso a las redes 172.16.1.0 de Sterling y 172.16.5.0 de Waycross. **1** Con esa configuración, los nodos locales de la red Sterling (172.16.1.0) no pueden llegar a los nodos locales de la red Waycross (172.16.5.0).

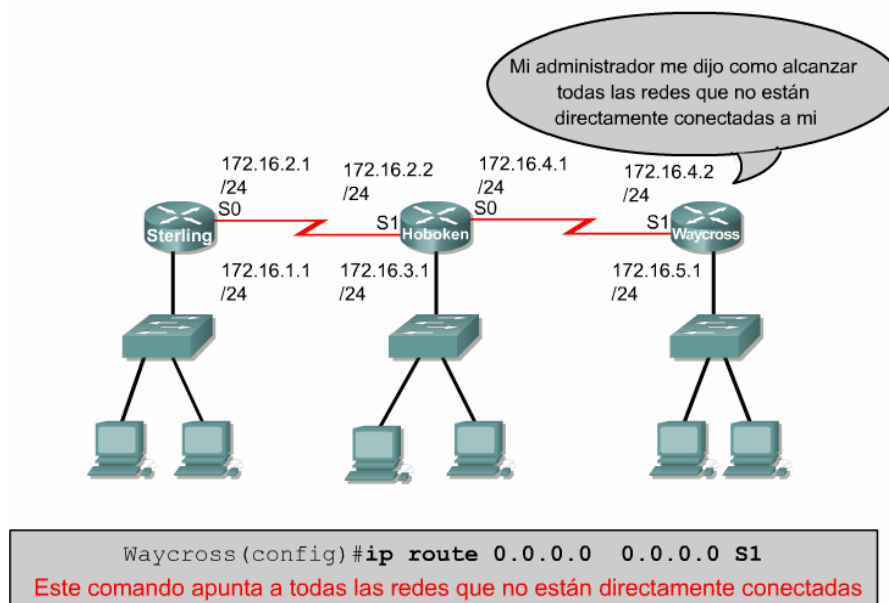


Figura 1

Desde el modo EXEC privilegiado en el router Sterling, ejecute un **ping** hacia el nodo de la red 172.16.5.0. El **ping** falla. Ahora, ejecute un **traceroute** desde Sterling a la dirección que se utilizó en el comando **ping**. Vea en qué punto falla el **traceroute**. El **traceroute** indica que el paquete regresó desde Hoboken pero no desde Waycross.

Esto implica que el problema está en el router Hoboken o en el Waycross. **2** Haga telnet en el router Hoboken. Intente nuevamente realizar un **ping** hacia el nodo de la red 172.16.5.0 conectado al router de Waycross. Este **ping** debería tener éxito ya que Hoboken está conectado directamente a Waycross.

```
Hoboken#ping 172.16.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

Hoboken#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
Hoboken#
```

Figura 2

6.2 Aspectos generales del enrutamiento dinámico

6.2.1 Introducción a los protocolos de enrutamiento

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento. ¹

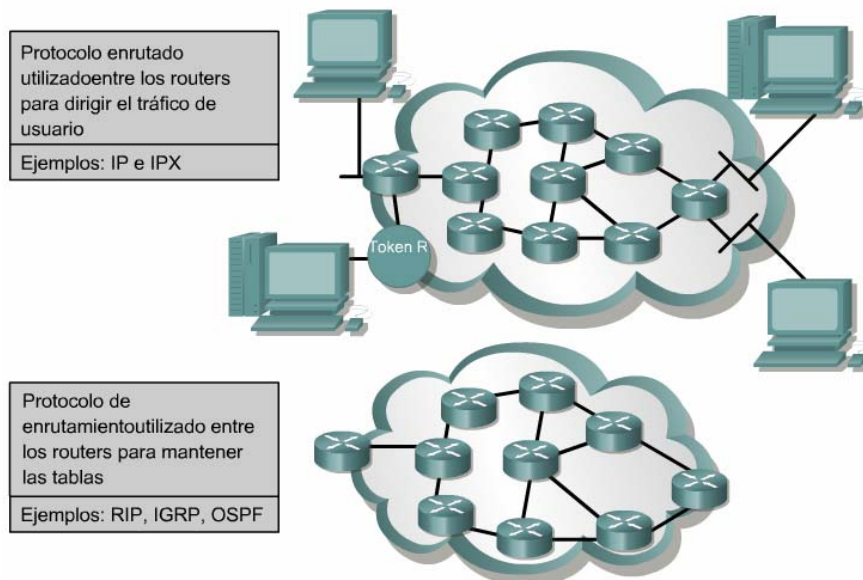


Figura 1

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP)
- Protocolo de enrutamiento de gateway interior (IGRP)
- Protocolo de enrutamiento de gateway interior mejorado (EIGRP)
- Protocolo "Primero la ruta más corta" (OSPF)

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados:

- Protocolo Internet (IP)
- Intercambio de paquetes de internetwork (IPX)

6.2.2 Sistemas autónomos

Un sistema autónomo (AS) es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única. El AS puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

Los números de identificación de cada AS son asignados por el Registro estadounidense de números de la Internet (ARIN), los proveedores de servicios o el administrador de la red. Este sistema autónomo es un número de 16 bits. Los protocolos de enrutamiento tales como el IGRP de Cisco, requieren un número único de sistema autónomo.

6.2.3 Propósito de los protocolos de enrutamiento y de los sistemas autónomos

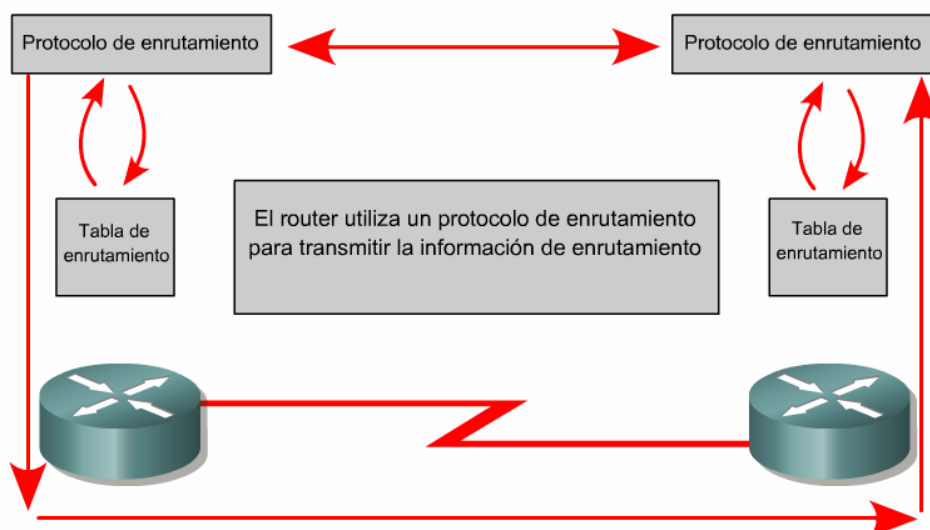
El objetivo de un protocolo de enrutamiento es crear y mantener una tabla de enrutamiento. Esta tabla contiene las redes conocidas y los puertos asociados a dichas redes. Los routers utilizan protocolos de enrutamiento para administrar la información recibida de otros routers, la información que se conoce a partir de la configuración de sus propias interfaces, y las rutas configuradas manualmente.

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos.

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Al haber cambios en la topología de una red, por razones de crecimiento, reconfiguración o falla, la información conocida acerca de la red también debe cambiar. La información conocida debe reflejar una visión exacta y coherente de la nueva topología.

Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia. Una rápida convergencia es deseable, ya que reduce el período de tiempo durante el cual los routers toman decisiones de enrutamiento erróneas.

Los sistemas autónomos (AS) permiten la división de la red global en subredes de menor tamaño, más manejables. Cada AS cuenta con su propio conjunto de reglas y políticas, y con un único número AS que lo distingue de los demás sistemas autónomos del mundo.



6.2.4 Identificación de las clases de protocolos de enrutamiento

La mayoría de los algoritmos de enrutamiento pertenecen a una de estas dos categorías:

- Vector-distancia
- Estado del enlace

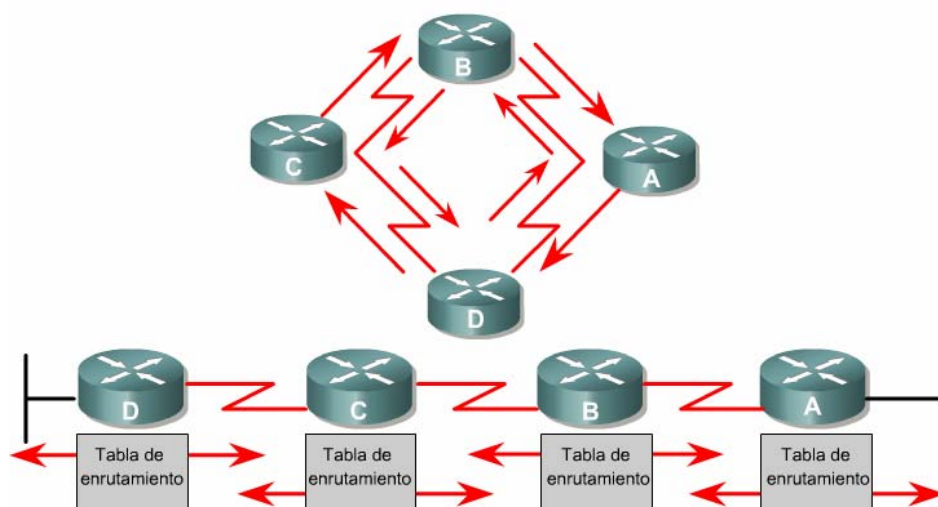
El método de enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la red. El método de estado del enlace, también denominado "primero la ruta más corta", recrea la topología exacta de toda la red.

6.2.5 Características del protocolo de enrutamiento por vector-distancia

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de enrutamiento basados en el vector-distancia también se conocen como algoritmos Bellman-Ford.

Cada router recibe una tabla de enrutamiento de los routers conectados directamente a él. ¹El router B recibe información del router A. El router B agrega un cifra de vector-distancia (por ejemplo: el número de saltos), la cual aumenta el vector-distancia. Luego el router B pasa esta nueva tabla de enrutamiento a su

otro vecino, el router C. Este mismo proceso, paso a paso, se repite en todas direcciones entre routers vecinos.



Enviar copias periódicas de una tabla de enrutamiento a los routers vecinos y acumular vectores-distancia

Figura 1

El algoritmo finalmente acumula información acerca de las distancias de la red, las cual le permite mantener una base de datos de la topología de la red. Sin embargo, los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Cada router que utiliza el enrutamiento por vector-distancia comienza por identificar sus propios vecinos. ² La interfaz que conduce a las redes conectadas directamente tiene una distancia de 0. A medida que el proceso de descubrimiento de la red avanza, los routers descubren la mejor ruta hacia las redes de destino, de acuerdo a la información de vector-distancia que reciben de cada vecino. Por ejemplo, el router A aprende acerca de otras redes según la información que recibe del router B. Cada una de las redes de destino en la tabla de enrutamiento tiene una cifra total de vector-distancia, la cual indica la distancia a la que se encuentra dicha red por una ruta determinada.

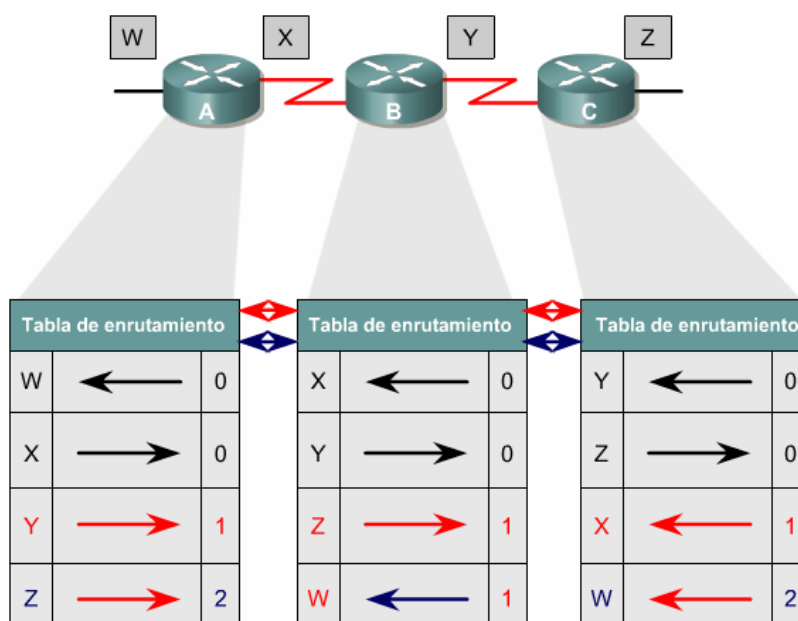


Figura 2

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambios de topología avanzan paso a paso, de un router a otro. ³ Los algoritmos de vector-distancia hacen que cada router envíe su tabla de

enrutamiento completa a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla. ⁴

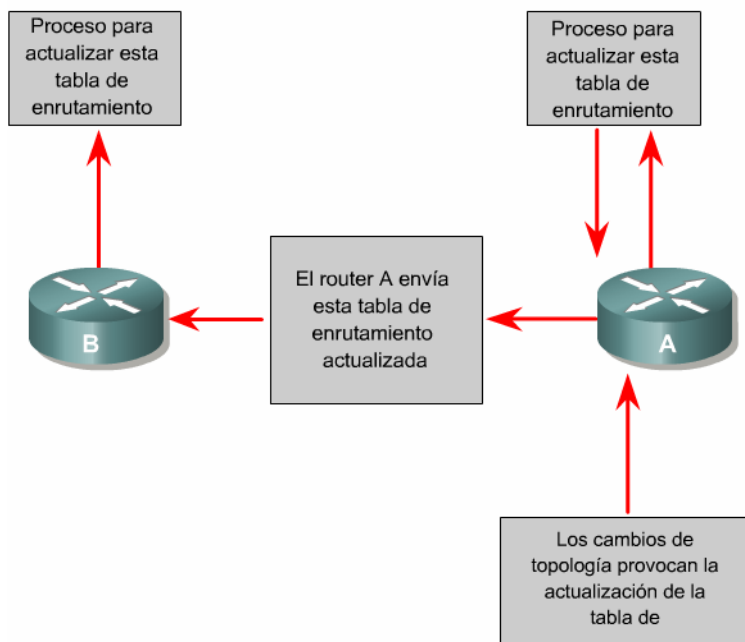


Figura 3

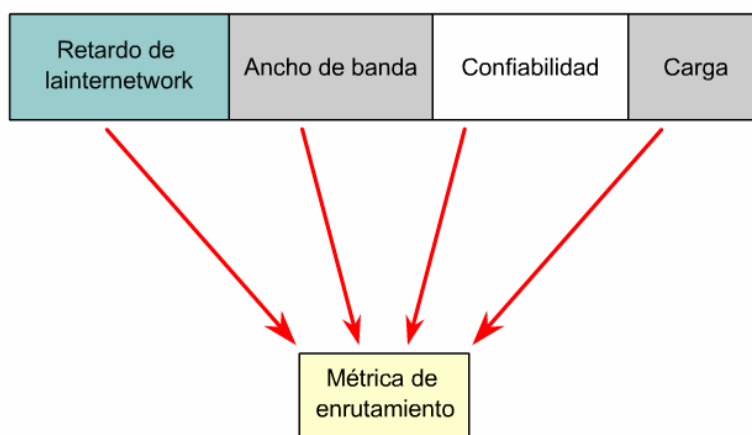


Figura 4

Una analogía del vector-distancia podría ser los carteles que se encuentran en las intersecciones de las autopistas. Un cartel indica el destino e indica la distancia hasta el destino. Más adelante en la autopista, otro cartel indica el destino, pero ahora la distancia es más corta. A medida que se acorta la distancia, el tráfico sigue la mejor ruta.

6.2.6 Características del protocolo de enrutamiento de estado del enlace

El segundo algoritmo básico que se utiliza para enrutamiento es el algoritmo de estado del enlace. Los algoritmos de estado del enlace también se conocen como algoritmos Dijkstras o SPF ("primero la ruta más corta"). Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de vector-distancia provee información indeterminada sobre las redes lejanas y no tiene información acerca de los routers distantes. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

El enrutamiento de estado del enlace utiliza: ¹

- **Publicaciones de estado del enlace (LSA):** una publicación del estado del enlace (LSA) es un paquete pequeño de información sobre el enrutamiento, el cual es enviado de router a router.

- **Base de datos topológica:** una base de datos topológica es un cúmulo de información que se ha reunido mediante las LSA.
- **Algoritmo SPF:** el algoritmo "primero la ruta más corta" (SPF) realiza cálculos en la base de datos, y el resultado es el árbol SPF.
- **Tablas de enrutamiento:** una lista de las rutas e interfaces conocidas.

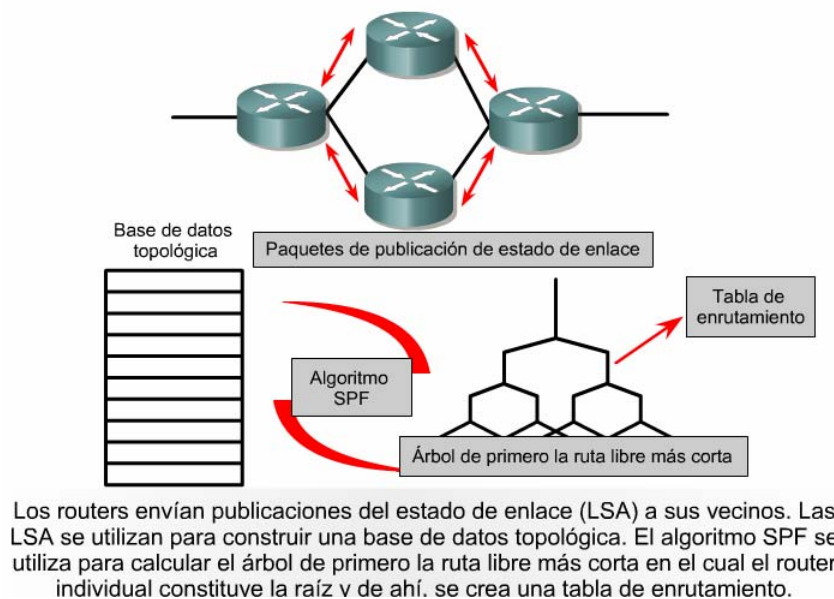


Figura 1

Proceso de descubrimiento de la red para el enrutamiento de estado del enlace:

el intercambio de LSAs se inicia en las redes conectadas directamente al router, de las cuales tiene información directa. Cada router, en paralelo con los demás, genera una base de datos topológica que contiene toda la información recibida por intercambio de LSAs.

El algoritmo SPF determina la conectividad de la red. El router construye esta topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca la ruta más corta primero (SPF). El router elabora una lista de las mejores rutas a las redes de destino, y de las interfaces que permiten llegar a ellas. Esta información se incluye en la tabla de enrutamiento. También mantiene otras bases de datos, de los elementos de la topología y de los detalles del estado de la red. ²

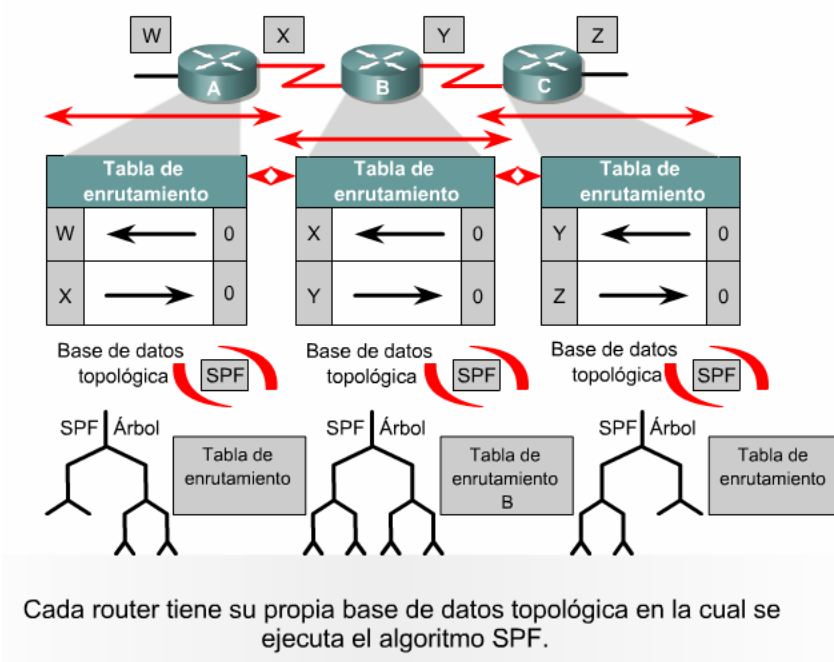


Figura 2

El router que primero conoce de un cambio en la topología envía la información al resto de los routers, para que puedan usarla para hacer sus actualizaciones y publicaciones. ³ Esto implica el envío de información de enrutamiento, la cual es común a todos los routers de la red. Para lograr la convergencia, cada router monitorea sus routers vecinos, sus nombres, el estado de la interconexión y el costo del enlace con cada uno de ellos. El router genera una LSA, la cual incluye toda esa información, junto con información relativa a nuevos vecinos, los cambios en el costo de los enlaces y los enlaces que ya no son válidos. La LSA es enviada entonces, a fin de que los demás routers la reciban.

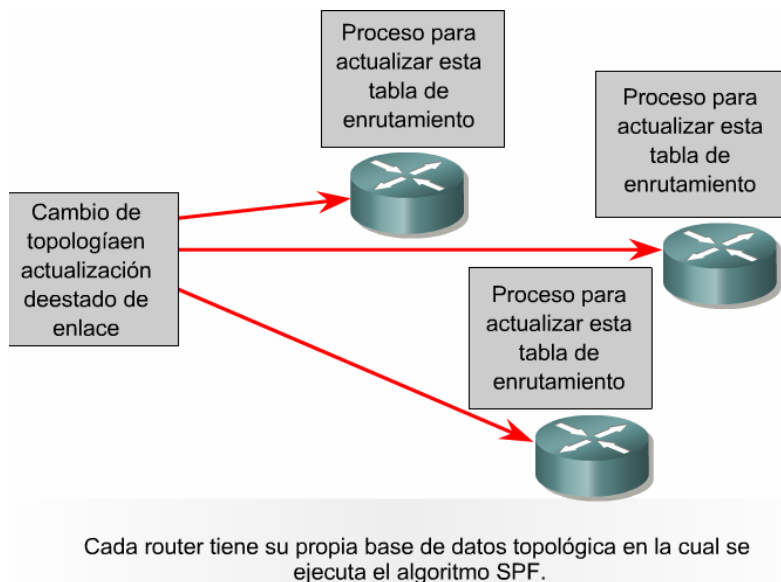


Figura 3

Cuando un router recibe una LSA, actualiza su base de datos con la información más reciente y elabora un mapa de la red con base en los datos acumulados, y calcula la ruta más corta hacia otras redes mediante el algoritmo SPF. Cada vez que una LSA genera cambios en la base de datos, el algoritmo de estado del enlace (SPF) vuelve a calcular las mejores rutas, y actualiza la tabla de enrutamiento.

Puntos de interés acerca del estado del enlace

- Carga sobre el procesador.
- Requisitos de memoria.
- Utilización del ancho de banda.

Los routers que usan protocolos de estado del enlace requieren de más memoria y exigen mas esfuerzo al procesador, que los que usan protocolos de enrutamiento por vector-distancia. Los routers deben tener la memoria suficiente para almacenar toda la información de las diversas bases de datos, el árbol de topología y la tabla de enrutamiento. ⁴ La avalancha de LSAs que ocurre al activar un router consume una porción del ancho de banda. Durante el proceso de descubrimiento inicial, todos los routers que utilizan protocolos de enrutamiento de estado del enlace envían LSAs a todos los demás routers. Esta acción genera un gran volumen de tráfico y reduce temporalmente el ancho de banda disponible para el tráfico enrutado de los usuario. Después de esta disminución inicial de la eficiencia de la red, los protocolos de enrutamiento del estado del enlace generalmente consumen un ancho de banda mínimo, sólo para enviar las ocasionales LSAs que informan de algún cambio en la topología.

6.3 Aspectos generales de los protocolos de enrutamiento

6.3.1 Determinación de rutas

Los routers determinan la ruta de los paquetes desde un enlace a otro, mediante dos funciones básicas:

- Una función de determinación de ruta
- Una función de conmutación.

La determinación de la ruta se produce en la capa de red. La función de determinación de ruta permite al router evaluar diversas rutas hacia un destino, y establecer cuál es la más deseable. El router utiliza la tabla de enrutamiento para determinar la mejor ruta, para luego enviar los paquetes de datos mediante la función de conmutación. ¹

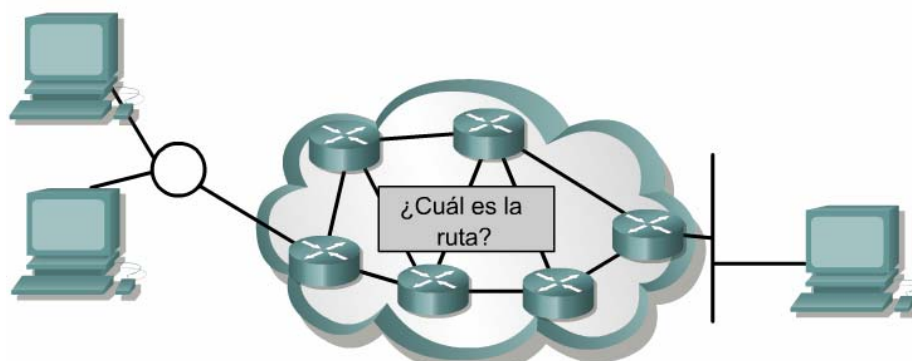
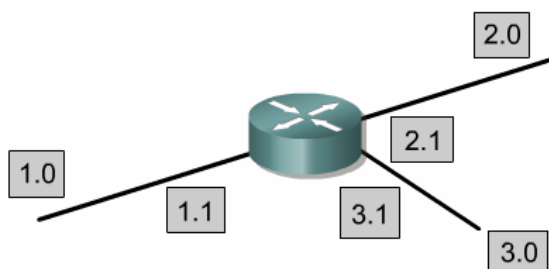


Figura 1

La función de conmutación es el proceso interno que el router utiliza para recibir un paquete en una interfaz y enviarlo a otra dentro del router mismo. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes de acuerdo a la estructura requerida por el siguiente enlace.

La Figura 2 ilustra de qué forma los routers utilizan las direcciones para estas funciones de enrutamiento y conmutación. El router utiliza el segmento de la dirección correspondiente a la red para seleccionar la ruta, y proceder a entregar el paquete al router siguiente en dicha ruta.



Red destino	Puerto directo y de router
1.0	1.1
2.0	2.1
3.0	3.1

- Porción de la red que corresponde a la dirección que se utiliza para hacer selecciones de ruta
- La porción de nodo de la dirección se refiere al puerto del router que conduce a la ruta

Figura 2

6.3.2 Configuración del enrutamiento

La habilitación del enrutamiento de paquetes de IP, requiere fijar parámetros tanto globales como de enrutamiento. Las tareas globales incluyen la selección de un protocolo de enrutamiento, por ejemplo: RIP, IGRP, EIGRP o OSPF. La tarea principal del modo configuración de enrutamiento es indicar los números IP de la red. El enrutamiento dinámico utiliza comunicaciones broadcast y multicast con los otros routers. La métrica de enrutamiento ayuda a los routers a encontrar la mejor ruta hacia cada red o subred. ¹

El comando **router** inicia el proceso de enrutamiento. ² ³

El comando **network** es necesario, ya que permite que el proceso de enrutamiento determine cuáles son las interfaces que participan en el envío y la recepción de las actualizaciones de enrutamiento. ² ⁴

Un ejemplo de configuración de enrutamiento es:

```
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
```

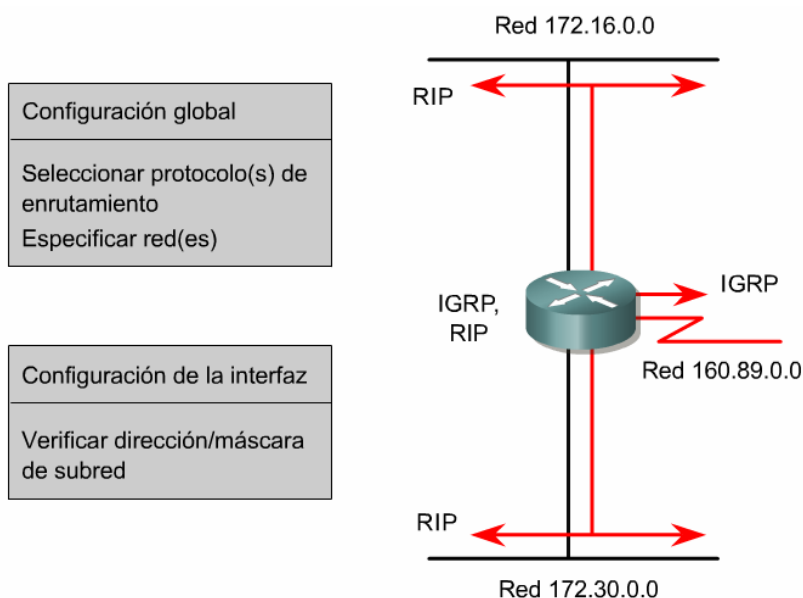



Figura 1

Comando

```
Router(config)#router protocol {options}
```

Define el protocolo de enrutamiento

Comando

```
Router(config-router)#network network-number
```

Los subcomandos de red son comandos de configuración obligatorios para cada proceso de enrutamiento

Figura 2

Comando Router	Descripción
protocolo	IGRP, EIGRP, OSPF o RIP
opciones	IGRP y EIGRP requieren un número autónomo. OSPF requiere un ID de proceso. RIP no requiere ninguno de los dos.

Figura 3

Comando Network	Descripción
network number	especifica una red directamente conectada

Figura 4

Los números de red se basan en las direcciones de clase de red, no en direcciones de subred ni direcciones de host individuales. Las direcciones de red principales se limitan a los números de red de las Clases A, B y C.

6.3.3 Protocolos de enrutamiento

Un router puede utilizar un protocolo de enrutamiento de paquetes IP para llevar a cabo el enrutamiento. Esto lo realiza mediante la implementación de un algoritmo de enrutamiento específico y emplea la capa de

interconexión de redes del conjunto de protocolos TCP/IP. Algunos ejemplos de protocolos de enrutamiento de paquetes IP son: **1**

- **RIP**: Un protocolo de enrutamiento interior por vector-distancia.
- **IGRP**: El protocolo de enrutamiento interior por vector-distancia de Cisco.
- **OSPF**: Un protocolo de enrutamiento interior de estado del enlace
- **EIGRP**: El protocolo mejorado de enrutamiento interior por vector-distancia de Cisco.
- **BGP**: Un protocolo de enrutamiento exterior por vector-distancia

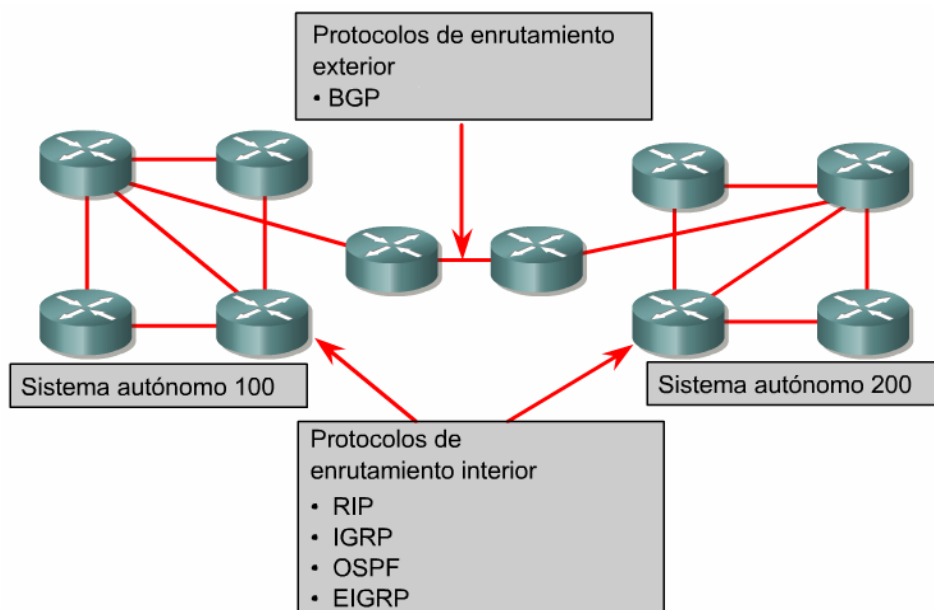


Figura 1

El Protocolo de información de enrutamiento (RIP) fue descrito originalmente en el RFC 1058. Sus características principales son las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

El Protocolo de enrutamiento interior de gateway (IGRP) es un protocolo patentado desarrollado por Cisco. Entre las características de diseño claves del IGRP se destacan las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

El protocolo público conocido como "Primero la ruta más corta" (OSPF) es un protocolo de enrutamiento de estado del enlace no patentado. Las características clave del OSPF son las siguientes:

- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público (open standard), y se describe en el RFC 2328.
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

El EIGRP es un protocolo mejorado de enrutamiento por vector-distancia, patentado por Cisco. Las características claves del EIGRP son las siguientes:

- Es un protocolo mejorado de enrutamiento por vector-distancia.
- Utiliza balanceo de carga asimétrico.
- Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace.
- Utiliza el Algoritmo de actualización difusa (DUAL) para el cálculo de la ruta más corta.
- Las actualizaciones son mensajes de multicast a la dirección 224.0.0.10 generadas por cambios en la topología.

El Protocolo de gateway de frontera (BGP) es un protocolo de enrutamiento exterior. Las características claves del BGP son las siguientes:

- Es un protocolo de enrutamiento exterior por vector-distancia.
- Se usa entre ISPs o entre los ISPs y sus clientes.
- Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

6.3.4 Sistemas autónomos - Protocolos IGP versus EGP

Los protocolos de enrutamiento interior están diseñados para ser usados en redes cuyos segmentos se encuentran bajo el control de una sola organización. Los criterios de diseño de los protocolos de enrutamiento interior requieren que el protocolo encuentre la mejor ruta a través de la red. En otras palabras, la métrica y la forma en que esta se utiliza es el elemento más importante de un protocolo de enrutamiento interior. ¹

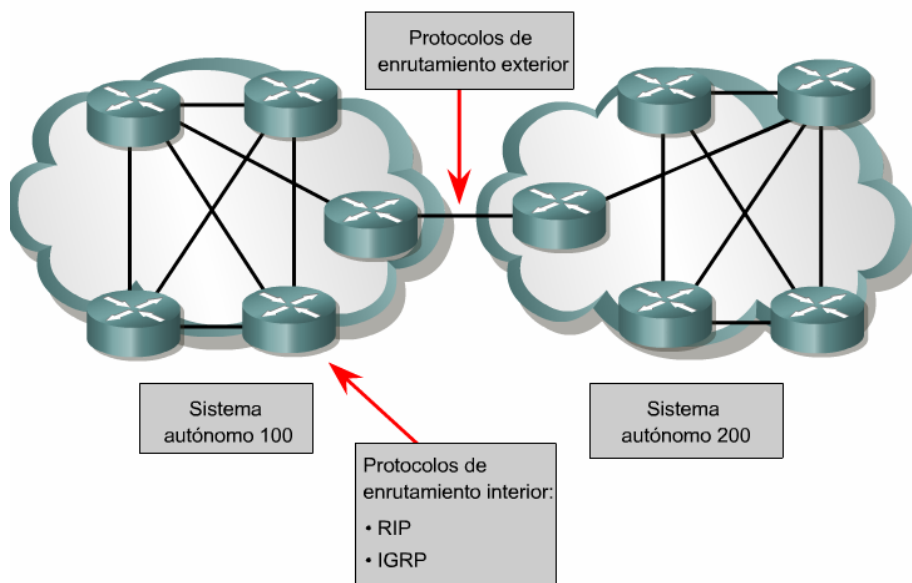


Figura 1

Un protocolo de enrutamiento exterior está diseñado para ser usado entre dos redes diferentes, las cuales se encuentran bajo el control de dos organizaciones diferentes. En general, se utilizan entre ISPs o entre una compañía y un ISP. Por ejemplo: una compañía puede usar el BGP, un protocolo de enrutamiento exterior, entre uno de sus routers y un router del ISP. Los protocolos de enrutamiento exterior necesitan de estos tres conjuntos de información antes de comenzar su operación:

- Una lista de los routers vecinos, con los que intercambiarán la información de enrutamiento.
- Una lista de las redes a ser publicadas como de acceso directo.
- El número de sistema autónomo del router local.

Un protocolo de enrutamiento exterior debe aislar los sistemas autónomos. Recuerde, los sistemas autónomos son administrados por entes distintos. Las redes deben disponer de un protocolo para interconectar los diferentes sistemas autónomos. ²

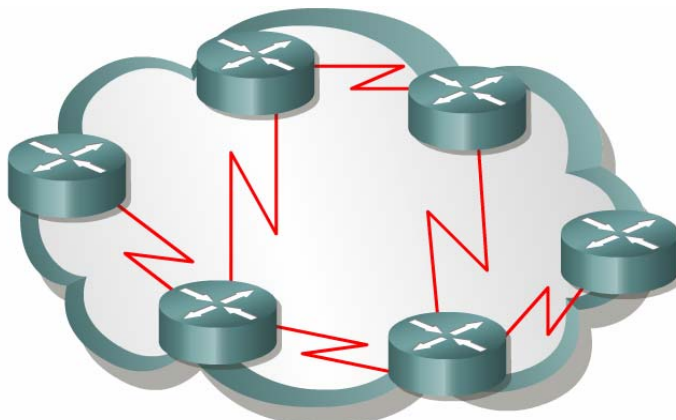


Figura 2

Los sistemas autónomos disponen de un número de identificación, asignado por el Registro estadounidense de números de Internet (ARIN) o por un proveedor de acceso. Dicho número consta de 16 bits. Los protocolos de enrutamiento como el IGRP y el EIGRP de Cisco, requieren la asignación de un número único de sistema autónomo.

Resumen

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

- Un router no enviará un paquete hacia la red de destino sin una ruta.
- Los administradores de redes son quienes configuran las rutas estáticas en forma manual.
- Las rutas por defecto son rutas estáticas especiales, las cuales proporcionan gateways de último recurso.
- Las rutas estáticas y las rutas por defecto se configuran con el comando **ip route**.
- Es posible verificar la configuración de las rutas estáticas y por defecto mediante los comandos **show ip route**, **ping**, y **traceroute**.
- Como verificar y diagnosticar las fallas de las rutas estáticas y por defecto.
- Protocolos de enrutamiento
- Sistemas autónomos
- Propósito de los protocolos de enrutamiento y de los sistemas autónomos
- Clases de protocolos de enrutamiento
- Características del protocolo de enrutamiento por vector-distancia y ejemplos.
- Características del protocolo de estado del enlace y ejemplos.
- Determinación de la ruta.
- Configuración del enrutamiento.
- Protocolos de enrutamiento (RIP, IGRP, OSPF, EIGRP, BGP)
- Sistemas autónomos y protocolos IGP versus EGP
- Enrutamiento por vector-distancia
- Enrutamiento por estado del enlace

Módulo 7: Protocolos de enrutamiento por vector-distancia

Descripción general

Los protocolos de enrutamiento dinámico pueden ayudar a simplificar la vida del administrador de redes. El enrutamiento dinámico hace innecesario el exigente y prolongado proceso de configurar rutas estáticas. El enrutamiento dinámico también hace posible que los routers se adapten a los cambios de la red y que ajusten sus tablas de enrutamiento en consecuencia, sin intervención del administrador de redes. Sin embargo, el enrutamiento dinámico puede ocasionar problemas. Este módulo cubre algunos de los problemas asociados con los protocolos de enrutamiento dinámico por vector-distancia, junto con algunos de los pasos que los diseñadores de protocolos han dado para resolverlos.

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, en uso en miles de redes en todo el mundo. El hecho que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados. Por su simplicidad, RIP es un buen protocolo de iniciación para el estudiante de redes. Este módulo también trata de la configuración y el diagnóstico de fallas del protocolo RIP.

Al igual que RIP, el Protocolo de enrutamiento de gateway interior (IGRP) es un protocolo de enrutamiento por vector-distancia. A diferencia de RIP, IGRP es un protocolo propietario de Cisco y no un protocolo basado en estándares públicos. Aunque es muy fácil de implementar, IGRP es un protocolo de enrutamiento más complejo que RIP. Es capaz de utilizar diversos factores para determinar la mejor ruta hacia la red de destino. Este módulo también trata de la configuración y el diagnóstico de fallas del protocolo IGRP.

Los estudiantes que completen este módulo deberán ser capaces de:

- Describir cómo se pueden ocurrir los bucles de enrutamiento en el enrutamiento por vector-distancia.
- Describir los distintos métodos utilizados por los protocolos de enrutamiento por vector-distancia para asegurar que la información de enrutamiento sea precisa.
- Configurar el protocolo RIP
- Utilizar el comando **ip classless**
- Diagnosticar fallas en el protocolo RIP
- Configurar RIP para el equilibrio de la carga
- Configurar RIP con rutas estáticas
- Verificar la operación del protocolo RIP
- Configurar el protocolo IGRP
- Verificar la operación del protocolo IGRP
- Diagnosticar fallas en el protocolo IGRP

7.1 Enrutamiento por vector-distancia

7.1.1 Actualizaciones en el enrutamiento por vector-distancia

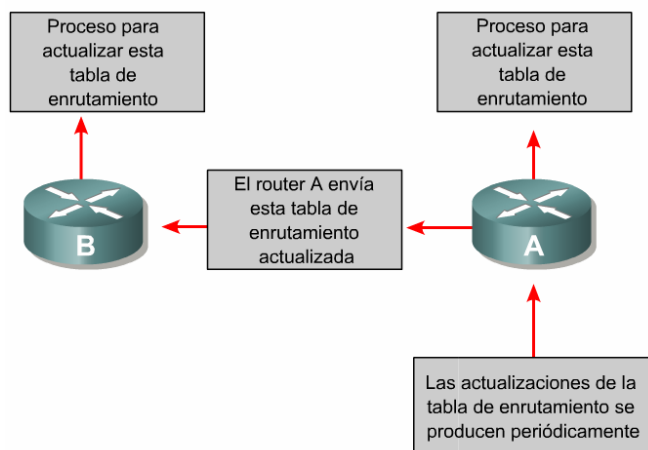


Figura 1

En el protocolo de vector-distancia, las actualizaciones de las tablas de enrutamiento se hacen periódicamente, o cuando cambia la topología de la red. Es importante que un protocolo de enrutamiento sea eficiente en su tarea de actualizar las tablas de enrutamiento. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambio de topología se producen de forma sistemática de un router a otro. ¹ Los algoritmos de vector-distancia requieren que cada router envíe toda la tabla de enrutamiento a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla. ²

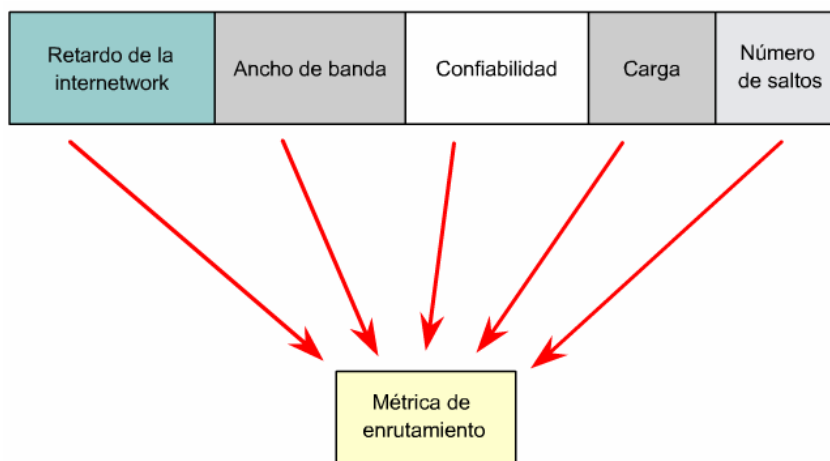


Figura 2

7.1.2 Bucles en el enrutamiento por vector-distancia

Los bucles de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes, las cuales no se han actualizado debido a la lenta convergencia de una red sujeta a cambios. ¹

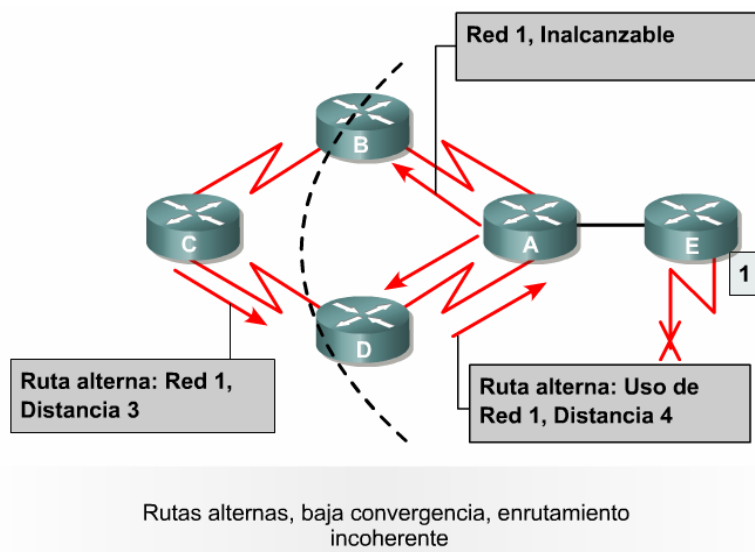


Figura 1

1. Antes de la falla de la red 1, todos los routers poseen información coherente y tablas de enrutamiento correctas. Se dice que la red ha logrado la convergencia. Supongamos, para el resto de este ejemplo, que la ruta preferida del router C hacia la red 1 es a través del router B y que la distancia del router C a la Red 1 es 3.
2. En el momento en que la red 1 falla, el router E envía una actualización al router A. El router A deja de enrutar paquetes hacia la red 1, pero los routers B, C y D siguen haciéndolo porque todavía no se les ha informado acerca de la falla. Cuando el router A envía su actualización, los routers B y D detienen el enrutamiento hacia la red 1; sin embargo, el router C no ha recibido la actualización. Para el router C, la red 1 todavía se puede alcanzar a través del router B.
3. El router C envía ahora una actualización periódica al router D, que señala una ruta hacia la red 1 a través del router B. El router D cambia su tabla de enrutamiento para introducir esta información

buena pero errónea, y transmite la información al router A. El router A transmite la información a los routers B y E, etc. Cualquier paquete destinado a la red 1 ahora realizará un bucle desde el router C al B, de allí al A y luego al D, y volverá nuevamente al C.

7.1.3 Definición de cuenta máxima

Las actualizaciones erróneas de la red 1 continuarán generando bucles hasta que algún otro proceso lo detenga. Esta condición, denominada cuenta al infinito, hace que los paquetes recorran la red en un ciclo continuo, a pesar del hecho fundamental de que la red de destino, la red 1, está fuera de servicio. Mientras los routers cuentan al infinito, la información errónea hace que se produzca un bucle de enrutamiento. ¹

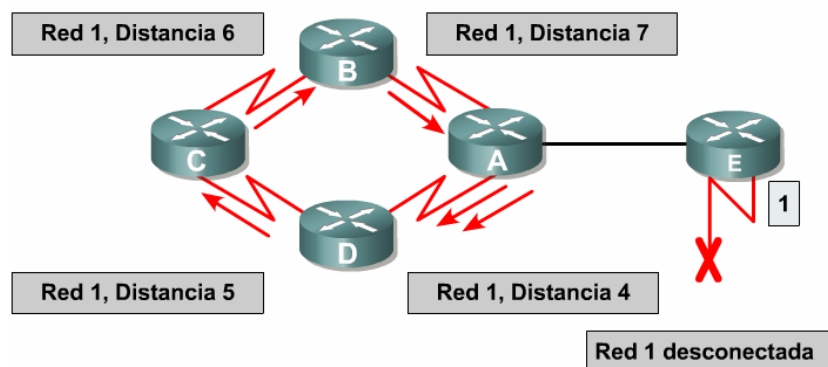


Figura 1

Si no se toman medidas para detener la cuenta al infinito, la métrica del vector-distancia del número de saltos aumenta cada vez que el paquete atraviesa otro router. Estos paquetes hacen un recorrido cíclico por la red debido a la información errónea en las tablas de enrutamiento.

Los algoritmos de enrutamiento por vector-distancia se corrigen automáticamente, pero un bucle de enrutamiento puede requerir primero una cuenta al infinito. Para evitar este problema, los protocolos de vector-distancia definen el infinito como un número máximo específico. Este número se refiere a una métrica de enrutamiento, la cual puede ser el número de saltos. ²

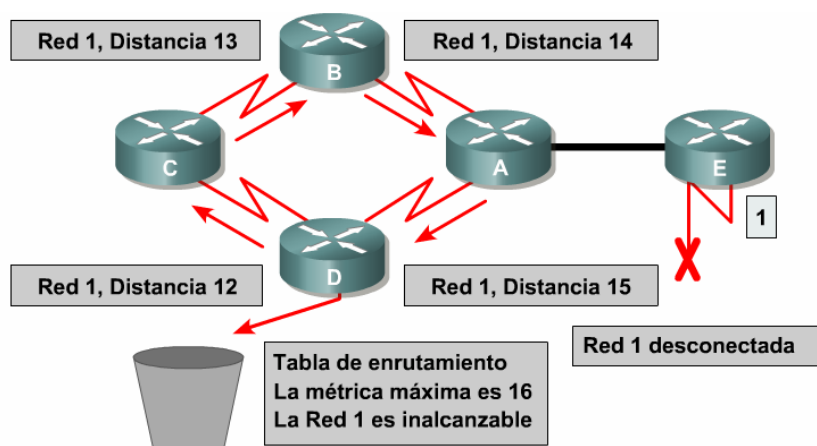


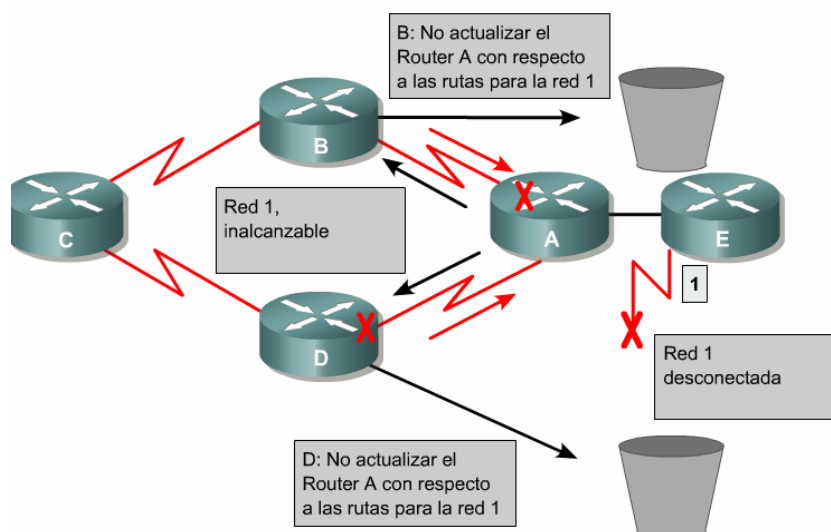
Figura 2

Con este enfoque, el protocolo de enrutamiento permite que el bucle de enrutamiento continúe hasta que la métrica supere el máximo valor permitido. El gráfico muestra que en este caso ya el valor alcanzó los 16 saltos. Esto supera la cifra máxima por defecto de 15 saltos del vector-distancia, de modo que el router descarta el paquete. En cualquier caso, cuando el valor de la métrica supera el valor máximo, se considera que no se puede alcanzar la red 1.

7.1.4 Eliminación de los bucles de enrutamiento mediante el horizonte dividido.

Otra fuente posible de bucles de enrutamiento se presenta cuando se envía información incorrecta a un router, la cual contradice información correcta que este envió originalmente. Así es como se produce el problema:

1. El router A transfiere una actualización al router B y al router D, la cual indica que la red 1 está fuera de servicio. El router C, sin embargo, transmite una actualización periódica al router B, que señala que la red 1 está disponible a una distancia de 4, a través del router D. Esto no rompe las reglas del horizonte dividido.
2. El router B determina erróneamente que el router C todavía tiene una ruta válida hacia la red 1, aunque con una métrica mucho menos favorable. El router B envía una actualización periódica al router A la cual indica al router A la nueva ruta hacia la red 1.
3. El router A ahora determina que puede enviar paquetes a la red 1 a través del router B, el router B determina que puede enviar paquetes a la red 1 a través del router C, y el router C determina que puede enviar paquetes a la red 1 a través del router D. Cualquier paquete introducido en este entorno quedará atrapado en un bucle entre los routers.
4. El horizonte dividido busca evitar esta situación. Si la actualización de enrutamiento relativa a la red 1 es enviada desde el router A, el router B o D no pueden enviar información sobre la red 1 de vuelta hacia el router A. El horizonte dividido reduce así los errores de enrutamiento, y también disminuye el procesamiento de información de enrutamiento.



7.1.5 Envenenamiento de rutas

El envenenamiento de rutas es utilizado por varios protocolos de vector-distancia para resolver grandes bucles de enrutamiento. A menudo, provee información explícita cuando no es posible el acceso a una subred o red. Esto se lleva a cabo normalmente mediante la configuración del número de saltos en la cantidad máxima más uno.

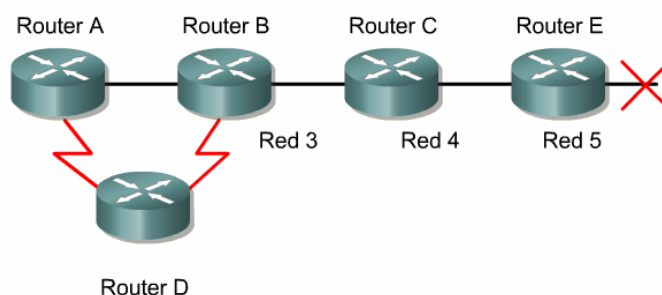


Figura 1

Una forma de evitar actualizaciones incongruentes es el envenenamiento de rutas. Cuando la red 5 sale fuera de servicio, el router E inicia el envenenamiento de la ruta, mediante una entrada de valor 16 para la red 5, es decir, fuera de alcance. **1**Debido al envenenamiento de la ruta hacia la red 5, el router C no es susceptible de efectuar actualizaciones incorrectas de la ruta hacia dicha red. Cuando el router C recibe el envenenamiento de ruta desde el Router E, envía una actualización llamada actualización de envenenamiento inversa de vuelta al router E. Esto asegura que todas las rutas del segmento hayan recibido la información del envenenamiento de la ruta.

Cuando se combina el envenenamiento de rutas con las actualizaciones generadas por eventos, se agiliza el tiempo de convergencia ya que los routers vecinos no tienen que esperar 30 segundos antes de publicar la ruta envenenada.

El envenenamiento de rutas hace que el protocolo de enrutamiento publique rutas de métrica infinita para la ruta que está fuera de servicio. El envenenamiento de rutas no rompe las reglas del horizonte dividido. El horizonte dividido con envenenamiento de rutas es en esencia un envenenamiento de rutas, pero, colocada en los enlaces en los el horizonte dividido no permitiría el paso de información de enrutamiento. En cualquiera de los casos, el resultado es que las rutas que están fuera de servicio se publican con métricas infinitas.

7.1.6 Prevención de bucles de enrutamiento mediante actualizaciones generadas por eventos

Los routers envían nuevas tablas de enrutamiento a los routers vecinos periódicamente. Por ejemplo, las actualizaciones en el protocolo RIP se producen cada 30 segundos. Sin embargo, una actualización generada por eventos es enviada de inmediato, en respuesta a algún cambio en la tabla de enrutamiento. El router que detecta un cambio de topología envía de inmediato un mensaje de actualización a los routers adyacentes, los cuales a su vez, generan actualizaciones a efectos de notificar el cambio a sus vecinos adyacentes. Cuando una ruta falla, inmediatamente se envía una actualización, sin esperar a que expiren los temporizadores de las actualizaciones. Las actualizaciones generadas por eventos, cuando se usan en conjunto con el envenenamiento de rutas, aseguran que todos los routers conozcan de la falla en las rutas, aun antes de que se cumpla el lapso de tiempo para una actualización periódica.

Las actualizaciones generadas por eventos envían actualizaciones porque la información de enrutamiento ha cambiado, no porque se ha cumplido el lapso para una actualización. El router envía otra actualización de enrutamiento a sus otras interfaces, sin esperar a que expire el temporizador de las actualizaciones de enrutamiento. Esto causa que la información acerca del estado de la ruta que ha cambiado sea enviada, y activa más rápidamente los temporizadores de espera (holddown timers) en los routers vecinos. La ola de actualizaciones se propaga a través de la red.

Mediante la actualización generada por eventos que genera el router C, éste anuncia que la red 10.4.0.0 está inaccesible. Al recibir esta información, el router B anuncia a través de la interfaz S0/1 que la red 10.4.0.0 está fuera de servicio. A su vez, el router A envía una actualización desde la interfaz Fa0/0.

7.1.7 Prevención de bucles de enrutamiento mediante temporizadores de espera

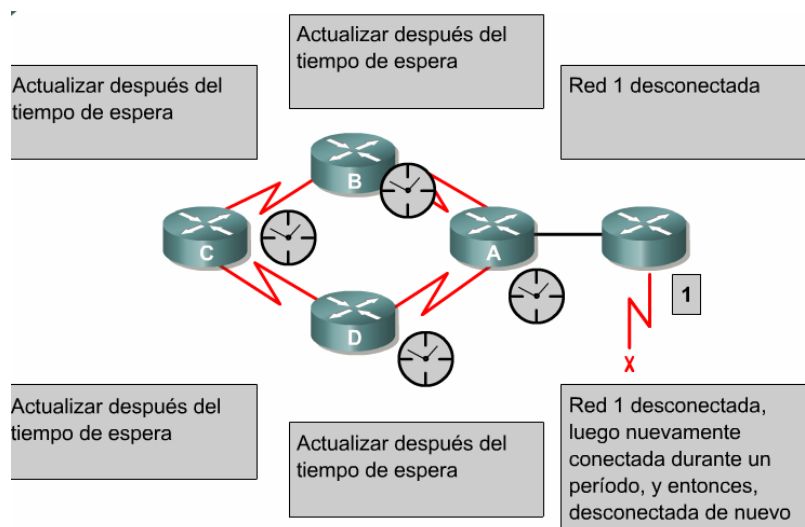


Figura 1

El problema de la cuenta al infinito puede evitarse mediante los temporizadores de espera (holddown timers): **1**

- Si un router recibe una actualización de un router vecino, la cual indique que una red previamente accesible está ahora inaccesible, el router marca la ruta como inaccesible y arranca un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del mismo router, la cual indique que la red se encuentra

nuevamente accesible, el router marca la red como accesible y desactiva el temporizador de espera.

- Si llega una actualización desde un router distinto, la cual establece una métrica más conveniente que la originalmente registrada para la red, el router marca la red como accesible y desactiva el temporizador de espera.
- Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un router distinto, la cual establece una métrica menos conveniente que la originalmente registrada para la red, la actualización no será tomada en cuenta. El descartar las actualizaciones con métricas menos convenientes mientras el temporizador de espera se encuentra activado, da más tiempo para que la información relativa a un cambio perjudicial sea transmitido a toda la red.

7.2 Protocolo RIP

7.2.1 Proceso de enrutamiento del protocolo RIP

La versión moderna del protocolo de estándar abierto RIP, a menudo denominado RIP IP, se describe formalmente en dos documentos distintos. El primero es el la Solicitud de comentarios 1058 (RFC 1058) y el segundo el Estándar de Internet 56 (STD 56). ¹

Entre las características clave de RIP se incluyen las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete se descarta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

Figura 1

RIP ha evolucionado a lo largo de los años desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Version 2 (RIP v2). Las mejoras en RIP v2 incluyen:

Capacidad para transportar mayor información relativa al enrutamiento de paquetes.

Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas.

Soporta enmascaramiento de subredes de longitud variable (VLSM).

RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea.

7.2.2 Configuración del protocolo RIP

El comando **router rip** habilita el protocolo de enrutamiento RIP. Luego se ejecuta el comando **network** para informar al router acerca de las interfaces donde RIP estará activo. A continuación, el proceso de enrutamiento asocia las interfaces específicas con las direcciones de red y comienza a enviar y a recibir actualizaciones RIP en estas interfaces.

RIP envía mensajes de actualización de enrutamiento a intervalos regulares. Cuando un router recibe una actualización de enrutamiento que incluya cambios a una entrada de su tabla de enrutamiento, actualiza la dicha tabla para reflejar la nueva ruta. El valor recibido de la métrica de la ruta aumenta en 1 y la interfaz de origen de la actualización se señala como el salto siguiente en la tabla de enrutamiento. Los routers RIP conservan sólo la mejor ruta hacia un destino pero pueden conservar más de una ruta al mismo destino si el costo de todas es igual.

La mayoría de los protocolos de enrutamiento usan una combinación de actualizaciones causadas por eventos (event-driven) o por tiempo (time-driven). RIP es time-driven, pero la implementación Cisco de RIP

envía actualizaciones tan pronto se detectan cambios. Cambios en la topología también originan actualizaciones inmediatas en routers IGRP, independientes del valor del temporizador de actualización. Sin actualizaciones event-driven RIP e IGRP no funcionarían adecuadamente. Una vez que se haya actualizado la tabla de enrutamiento por cambios en la configuración, el router comienza inmediatamente a transmitir las actualizaciones de enrutamiento, a fin de informar de estos cambios a los otros routers. Estas actualizaciones, denominadas actualizaciones generadas por eventos, se envían independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares. Por ejemplo, las descripciones de los comandos que se utilizan para configurar el router BHM que se muestra en la figura son las siguientes:

- BHM(config)#**router rip**: selecciona al RIP como protocolo de enrutamiento.
- BHM(config-router)#**network 10.0.0.0**: especifica una red conectada directamente.
- BHM(config-router)#**network 192.168.13.0**: especifica una segunda red conectada directamente.

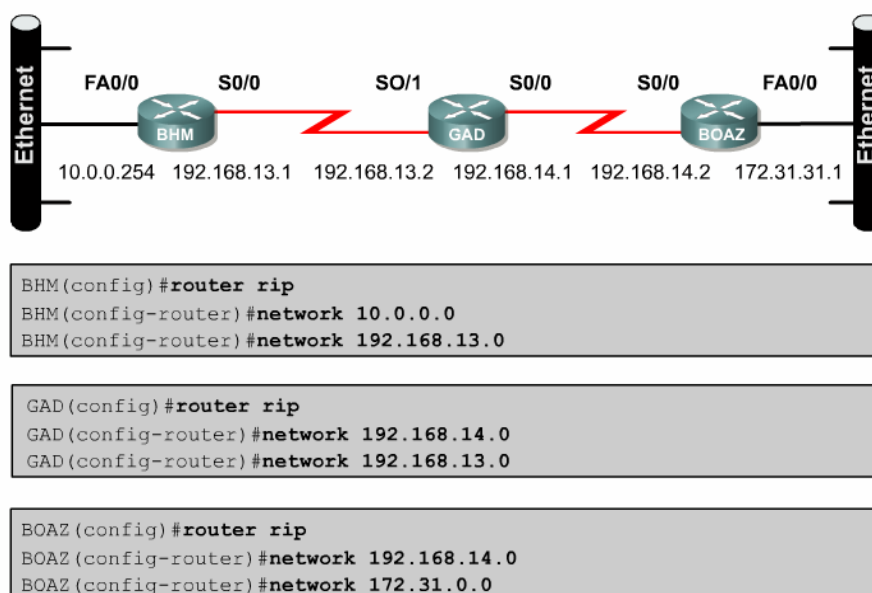
Las interfaces del router Cisco conectadas a las redes 10.0.0.0 y 192.168.13.0 envían y reciben actualizaciones RIP. Estas actualizaciones de enrutamiento permiten que el router conozca la topología de la red desde routers vecinos que también ejecutan RIP.

RIP debe estar habilitado, y las redes configuradas. Las otras tareas son opcionales. Entre las tareas opcionales se encuentran:

- Aplicar compensaciones a la métrica de enrutamiento.
- Ajustar los temporizadores.
- Especificar una versión de RIP.
- Habilitar la autenticación de RIP.
- Configurar el resumen de las rutas en una interfaz.
- Verificar el resumen de las rutas IP.
- Inhabilitar el resumen automático de rutas.
- Ejecutar IGRP y RIP al mismo tiempo.
- Inhabilitar la validación de las direcciones de IP de origen.
- Habilitar o inhabilitar el horizonte dividido.
- Conectar RIP a una WAN.

Para habilitar RIP, ejecute los siguientes comandos desde el modo de configuración global:

- Router(config)#**router rip**: habilita el proceso de enrutamiento RIP.
- Router(config-router)#**network número-de-la-red** : asocia una red al proceso de enrutamiento RIP.



7.2.3 Uso del comando ip classless

A veces, un router recibe paquetes destinados a una subred desconocida de una red que tiene interconexiones directas a subredes. Para que el IOS de Cisco envíe estos paquetes hacia la mejor ruta de super-net posible, ejecute el comando **ip classless** de configuración global. Una ruta de super-red es una ruta que abarca un ámbito más amplio de subredes mediante una sola entrada. Por ejemplo, una compañía

utiliza toda la subred 10.10.0.0 /16, entonces la ruta de super-red para 10.10.10.0 /24 sería 10.10.0.0 /16. El comando **ip classless** está habilitado por defecto en el IOS de Cisco de las versiones 11.3 y posteriores. Para inhabilitar esta función, ejecute la forma **no** de este comando.

Al inhabilitar esta función, todos los paquetes que se reciban con destino a direcciones en subredes que encajen numéricamente dentro del esquema de direcciones de la subred en el router serán desechados.

El comando **ip classless** sólo afecta la operación de los procesos del IOS relativos al envío de paquetes. El comando **ip classless** no afecta la forma en que se crea la tabla de enrutamiento. Esta es la esencia del enrutamiento con definición de clases. Si se conoce una porción de una red principal, pero no se conoce la subred de destino de un paquete dentro de dicha red principal, el paquete es desechado.

El aspecto más confuso de esta regla es que el router sólo usa la ruta por defecto si la ruta a la red principal no existe en la tabla de enrutamiento. Por defecto, un router supone que todas las subredes de una red conectada directamente deben figurar en la tabla de enrutamiento. Si se recibe un paquete cuya dirección de destino es desconocida, la cual pertenece a una subred desconocida de una red conectada directamente, el router considera que la subred no existe. De modo que el router desechará el paquete aun si existe una ruta por defecto. El configurar **ip classless** en el router resuelve este problema, al permitir que el router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto. [1](#) [2](#) [3](#)

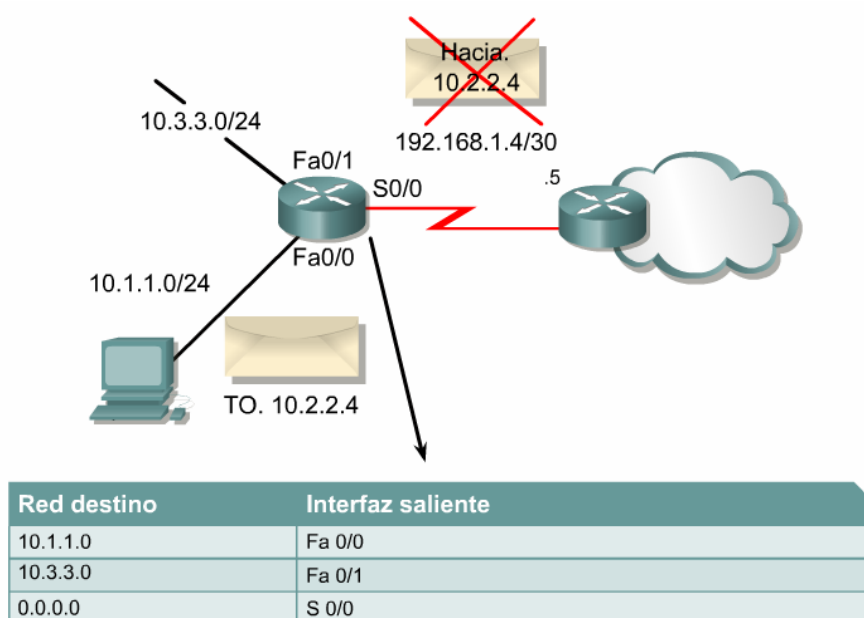


Figura 1

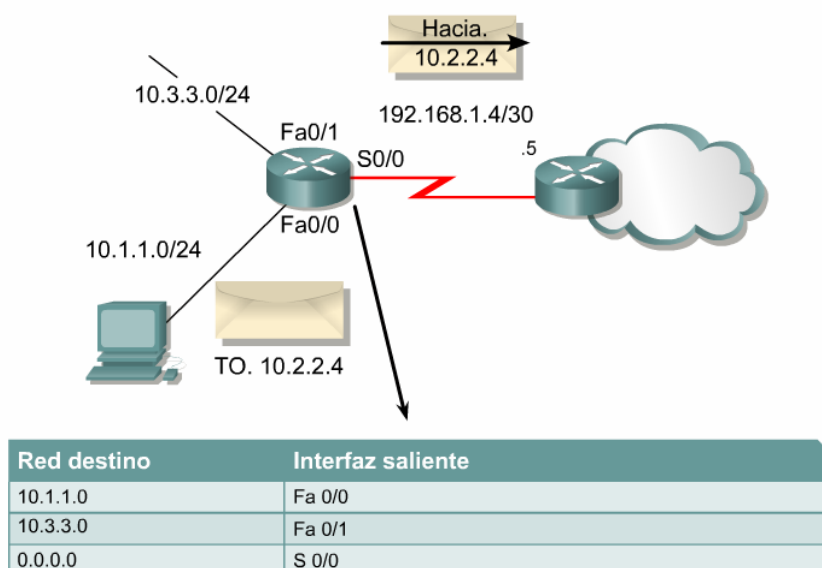


Figura 2

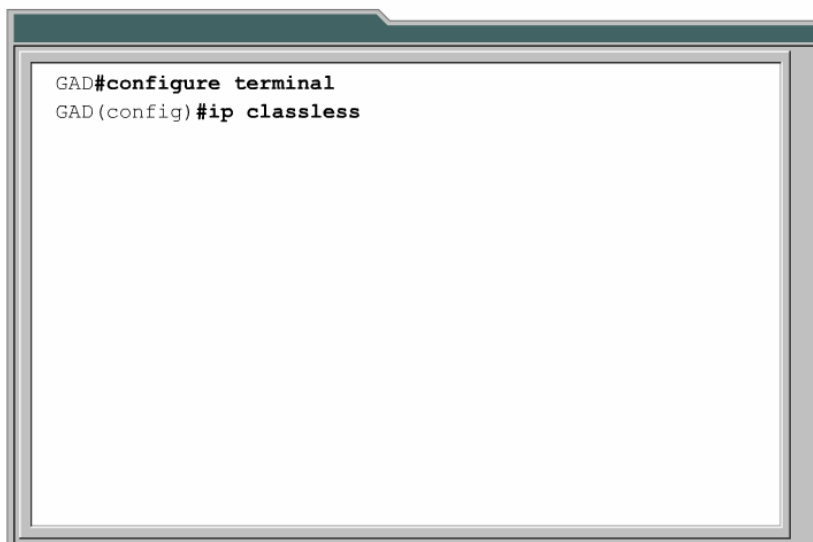


Figura 3

7.2.4 Detalles frecuentes en la configuración de RIP

Los routers RIP dependen de los routers vecinos para obtener la información de la red que no conocen de primera mano. Un término común empleado para describir esta funcionalidad es Enrutamiento por rumor. El protocolo RIP usa un algoritmo de enrutamiento por vector-distancia. Todos los protocolos de enrutamiento por vector-distancia tienen detalles importantes que son producto principalmente de una convergencia lenta. La convergencia ocurre cuando todos los routers de una red tienen la misma información de enrutamiento.

Entre estos detalles se encuentran los bucles de enrutamiento y la cuenta al infinito. Éstos generan incongruencias debido a la propagación por la red de actualizaciones de enrutamiento con información obsoleta.

Para reducir los bucles de enrutamiento y la cuenta al infinito, RIP emplea las siguientes técnicas.

- Cuenta al infinito
- Horizonte dividido
- Actualización inversa:
- Temporizadores de espera
- Actualizaciones generadas por eventos.

Algunos de estos métodos pueden requerir hacer algunas configuraciones, mientras que otros no lo requieren o rara vez lo requieren.

RIP permite un número de saltos máximo de 15. Todo destino que exceda los 15 saltos se considera como fuera de alcance. El número máximo de saltos restringe en gran medida su uso en redes de gran tamaño, pero evita que un problema llamado "cuenta al infinito" produzca bucles de enrutamiento infinitos en la red.

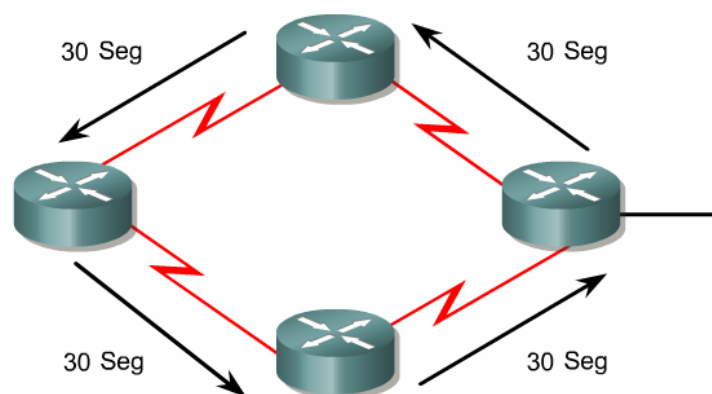
La regla de horizonte dividido se basa en la teoría que no es útil enviar información acerca de una ruta de vuelta a la dirección desde donde se originó. En algunas configuraciones de red, puede resultar necesario inhabilitar el horizonte dividido.

El siguiente comando se utiliza para inhabilitar el horizonte dividido:

GAD(config-if)#no ip split-horizon

El temporizador de espera es otro mecanismo que puede requerir algunos cambios. Los temporizadores de espera ayudan a prevenir la cuenta al infinito, pero también aumentan el tiempo de convergencia. La espera por defecto en el protocolo RIP es de 180 segundos. Esto evita que una ruta menos conveniente ingrese en la tabla de enrutamiento pero también puede evitar que se instale una ruta alternativa válida. Es posible reducir el lapso del temporizador de espera, para agilizar la convergencia pero esto se debe hacer con cautela. El ajuste ideal es el que fije el temporizador con una duración apenas mayor al lapso máximo de actualización posible de la red. En el ejemplo de la Figura 1, el bucle consta de cuatro routers. Si cada

router tiene un lapso de actualización de 30 segundos, el bucle más largo posible es de 120 segundos. Por lo tanto, el temporizador de espera debe ser apenas mayor a 120 segundos.



$$30 + 30 + 30 + 30 = 120 \text{ segundos}$$

Establecer temporizador de espera > 120 segundos

Figura 1

Use el siguiente comando para cambiar el temporizador del contador de "holddown" , así como el temporizador de actualizaciones, el intervalo de invalidez y el intervalo de desecho.

Router(config-router)#**timers basic***update invalid holddown flush [sleeptime]*

Un punto adicional que afecta el tiempo de convergencia y que puede configurarse es el intervalo entre actualizaciones. El intervalo entre actualizaciones por defecto de RIP en el IOS de Cisco es de 30 segundos. Puede configurarse para intervalos más prolongados, a fin de ahorrar ancho de banda, o más cortos para disminuir el tiempo de convergencia.

Otro detalle de los protocolos de enrutamiento es la publicación indeseada de actualizaciones del enrutamiento desde una interfaz en particular. Cuando se ejecuta un comando **network** para una red dada, RIP comenzará inmediatamente a enviar publicaciones hacia todas las interfaces dentro del ámbito de direcciones de red especificado. Para controlar cuáles serán las interfaces que harán intercambio de actualizaciones de enrutamiento, el administrador de redes puede inhabilitar el envío de actualizaciones desde las interfaces que escoja. Para ello se usa el comando **passive-interface**. [2](#)

Comando	Propósito
GAD(config-router)# passive-interface Fa0/0	Configura una interfaz para evitar que envíe paquetes RIP

Figura 2

Como RIP es un protocolo de tipo broadcast, el administrador de la red podría tener que configurar RIP para que intercambie información de enrutamiento en redes no broadcast, como en el caso de las redes Frame Relay. En este tipo de redes, RIP necesita ser informado de otros routers RIP vecinos. Para esto se utiliza el comando que se muestra en la Figura [3](#).

Comando	Propósito
GAD(config-router)# neighbor ip address	Define un router vecino con el cual puede intercambiar información de enrutamiento

Figura 3

Por defecto, el IOS de Cisco acepta paquetes de la Versión 1 y de la Versión 2 de RIP, pero sólo envía paquetes de la Versión 1. El administrador de redes puede configurar el router para que sólo reciba y envíe paquetes de la Versión 1 o para que sólo envíe paquetes de la Versión 2. A efectos de configurar el router para enviar y recibir paquetes de una sola versión, utilice los comandos de la Figura [4](#).

Comando	Propósito
<code>GAD(config-router)#version {1 2}</code>	Configura el software para recibir y enviar paquetes RIP versión 1 o versión 2
<code>GAD(config-if)#ip rip send version 1</code>	Configura una interfaz para aceptar los paquetes RIP, versión 1
<code>GAD(config-if)#ip rip send version 2</code>	Configura una interface para enviar solamente paquetes RIP versión 2
<code>GAD(config-if)#ip rip send version 1 2</code>	Configura una interfaz para enviar los paquetes RIP, versión 1 ó 2

Figura 4

Para controlar cómo se procesan los paquetes recibidos desde una interfaz, utilice los comandos de la Figura 5.

Comando	Propósito
<code>GAD(config-if)#ip rip receive version 1</code>	Configura una interface para aceptar solamente paquetes RIP versión 1
<code>GAD(config-if)#ip rip receive version 2</code>	Configura una interface para aceptar solamente paquetes RIP versión 2
<code>GAD(config-if)#ip rip receive version 1 2</code>	Configura una interface para aceptar paquetes RIP de las versiones 1 ó 2

Figura 5

7.2.5 Verificación de la configuración del protocolo RIP

Existen diversos comandos que se pueden utilizar para verificar que RIP esté correctamente configurado. Los dos comandos más comunes son el **show ip route** y el **show ip protocols**.

El comando **show ip protocols** muestra cuáles son los protocolos que transportan tráfico IP en el router. Este resultado puede utilizarse para verificar la mayor parte, si no toda, la configuración del protocolo RIP. Algunos de los aspectos de la configuración más comunes que deben ser verificados son:

- El uso del enrutamiento RIP está configurado.
- Las interfaces correctas están enviando y recibiendo las actualizaciones RIP.
- El router publica las redes correctas.

El comando **show ip route** se puede utilizar para verificar que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento. Examine el resultado del comando y busque las rutas RIP que señaladas con "R". Recuerde que la red tardará algún tiempo en converger, de modo que puede que no aparezcan las rutas de forma inmediata.

Otros comandos para verificar la configuración del protocolo RIP son los siguientes:

- **show interface***interface*
- **show ip interface***interface*
- **show running-config**

7.2.6 Detalles del diagnóstico de fallas en la actualización con protocolo RIP

La mayoría de los errores de configuración del protocolo RIP incluyen comandos de red incorrectos, subredes discontinuas u horizontes divididos. Un comando muy efectivo para detectar problemas de actualización es el **debug ip rip**.

El comando **debug ip rip** muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe. El ejemplo de la Figura 1 muestra el resultado del comando **debug ip rip** en un router, luego de recibir una actualización RIP. Después de recibir y procesar la actualización, el router envía la información recientemente actualizada hacia sus dos interfaces RIP. El resultado muestra que el router utiliza la versión 1 de RIP y que hace un broadcast de la actualización (dirección de broadcast 255.255.255.255). El número entre paréntesis representa la dirección de origen encapsulada en el encabezado IP de la actualización RIP.

Existen varios indicadores clave a inspeccionar en el resultado del comando **debug ip rip**. Problemas tales como subredes discontinuas o redes duplicadas pueden ser diagnosticadas con este comando. Un síntoma de estos problemas sería que un router publicara una ruta con una métrica más baja que la métrica que recibió de la red.

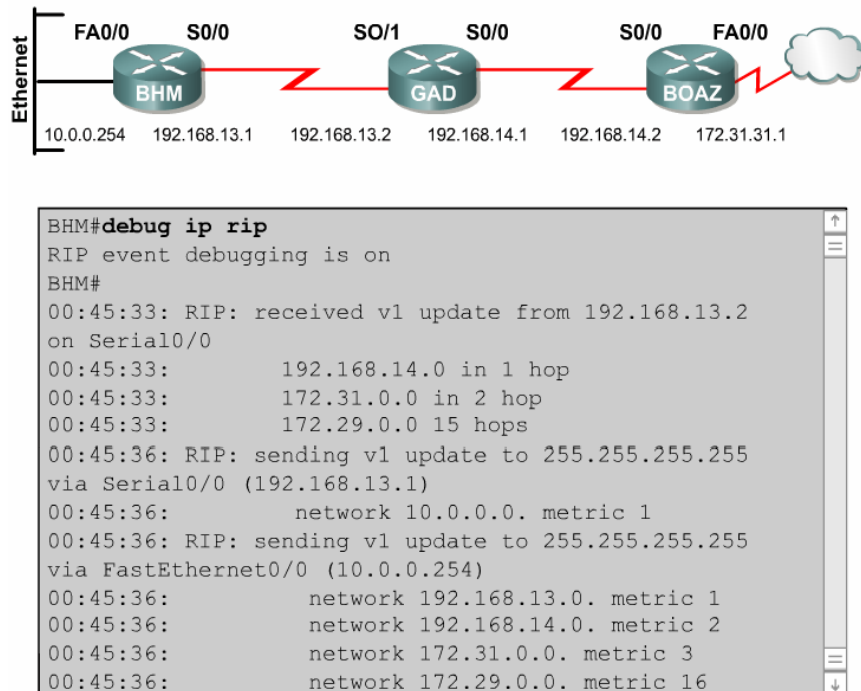


Figura 1

Otros comandos para diagnosticar fallas en el protocolo RIP son:

- **show ip rip database**
- **show ip protocols** {sumario}
- **show ip route**
- **debug ip rip** {eventos}
- **show ip interface brief**

7.2.7 Prevención del envío de actualizaciones de enrutamiento a través de una interfaz

El filtro de rutas funciona regulando las rutas que se incluyen o que se publican desde la tabla de enrutamiento. En el caso de los protocolos de enrutamiento de estado del enlace, los filtros de rutas tienen efectos diferentes a los correspondientes a los protocolos de vector-distancia. Un router que ejecuta un protocolo de vector-distancia publica rutas de acuerdo al contenido de la tabla de enrutamiento. Como resultado, el filtro de rutas tiene influencia sobre cuáles son las rutas que el router publica a sus vecinos.

Por otra parte, los routers que usan protocolos de estado del enlace determinan las rutas de acuerdo a la información en su base de datos del estado del enlace, en vez de guiarse por la tabla publicada por un router vecino. Los filtros de ruta no tienen efectos sobre las publicaciones del estado del enlace o sobre la base de datos del estado del enlace. Por este motivo, la información en este documento sólo es válida para los protocolos de enrutamiento de paquetes IP por vector-distancia tales como Protocolo de información de enrutamiento (RIP) y el Protocolo de enrutamiento de gateway interior (IGRP).

El uso del comando **passive interface** puede evitar que los routers envíen las actualizaciones de enrutamiento a través de una interfaz en particular del router. El evitar que los mensajes de actualización del enrutamiento sean enviados a través de una interfaz en particular del router impide que otros sistemas de esa red aprendan las rutas de forma dinámica. En la figura 1, el router E utiliza el comando **passive-interface** para prevenir que se envíen las actualizaciones de enrutamiento.

En los protocolos RIP e IGRP, el comando **passive interface** evita que el router envíe las actualizaciones hacia un vecino en particular, pero el router continúa recibiendo las actualizaciones de enrutamiento de dicho vecino. El evitar que los mensajes de actualización del enrutamiento sean enviados a través de una

interfaz en particular del router impide que otros sistemas conectados a esa interfaz aprendan las rutas de forma dinámica.

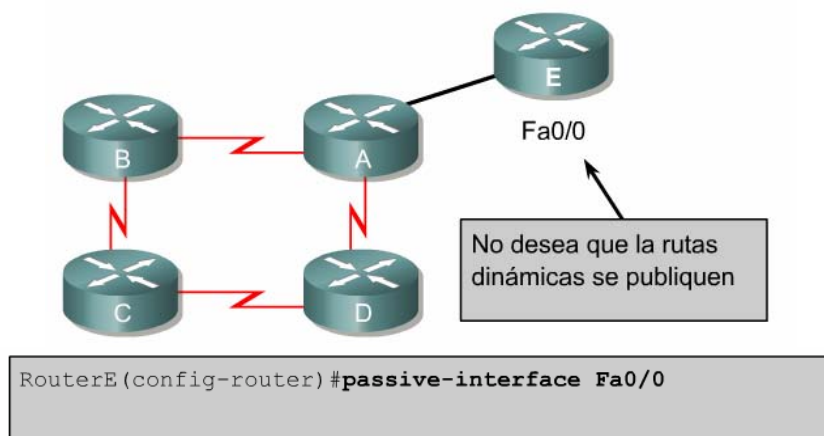


Figura 1

7.2.8 Balanceo de las cargas con el protocolo RIP

El balanceo de las cargas es un concepto que permite que un router saque ventaja de múltiples y mejores rutas hacia un destino dado. Estas rutas están definidas de forma estática por el administrador de la red o calculadas por un protocolo de enrutamiento dinámico, como RIP.

RIP es capaz de balancear las cargas hasta en seis rutas de igual costo, cuatro de ellas por defecto. RIP realiza lo que se conoce como balanceo de cargas "por turnos" o "en cadena" (round robin). Significa que RIP, envía los paquetes por turnos a través de las rutas paralelas.

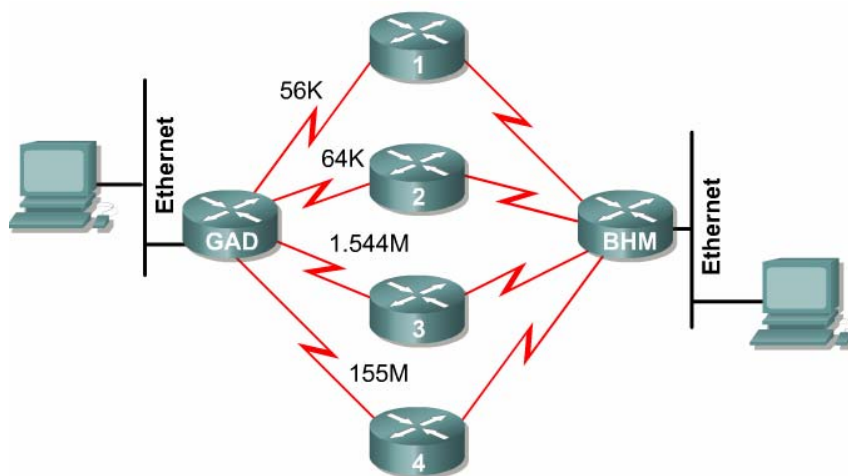


Figura 1

La Figura 1 muestra un ejemplo de rutas RIP con cuatro rutas de igual costo. El router comenzará con un apuntador hacia la interfaz conectada al router 1. Luego el apuntador iniciará un ciclo a través de las interfaces y rutas en un orden preconfigurado, por ejemplo: 1-2-3-4-1-2-3-4-1 y así sucesivamente. Como la métrica del protocolo RIP es el número de saltos, no se toma en cuenta la velocidad de los enlaces. Por lo tanto, la ruta de 56 Kbps tendrá la misma preferencia que la ruta de 155 Mbps.

Es posible encontrar rutas de igual costo mediante el comando **show ip route**. Por ejemplo, la Figura 2 muestra el resultado de **show ip route** para una subred particular con rutas múltiples.

Note que existen dos segmentos descriptores de enrutamiento. Cada bloque es una ruta. También hay un asterisco (*) al lado de uno de los segmentos. Esto corresponde a la ruta activa que se utiliza para el tráfico nuevo.

```

RouterC#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.4.2 on FastEthernet0/0,
  00:00:18 ago
  Routing Descriptor Blocks:
    192.168.4.1, from 192.168.4.1, 00:02:45 ago, via
    FastEthernet0/0
    Route metric is 1, traffic share count is 1
    * 192.168.4.2, from 192.168.4.2, 00:00:18 ago,
    via FastEthernet0/0
    Route metric is 1, traffic share count is 1

```

Figura 2

7.2.9 Equilibrio de cargas a través de rutas múltiples

El balanceo de cargas describe la capacidad de un router para transmitir paquetes a una dirección IP de destino a través de más de una ruta. El balanceo de las cargas es un concepto que permite que un router saque ventaja de múltiples y mejores rutas hacia un destino dado. Las rutas provienen de configuraciones estáticas o de protocolos dinámicos tales como RIP, EIGRP, OSPF e IGRP.

Cuando un router conoce las múltiples rutas hacia una red específica, instala la ruta de distancia administrativa más corta en la tabla de enrutamiento. ¹A veces, el router debe elegir una ruta entre las muchas que ha conocido mediante el mismo proceso de enrutamiento, y cuyas distancias administrativas son iguales. En este caso, el router elige la ruta con el costo o métrica más baja. Cada proceso de enrutamiento calcula sus costos de distinta forma y éstos pueden requerir de una configuración manual a fin de lograr el equilibrio de cargas.

Origen de la ruta de distancia administrativa	Distancia por defecto
Interfaz conectada	0
Ruta estática	1
Ruta sumaria EIGRP	5
BGP externo	20
Ruta interna EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Ruta externa EIGRP	170
BGP interno	200
Desconocido	255

Figura 1

Si el router recibe e instala rutas múltiples con los mismos valores de distancia administrativa y costo, puede activarse el balanceo de las cargas. Puede haber hasta seis rutas de igual costo (un límite impuesto por el IOS de Cisco en la tabla de enrutamiento), pero algunos Protocolos de gateway interior (IGP) tienen sus propias limitaciones. El protocolo EIGRP permite hasta cuatro rutas de igual costo.

Por defecto, la mayoría de los protocolos de enrutamiento de paquetes IP instalan un máximo de cuatro rutas paralelas en la tabla de enrutamiento. Las rutas estáticas siempre instalan seis rutas. La excepción es el protocolo BGP que, por defecto, permite sólo una ruta hacia el destino.

El número máximo de rutas es de uno a seis. Para cambiar el número máximo de rutas paralelas permitidas, utilice el siguiente comando en el modo configuración del router.

Router(config-router)#**maximum-paths** [number]

El protocolo IGRP puede balancear las cargas hasta en seis enlaces distintos. Las redes RIP deben disponer de rutas con el mismo número de saltos para efectuar el balanceo de las cargas, mientras que el protocolo IGRP usa el ancho de banda para determinar el esquema de balanceo de cargas.

Existen tres formas para llegar a la red X: 2

- De E a B a A, con una métrica de 30
- De E a C a A, con una métrica de 20
- DE E a D a A, con una métrica de 45

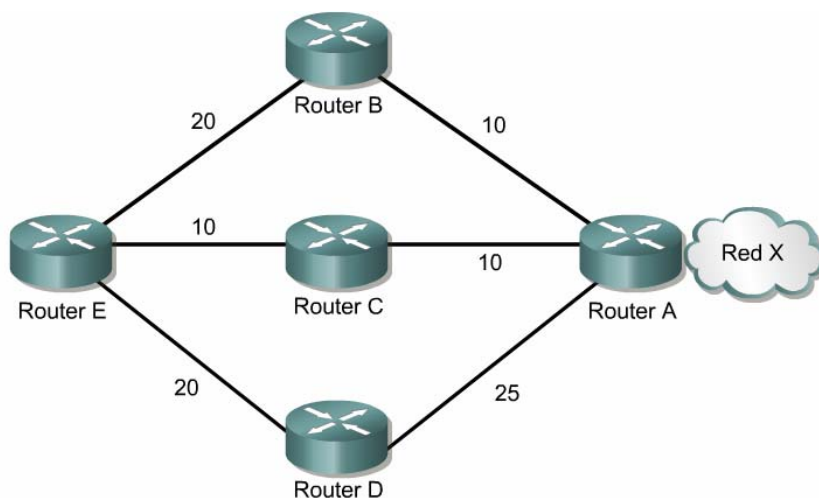


Figura 2

El router E elige la segunda ruta, E-C-A, con una métrica de 20 ya que su costo es inferior a 30 y 45.

El software Cisco IOS soporta dos métodos de balanceo de carga de paquetes IP. Estos son balanceo de carga por paquete o balanceo de carga por destino. Si está habilitado el método de conmutación conocido como process switching, el router alternará los caminos paquete a paquete. Si el método de conmutación conocido como fast switching está habilitado, solamente una de las rutas se guardará en la memoria cache para la red de destino. Todos los paquetes dirigidos a un host específico tomarán el mismo camino. Los paquetes dirigidos a hosts distintos en la misma red pueden usar una ruta alternativa. El tráfico se balancea de acuerdo al destino.

Por defecto, el router usa balanceo de cargo por destino también llamado fast switching. El cache de las rutas permite que los paquetes salientes sean balanceados por destino y no por paquete. Para deshabilitar fast switching, use el comando **no ip route-cache**. El usar este comando permitirá que los paquetes sean balanceados por paquete.

7.2.10 Integración de las rutas estáticas con el protocolo RIP

Las rutas estáticas son rutas definidas por el usuario, que obligan a los paquetes a tomar una ruta determinada entre su origen y su destino. Las rutas estáticas adquieren importancia si el IOS de Cisco no aprende una ruta hacia un destino en particular. Son útiles también para especificar "un gateway de último recurso", el cual generalmente se conoce como una ruta por defecto. Si un paquete tiene como destino una subred que no aparece expresamente en la tabla de enrutamiento, el paquete es enviado a través de una ruta por defecto.

Un router que ejecuta el protocolo RIP puede recibir una ruta por defecto a través de una actualización de otro router que ejecuta RIP. Otra opción es que el router genere, por sí mismo la ruta por defecto.

Las rutas estáticas pueden eliminarse con el comando de configuración global **no ip route**. El administrador puede dejar de lado una ruta estática y dar prioridad a la información de enrutamiento dinámico mediante el ajuste de los valores de distancia administrativa. Cada protocolo de enrutamiento dinámico tiene una distancia administrativa (AD) por defecto. Es posible definir una ruta estática como menos conveniente que una ruta aprendida de forma dinámica, siempre que la AD de la ruta estática sea mayor que la de la ruta dinámica. Note que después de configurar la ruta estática a la red 172.16.0.0 vía 192.168.14.2, la tabla de

enrutamiento no la muestra. Se muestran únicamente las rutas dinámicas aprendidas mediante RIP. Esto se debe a que la AD es mayor (130) para las rutas estáticas, y al menos que la ruta RIP en S0/0 se pierda, no será instalada en la tabla de enrutamiento. ¹

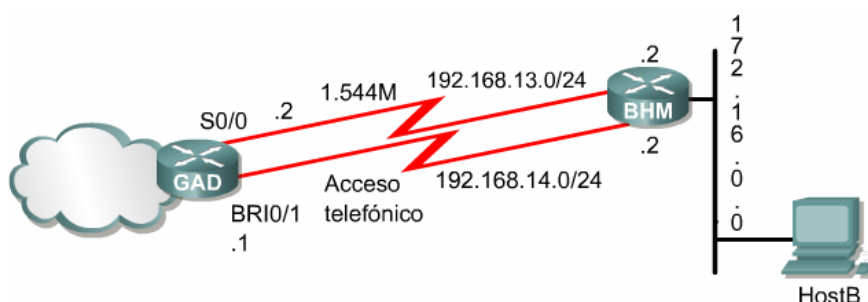


Figura 1

Las rutas estáticas que señalan una interfaz serán publicadas a través del router propietario de las rutas estáticas, y se propagarán por toda la red. Esto se debe a que las rutas estáticas que apuntan a una interfaz se consideran en la tabla de enrutamiento como conectadas, y por ello pierden su naturaleza estática en la actualización. Si se asigna una ruta estática a una interfaz que no está definida en el proceso RIP, mediante el comando **network**, RIP no publicará la ruta a menos que se especifique un comando **redistribute static** en el proceso de RIP.

Cuando una interfaz sale fuera de servicio, todas las rutas estáticas que apuntan a ella son eliminadas de la tabla de enrutamiento de paquetes IP. De igual forma, cuando el IOS no puede encontrar un salto siguiente válido para la dirección especificada en la ruta estática, la ruta es eliminada de la tabla de enrutamiento de paquetes IP.

En la Figura ², se ha configurado una ruta estática en el router GAD para que tome el lugar de la ruta dinámica RIP en caso de fallas en el proceso de enrutamiento RIP. Esto se conoce como ruta estática flotante. La configuración de la ruta estática flotante indica una AD de (130) superior a la AD por defecto de la creada por RIP (120). El router BHM también necesita disponer de una ruta por defecto.

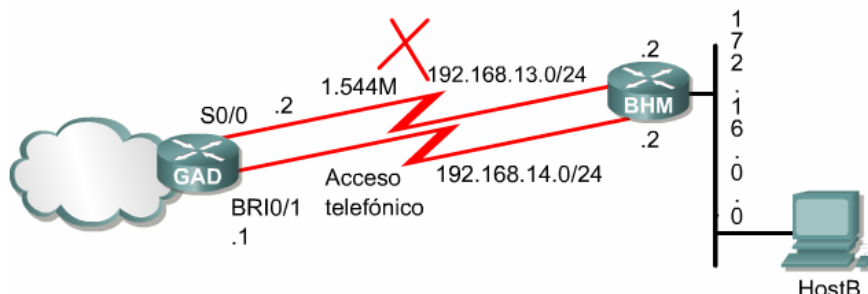


Figura 2

Para configurar una ruta estática, ejecute el comando de la Figura ³ en el modo de configuración global.

Comando	Propósito
<code>ip route destination mask {interface/nexthop}</code>	Establecer una ruta estática

Figura 3

7.3 Protocolo IGRP

7.3.1 Características del protocolo IGRP

IGRP es un protocolo de enrutamiento de gateway interior (IGP) por vector-distancia. Los protocolos de enrutamiento por vector-distancia comparan matemáticamente las rutas al medir las distancias. Dicha medición se conoce como vector-distancia. Los routers que usan los protocolos de vector-distancia deben enviar toda o parte de su tabla de enrutamiento en un mensaje de actualización de enrutamiento, a

intervalos regulares y a cada uno de sus routers vecinos. A medida que se propaga la información de enrutamiento por toda la red, los routers realizan las siguientes funciones:

- Identificar nuevos destinos.
- Conocer de fallas.

IGRP es un protocolo de enrutamiento de vector-distancia desarrollado por Cisco. IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, las cuales publican las redes de un sistema autónomo en particular. Las características claves de IGRP son las siguientes:

- La versatilidad para manejar automáticamente topologías indefinidas y complejas.
- La flexibilidad necesaria para segmentarse con distintas características de ancho de banda y de retardo.
- La escalabilidad para operar en redes de gran tamaño

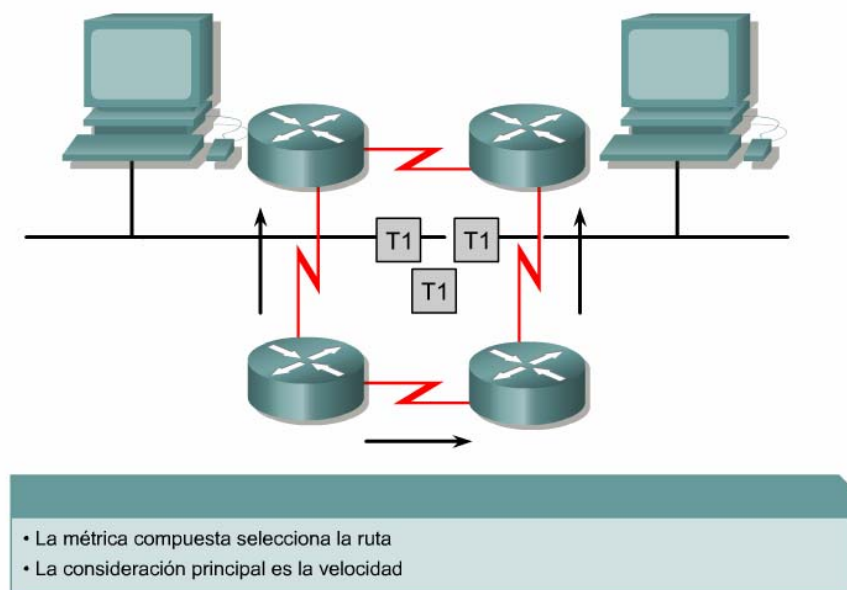


Figura 1

Por defecto, el protocolo IGRP de enrutamiento usa el ancho de banda y el retardo como métrica. ¹ Además, IGRP puede configurarse para utilizar una combinación de variables para calcular una métrica compuesta. Estas variables incluyen:

- Ancho de banda
- Retardo
- Carga
- Confiabilidad

7.3.2 Métricas de IGRP

El comando **show ip protocols** muestra los parámetros, los filtros y la información de la red relacionada con los protocolos de enrutamiento que están en uso en el router. El algoritmo utilizado para calcular la métrica de enrutamiento para IGRP se muestra en los gráficos. Define el valor de las métricas K1-K5, y proporciona información sobre el máximo número de saltos. La métrica K1 representa el ancho de banda y la métrica K3 representa el retardo. Por defecto, los valores de las métricas K1 y K3 se fijan en 1, mientras que K2, K4 y K5 se fijan en 0.

Esta métrica compuesta es más precisa que la métrica del número de saltos que usa RIP para elegir una ruta hacia un destino. La ruta de menor valor métrico es la mejor.

Las métricas que utiliza el protocolo IGRP son:

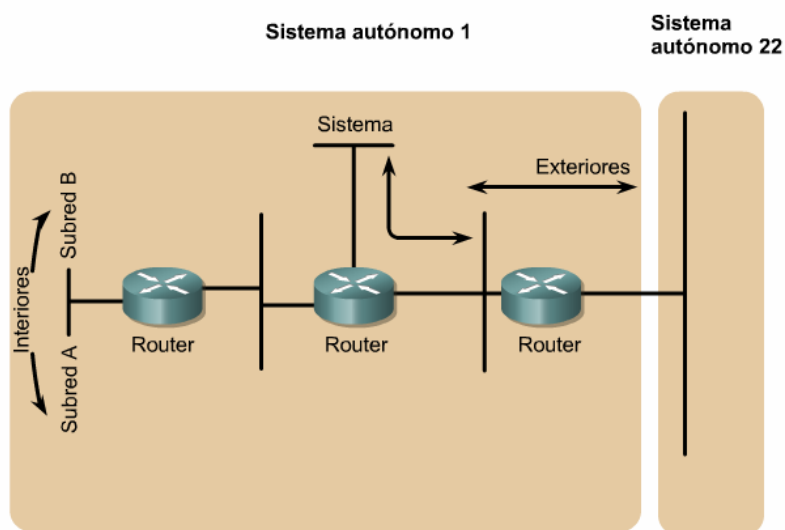
- **Ancho de banda:** el menor valor de ancho de banda en la ruta.
- **Retardo:** el retardo acumulado de la interfaz a lo largo de la ruta.
- **Confiabilidad:** la confiabilidad del enlace hacia el destino, según sea determinada por el intercambio de mensajes de actividad (keepalives).
- **Carga:** la carga sobre un enlace hacia el destino, medida en bits por segundos.

IGRP utiliza una métrica compuesta. Esta métrica se calcula como función del ancho de banda, el retardo, la carga y la confiabilidad. Por defecto, sólo se considera el ancho de banda y el retardo. Los parámetros restantes sólo se consideran si se habilitan a través de la configuración. El retardo y el ancho de banda no son valores medidos, sino que se fijan a través de los comandos de interfaces relativos al ancho de banda y al retardo. El comando **show ip route** del ejemplo muestra entre corchetes los valores de la métrica de IGRP. Un enlace de mayor ancho de banda tendrá una métrica de menor valor y una ruta con menor retardo acumulado tendrá una métrica de menor valor.

7.3.3 Rutas IGRP

IGRP publica tres tipos de rutas:

- Interiores
- Del sistema
- Exteriores



Interiores

Las rutas interiores son rutas entre subredes de la red conectada a una interfaz de un router. Si la red que está conectada a un router no está dividida en subredes, IGRP no publica rutas interiores.

Sistema

Las rutas del sistema son rutas hacia redes ubicadas dentro de un sistema autónomo. El IOS de Cisco deriva rutas de sistema de las interfaces de red conectadas directamente y de la información de rutas de sistema suministrada por otros routers que ejecutan IGRP o por servidores de acceso. Las rutas de sistema no incluyen información acerca de las subredes.

Exteriores

Las rutas exteriores son rutas hacia redes fuera del sistema autónomo, las cuales se tienen en cuenta al identificar un gateway de último recurso. El IOS de Cisco elige un gateway de último recurso de la lista de rutas exteriores que suministra IGRP. El software usa el gateway (router) de último recurso si no se encuentra una ruta mejor y si el destino no es una red conectada. Si el sistema autónomo tiene más de una conexión hacia una red externa, cada router puede seleccionar un router exterior diferente como gateway de último recurso.

7.3.4 Características de estabilidad del protocolo IGRP

IGRP ofrece una serie de funciones diseñadas para mejorar su estabilidad, por ejemplo:

- Lapsos de espera.
- Horizontes divididos.
- Actualizaciones inversas envenenadas.

Lapsos de espera.

Los lapsos de espera se utilizan para evitar que los mensajes periódicos de actualización puedan reinstalar erróneamente una ruta que podría estar fuera de servicio. Cuando un router sale de servicio, los routers vecinos detectan ese evento por la falta de mensajes de actualización periódicos.

Horizontes divididos.

Los horizontes divididos se originan en la premisa que dice que no es útil enviar información acerca de una ruta de vuelta a la dirección desde donde se originó. La técnica del horizonte dividido ayuda a prevenir los bucles de enrutamiento entre router adyacentes.

Actualizaciones inversas envenenadas.

Las actualizaciones inversas envenenadas son necesarias para romper los bucles de enrutamiento de mayor envergadura. En general, los aumentos en las métricas de enrutamiento señalan la presencia de bucles. Entonces, se envían actualizaciones inversas envenenadas para eliminar la ruta y colocarla en espera. En IGRP, las actualizaciones inversas envenenadas se envían sólo si la métrica de la ruta ha aumentado en un factor de 1,1 o más.

IGRP también mantiene un cierto número de temporizadores y de variables que contienen los intervalos de tiempo. Estos incluyen un temporizador de actualizaciones, un temporizador de caída del servicio, un temporizador de espera y un temporizador de purga.

El temporizador de actualizaciones especifica a qué frecuencia se deben enviar los mensajes de actualización de enrutamiento. Por defecto, en IGRP el valor de esta variable es de 90 segundos.

El temporizador de caída del servicio especifica cuánto tiempo debe esperar un router ante la ausencia de mensajes de actualización de enrutamiento en relación a una ruta específica antes de declarar que está fuera de servicio. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones.

El temporizador de espera especifica la cantidad de tiempo durante el cual no se toma en cuenta la información sobre rutas menos convenientes. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones, más 10 segundos.

Por último, el temporizador de purga indica cuánto tiempo debe transcurrir antes de que se purgue una ruta de la tabla de enrutamiento. Por defecto, es siete veces el lapso de las actualizaciones del temporizador de enrutamiento.

En la actualidad se hace evidente la antigüedad de IGRP, ya que carece de capacidades para manejar máscaras de subred de longitud variable (VLSM). Antes que desarrollar un IGRP versión 2 para corregir este problema, Cisco se ha apoyado en el legado de éxito de IGRP para desarrollar el Enhanced IGRP (IGRP mejorado).

7.3.5 Configuración del protocolo IGRP

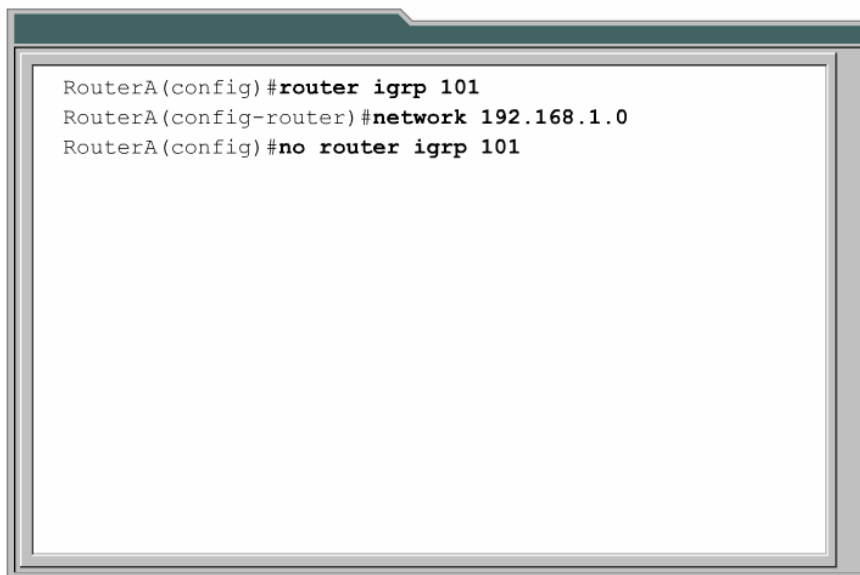


Figura 1

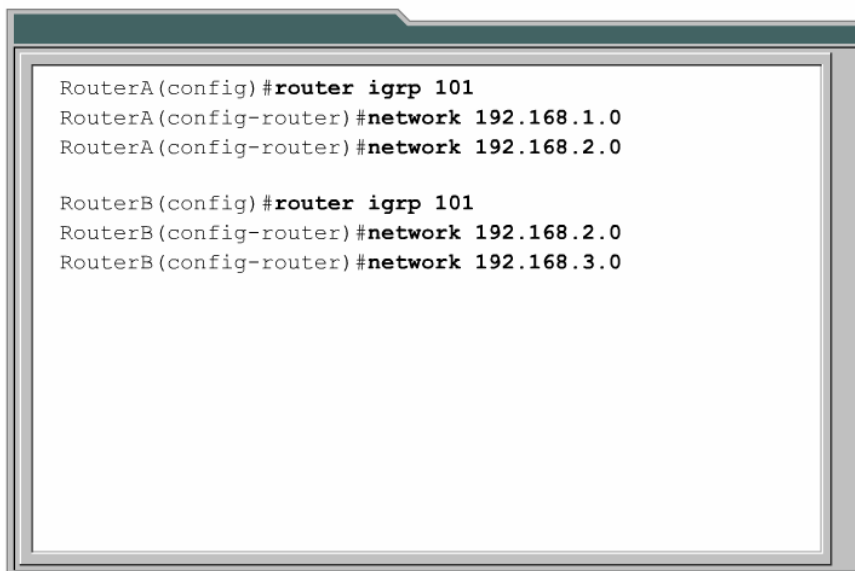
Para configurar un proceso de enrutamiento IGRP, use el comando de configuración **router igrp**. Para desactivar un proceso de enrutamiento IGRP, use la forma **no** del comando. ¹

```
RouterA(config)#router igrpas-number  
RouterA(config)#no router igrpas-number
```

El número de Sistema Autónomo (AS) identifica el proceso IGRP. También se utiliza para marcar la información de enrutamiento.

Para especificar una lista de redes para los procesos de enrutamiento IGRP, use el comando **network** de configuración del router. Para eliminar una entrada, utilice la forma **no** del comando.

La Figura 2 es un ejemplo de cómo configurar IGRP mediante AS 101.

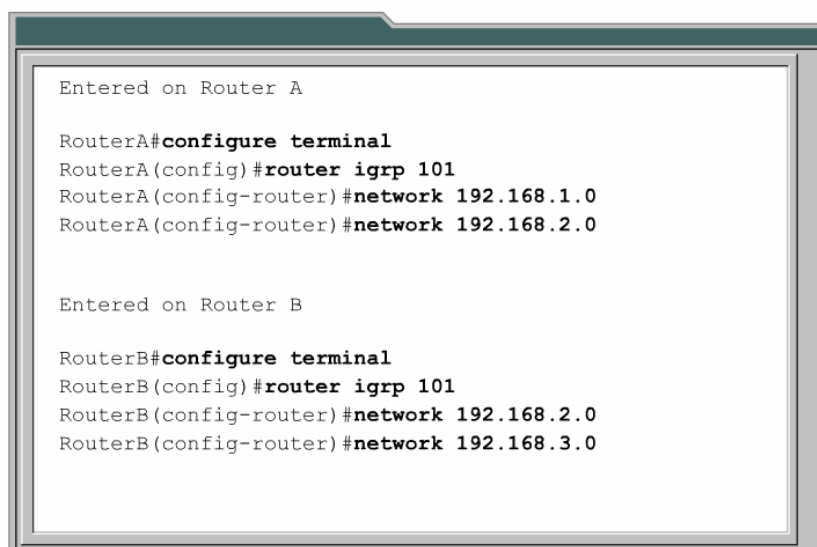


```
RouterA(config) #router igrp 101  
RouterA(config-router) #network 192.168.1.0  
RouterA(config-router) #network 192.168.2.0  
  
RouterB(config) #router igrp 101  
RouterB(config-router) #network 192.168.2.0  
RouterB(config-router) #network 192.168.3.0
```

Figura 2

7.3.6 Migración de RIP a IGRP

Con el desarrollo de IGRP a principios de los años ochenta, Cisco Systems fue la primera compañía en resolver los problemas asociados al uso de RIP para enrutar datagramas entre routers interiores. IGRP determina la mejor ruta a través de la red mediante el examen del ancho de banda y el retardo de las redes entre los routers. IGRP converge más velozmente que RIP, evitando de esta manera los bucles de enrutamiento causados por desacuerdos respecto al salto que se debe realizar a continuación. Más aún, IGRP no comparte la limitación de número máximo de saltos que tiene RIP. Como resultados de lo anterior y de otras mejoras que aventajan a RIP, IGRP hizo posible la instalación de muchas redes de diversas topologías, complejas y de gran tamaño.



```
Entered on Router A  
  
RouterA#configure terminal  
RouterA(config) #router igrp 101  
RouterA(config-router) #network 192.168.1.0  
RouterA(config-router) #network 192.168.2.0  
  
Entered on Router B  
  
RouterB#configure terminal  
RouterB(config) #router igrp 101  
RouterB(config-router) #network 192.168.2.0  
RouterB(config-router) #network 192.168.3.0
```

Figura 1

Estos son los pasos a seguir para efectuar una conversión de RIP a IGRP:

1. Usando el comando **show ip route**, verifique el protocolo de enrutamiento en uso (RIP) en los routers que se van a convertir.
2. Configure IGRP en el router A y en el router B [1](#)
3. Ejecute **show ip protocols** en el router A y en el router B
4. Ejecute **show ip route** en el router A y en el router B

7.3.7 Verificación de la configuración de IGRP

Para verificar que se haya configurado correctamente IGRP, ejecute el comando **show ip route** y observe las rutas IGRP señaladas con una "I".

Los comandos adicionales para verificar la configuración del IGRP son los siguientes:

- **show interface interface**
- **show running-config**
- **show running-config interface interface**
- **show running-config | begin interface interface**
- **show running-config | begin igrp**
- **show ip protocols**

Para verificar que la interfaz Ethernet está correctamente configurada, ejecute el comando **show interface fa0/0**.

Para determinar si el protocolo IGRP está habilitado en el router, ejecute el comando **show ip protocols**.

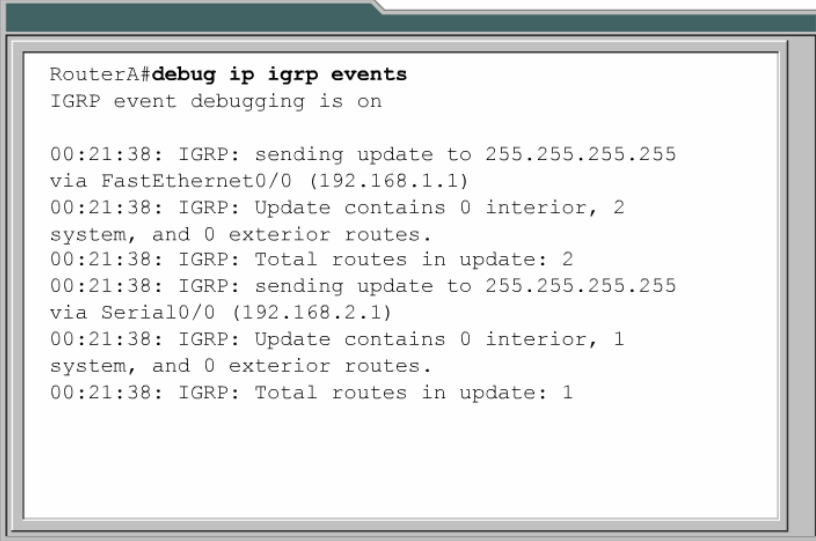
7.3.8 Diagnóstico de fallas de IGRP

La mayoría de los errores de configuración de IGRP son comandos de red mal tecleados, subredes discontinuas o un número de sistema autónomo incorrecto.

Los siguientes comandos son útiles en el diagnóstico de fallas en IGRP:

- **show ip protocols**
- **show ip route**
- **debug ip igrp events**
- **debug ip igrp transactions**
- **ping**
- **traceroute**

La Figura [1](#) muestra el resultado del comando **debug ip igrp events**.

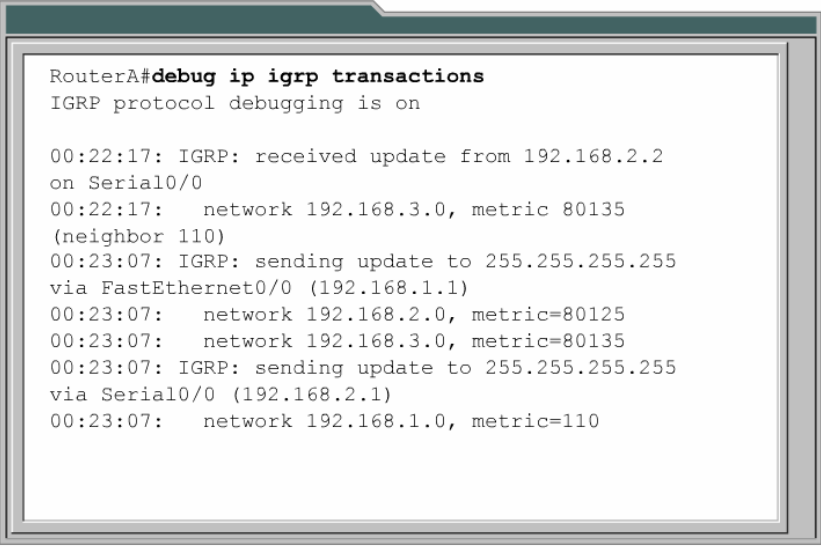


```
RouterA#debug ip igrp events
IGRP event debugging is on

00:21:38: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:21:38: IGRP: Update contains 0 interior, 2
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 1
```

Figura 1

La Figura [2](#) muestra el resultado del comando **debug ip igrp transactions**.



```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on

00:22:17: IGRP: received update from 192.168.2.2
on Serial0/0
00:22:17:   network 192.168.3.0, metric 80135
(neighbor 110)
00:23:07: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:23:07:   network 192.168.2.0, metric=80125
00:23:07:   network 192.168.3.0, metric=80135
00:23:07: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:23:07:   network 192.168.1.0, metric=110
```

Figura 2

Se determinó que el número de AS en uso era incorrecto.

Resumen

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

- Cómo se mantiene la información de enrutamiento a través de los protocolos de vector-distancia.
- Cómo se producen los bucles de enrutamiento al usar protocolos de vector-distancia.
- Definición de un número máximo de saltos para evitar la cuenta al infinito.
- Eliminar los bucles de enrutamiento mediante el horizonte dividido.
- Envenenamiento de rutas
- Evitar bucles de enrutamiento con actualizaciones generadas por eventos
- Prevenir bucles de enrutamiento con temporizadores de espera
- Prevenir las actualizaciones de enrutamiento a través de una interfaz.
- Equilibrio de cargas entre rutas múltiples.
- Proceso del protocolo RIP.
- Configuración del protocolo RIP.
- Uso del comando **ip classless**.
- Detalles frecuentes en la configuración de RIP.
- Equilibrio de cargas con el protocolo RIP.
- Integración de rutas estáticas con el protocolo RIP.
- Verificación de la configuración del protocolo RIP.
- Características del protocolo IGRP.
- Métricas del protocolo IGRP.
- Rutas IGRP.
- Características de estabilidad de IGRP.
- Configuración del protocolo IGRP.
- Migración de RIP a IGRP.
- Verificación de la configuración del protocolo IGRP.
- Diagnóstico de fallas del protocolo IGRP.

Módulo 8: Mensajes de control y error del conjunto TCP/IP

Descripción general

El protocolo IP es limitado porque es un sistema de entrega de mejor esfuerzo. No dispone de un mecanismo para garantizar la entrega de los paquetes de datos, a pesar de los problemas con los que se puedan encontrar en la red. Los paquetes pueden no llegar a su destino por diversas razones, tales como fallas de hardware, configuración inadecuada o información de enrutamiento incorrecta. Para ayudar a identificar estas fallas, el IP usa el Protocolo de mensajes de control en Internets (ICMP), para notificar al emisor de los paquetes que se produjo un error durante el proceso de envío. Este módulo describe los diversos tipos de mensajes de error del ICMP y algunas de las formas en las que se utilizan.

Dado que el protocolo IP no cuenta con un mecanismo incorporado para enviar mensajes de error y control, usa ICMP para enviar y recibir mensajes de error y control a los hosts de la red. Este módulo se refiere principalmente a los mensajes de control, que son los mensajes que suministran información o parámetros de configuración a los hosts. El conocimiento de los mensajes de control del ICMP es una parte esencial del diagnóstico de fallas de la red y es un elemento clave para lograr una comprensión absoluta de las redes IP.

Los estudiantes que completen este módulo deberán ser capaces de:

- Describir el protocolo ICMP
- Describir el formato de mensajes del ICMP
- Identificar los tipos de mensajes de error del ICMP
- Identificar las causas potenciales de mensajes de error específicos
- Describir los mensajes de control del ICMP
- Identificar diversos mensajes de control del ICMP que se usan actualmente en las redes
- Determinar las causas de los mensajes de control del ICMP

8.1 Descripción general de los mensajes de error del TCP/IP

8.1.1 Protocolo de mensajes de control de Internets (ICMP)

El IP es un método poco confiable para la entrega de paquetes de red. Se le conoce como un mecanismo de entrega de mejor esfuerzo. No cuenta con ningún proceso incorporado para garantizar la entrega de paquetes en caso de que se produzca un problema de comunicación en la red. Si un dispositivo que actúa como intermediario falla como por ejemplo un router, o si un dispositivo de destino sale fuera de la red, los paquetes no se pueden entregar. Además, nada en su diseño básico hace que el IP notifique al emisor de que la transmisión ha fallado. El Protocolo de control de mensajes de Internet (ICMP) es el componente del conjunto de protocolos TCP/IP que corrige esta limitación básica del IP. ¹El ICMP no resuelve los problemas de falta de confiabilidad en el protocolo IP. En caso de ser necesario, la confiabilidad debe ser prevista por los protocolos de capa superior.

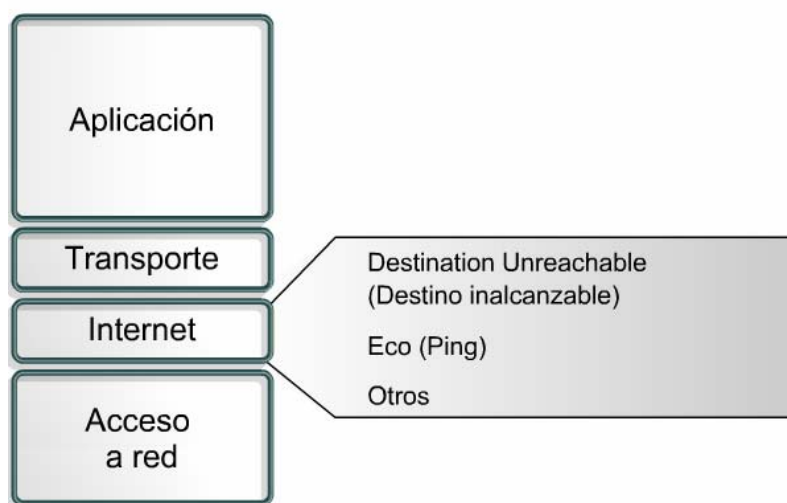


Figura 1

8.1.2 Informes de error y corrección de errores

El ICMP es un protocolo de notificación de errores para el protocolo IP. Cuando se produce un error en la entrega de datagramas, se usa el ICMP para notificar de dichos errores a la fuente de los datagramas. Por ejemplo, si la estación de trabajo 1 de la Figura 1 envía un datagrama a la estación de trabajo 6, pero la interfaz Fa0/0 del router C deja de funcionar, el router C utiliza ICMP para enviar un mensaje de vuelta a la estación de trabajo 1, el cual notifica que el datagrama no se pudo entregar. El ICMP no corrige el problema en la red; sólo informa del problema.

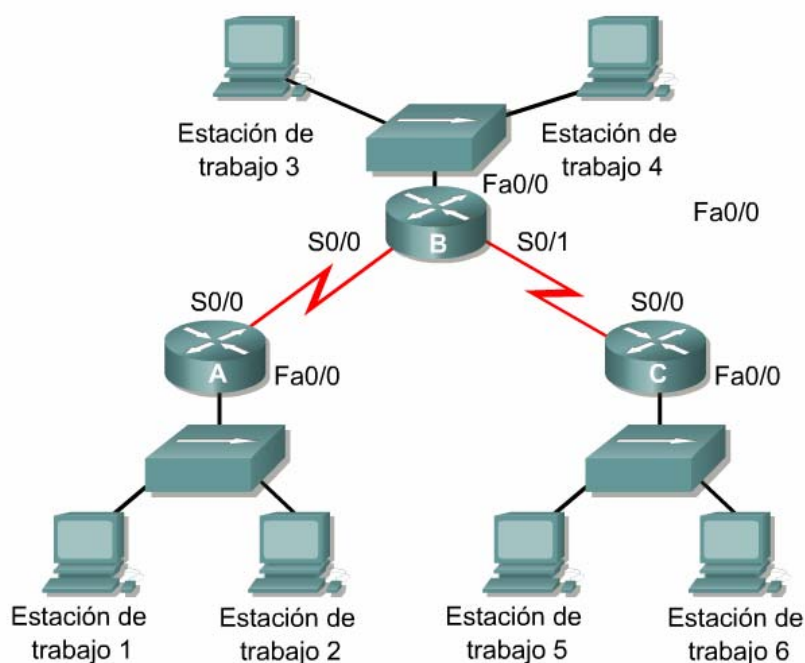


Figura 1

Cuando el router C recibe el datagrama de la estación de trabajo 1, sólo conoce las direcciones de IP de origen y destino del datagrama. No sabe cuál es la ruta exacta que tomó el datagrama en su camino hacia él. Por lo tanto, el router C sólo puede notificar a la estación de trabajo 1 acerca de la falla, y no se envía ningún mensaje de error ICMP al router A y al router B. El ICMP sólo informa al dispositivo de origen acerca del estado del paquete. No envía ninguna información sobre cambios en la red a los routers.

8.1.3 Entrega de mensajes ICMP

Los mensajes del ICMP se encapsulan en datagramas, del mismo modo en que se entrega cualquier otro dato mediante el protocolo IP. La Figura 1 muestra el encapsulamiento de datos ICMP dentro de un datagrama IP.

Encabezado de trama	Encabezado de datagrama	Encabezado ICMP	Datos ICMP
Encabezado de trama	Encabezado de datagrama	Área de datos del datagrama	
Encabezado de trama	Área de datos de la trama		

Figura 1

Dado que los mensajes del ICMP se transmiten del mismo modo que cualquier otro paquete, están sujetos a las mismas fallas en la entrega. Esto crea una situación en la que los informes de error pueden generar más informes de error, lo que provoca una congestión creciente en una red que ya tiene fallas. Por esta razón, las fallas relativas a los mensajes del ICMP no generan sus propios mensajes de ICMP. De este modo, es posible que haya un error de entrega cuyo informe no llegue nunca de vuelta al emisor de los datos.

8.1.4 Redes fuera de alcance

Las comunicaciones en una red dependen de que se cumpla determinadas condiciones básicas. En primer lugar, los dispositivos emisor y receptor deben disponer de la pila del protocolo TCP/IP debidamente configurada. Esto incluye la instalación del protocolo TCP/IP y de la configuración adecuada de la dirección de IP y la máscara de subred. También se debe configurar una puerta de enlace predeterminada (también conocido como gateway por defecto), si va a haber envío de datagramas fuera de la red local. En segundo lugar, se debe proveer de dispositivos que actúen como intermediarios, para el enrutamiento de los datagramas desde el dispositivo y la red de origen hacia la red de destino. Los routers cumplen esta función. El router también debe disponer del protocolo TCP/IP debidamente configurado en sus interfaces y debe usar un protocolo de enrutamiento adecuado.

Si no se cumplen estas condiciones, no se puede realizar la comunicación entre redes. Por ejemplo, el dispositivo emisor puede dirigir el datagrama a una dirección de IP inexistente o a un dispositivo de destino que está fuera de la red. Los routers también pueden ser puntos de falla si la interfaz de conexión está desactivada o si el router no cuenta con la información necesaria para detectar la red de destino. Si la red de destino no está accesible, se dice que es una red que está fuera de alcance.

La Figura 1 muestra un router que recibe un paquete, el cual no puede enviar a su destino final. No se puede entregar el paquete porque no existe ninguna ruta conocida hacia el destino. Por ello, el router envía al origen un mensaje ICMP llamado de host fuera de alcance.

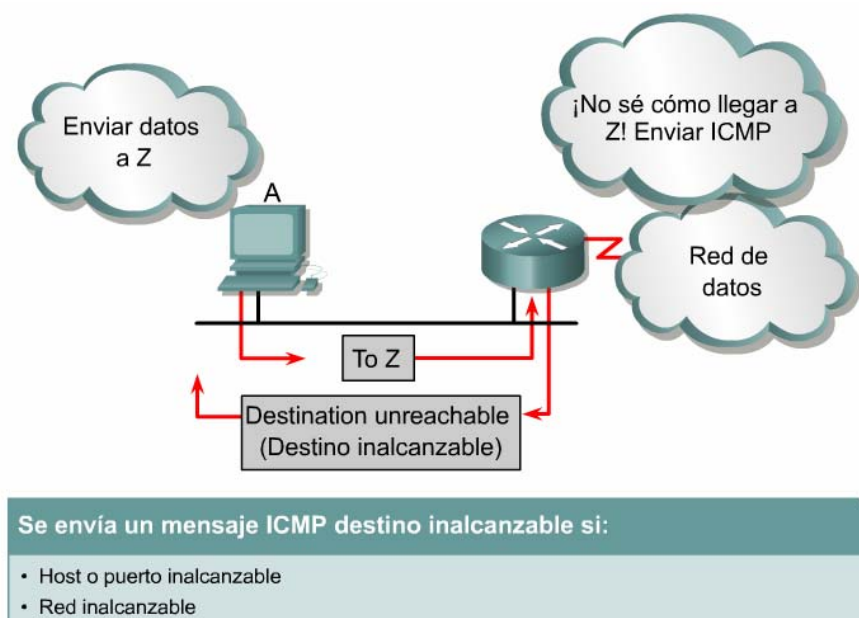


Figura 1

8.1.5 Uso de ping para verificar el estado del destino

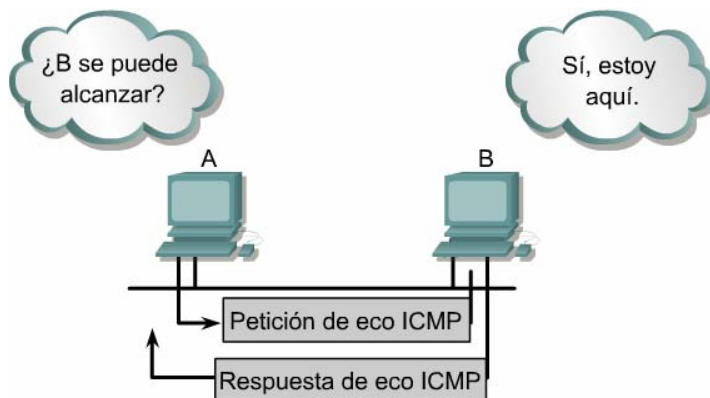


Figura 1

El protocolo ICMP se puede usar para verificar el estado de un destino en particular. La Figura 1 muestra el uso del ICMP para emitir un mensaje de solicitud de eco a un dispositivo de destino. Si el dispositivo de

destino recibe la petición de eco, crea un mensaje de respuesta el cual es enviado de vuelta al origen de la petición. Si el emisor recibe la respuesta, confirma que el dispositivo destino se puede alcanzar mediante el uso del protocolo IP.

Generalmente, el mensaje de petición de eco se inicia al ejecutar el comando **ping**, como se muestra en la Figura 2. En este ejemplo, el comando se usa con la dirección de IP del dispositivo de destino. El comando se puede usar también como se muestra en la Figura 3 usando la dirección IP del dispositivo destino. En estos ejemplos, el comando **ping** emite cuatro peticiones de eco y recibe cuatro respuestas, lo que confirma la conectividad IP entre los dos dispositivos.

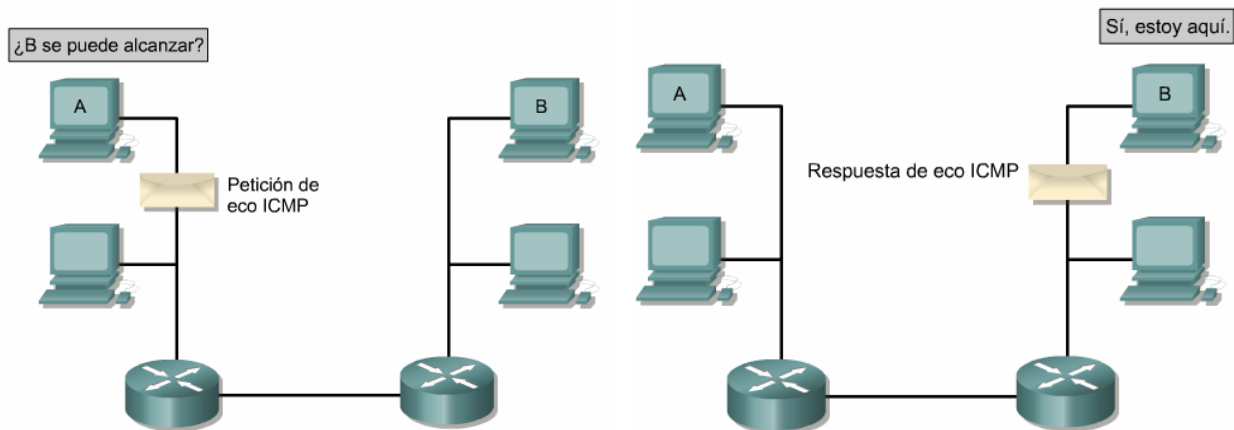


Figura 2

```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-2000 Microsoft Corp.

C:\> ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:

Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Recieved = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 16ms, Average = 16ms
C:\>
  
```

Figura 3

Como se muestra en la figura 3, la respuesta de eco incluye un valor TTL (tiempo de vida) el cual es un campo del encabezado de un paquete IP que limita el número de reenvíos de un paquete. al procesar un paquete, cada router decrementa el valor de TTL en uno. Cuando un router recibe un paquete con un valor de 1, éste no puede ser reenviado. Un mensaje ICMP se genera y se manda al origen, y el paquete original se elimina.

8.1.6 Detección de rutas excesivamente largas

Se puede producir situaciones en las comunicaciones de red en las que un datagrama viaje en círculos, sin llegar nunca a su destino. Esto puede ocurrir si dos routers enrutan continuamente un datagrama de ida y vuelta entre ellos, pensando que el otro debe ser el siguiente salto hacia el destino. Éste es un ejemplo de información de enrutamiento defectuosa.¹

Las limitantes del protocolo de enrutamiento pueden dar como resultado destinos inalcanzables. ¹El número máximo de saltos en RIP es de 15, lo cual significa que las redes mayores a los 15 saltos no se pueden manejar con RIP.

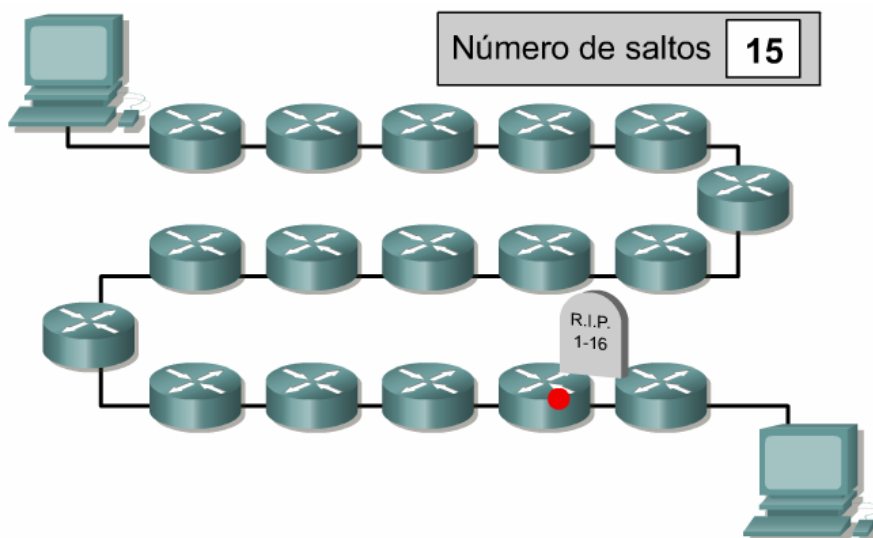


Figura 1

En cualquiera de los casos, existe una ruta excesivamente larga. Ya sea que la ruta actual incluya un círculo, o bien que el paquete exceda el número máximo de saltos.

8.1.7 Mensajes de eco

Al igual que cualquier tipo de paquete, los mensajes ICMP tienen formatos especiales. Cada tipo de mensaje ICMP que se muestra en la Figura 1 tiene sus propias características, pero todos los formatos de mensaje ICMP comienzan con estos mismos tres campos:

- Tipo
- Código
- Suma de comprobación (checksum)

Tipos de mensajes ICMP	
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen
5	Redireccionar/cambiar petición
8	Petición de eco
9	Publicación del router
10	Selección del router
11	Tiempo superado
12	Problema de parámetros
13	Petición de marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información
17	Petición de máscara de dirección
18	Respuesta de máscara de dirección

Figura 1

El campo de tipo indica el tipo de mensaje ICMP que se envía. El campo de código incluye información adicional relativa al tipo de mensaje en particular. El campo checksum (suma de comprobación), al igual que en los otros tipos de paquetes, se usa para verificar la integridad de los datos.

La Figura 2 muestra el formato de los mensajes ICMP "echo request" (petición de eco) y "echo reply" (respuesta de eco). Se muestra el tipo y los números de código pertinentes para cada tipo de mensaje. El campo identificador y el de número de secuencia son exclusivos de los mensajes de petición de eco y

respuesta de eco. Estos campos se usan para comparar las respuestas de eco con la petición de eco correspondiente. El campo de datos contiene información adicional que puede formar parte de un mensaje de petición de eco o de respuesta de eco).

0	8	16	31
Tipo (0 ú 8)	Código (0)	checksum	
Identificador		Número de secuencia	
Datos opcionales			
...			

Figura 2

8.1.8 Mensaje "destination unreachable" (destino fuera de alcance)

No siempre es posible enviar los datagramas a sus destinos. ¹Las fallas de hardware, configuraciones inadecuadas del protocolo, interfaces inactivas y errores en la información de enrutamiento son algunas de las razones que pueden impedir que la entrega se complete con éxito. En estos casos, el ICMP envía de vuelta al emisor un mensaje llamado "destination unreachable" (destino fuera de alcance), el cual le indica al emisor que el datagrama no se pudo entregar adecuadamente.

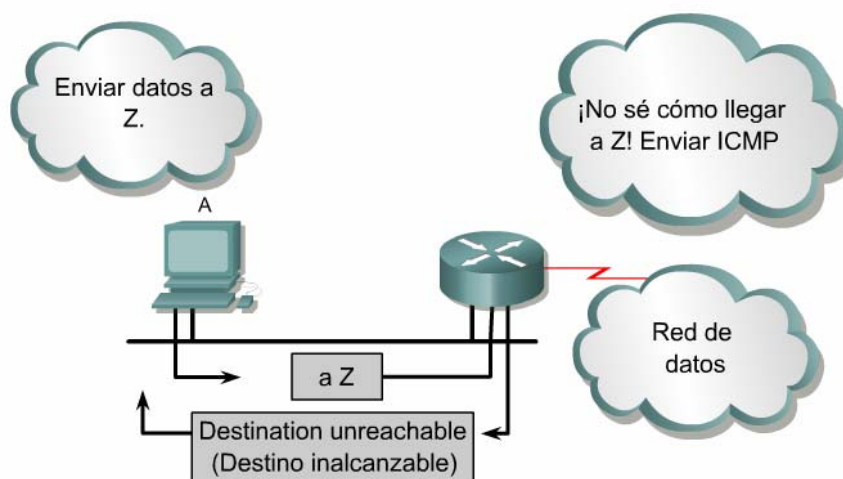


Figura 1

0	8	16	31
Tipo (3)	Código (0)	Checksum	
Sin usar (debe ser cero)			
Encabezado de Internet+ Primeros 64 bits de datagrama			
...			

Figura 2

La Figura ²muestra el encabezado de un mensaje de destino fuera de alcance del ICMP. El valor 3 en el campo de tipo señala que es un mensaje de destino fuera de alcance. El valor del código indica el motivo por el cual el paquete no se pudo entregar. La Figura ²muestra un valor de código de 0, lo que indica que la red está fuera de alcance. La Figura ³muestra el significado de cada uno de los valores de código posibles en un mensaje de destino fuera de alcance.

0 = red inalcanzable
1 = host inalcanzable
2 = protocolo inalcanzable
3 = puerto inalcanzable
4 = fragmentación necesaria y DF puesto en uno
5 = falla de la ruta origen
6 = red de destino desconcida
7 = host de destino desconcido
8 = host de origen aislado
9 = comunicación con red destino prohibida por la administración
10 = comunicación con host destino prohibida por la administración
11 = red inalcanzable por tipo de servicio
12 = host inalcanzable para el tipo de servicio

Figura 3

También se puede enviar un mensaje de destino fuera de alcance cuando se requiere la fragmentación de los paquetes para hacer posible su envío. La fragmentación generalmente es necesaria cuando se envía un datagrama desde una red Token-Ring a una red Ethernet. Si el datagrama no permite la fragmentación, el paquete no puede enviarse, por lo que se envía un mensaje de destino fuera de alcance. Los mensajes de destino fuera de alcance también se pueden generar si los servicios IP relacionados, como por ejemplo el FTP o los servicios WWW, no están disponibles. Para diagnosticar las fallas de una red IP de forma eficaz, es necesario comprender las diversas causas de los mensajes ICMP de destino fuera de alcance.

8.1.9 Otros informes de error

Es posible que los dispositivos que procesan datagramas no puedan enviar un datagrama debido a un error en el encabezado. Este error no se relaciona con el estado del host de destino o de su red, pero impide que el datagrama se procese y se envíe, y debido a esto, el datagrama se descarta. En este caso, se envía un mensaje ICMP "parameter problem" (problema de parámetros) de tipo 12 a la fuente del datagrama. La Figura 1 muestra el encabezado del mensaje de problema de parámetros.

0	8	16	31
Tipo (12)	Código (0-2)	Checksum	
Puntero		Sin usar (debe ser cero)	
Encabezado de Internet+ Primeros 64 bits de datagrama			
...			

Figura 1

El mensaje de problema de parámetros incluye el campo del marcador o apuntador del encabezado. Si el valor del código es 0, el campo de marcador indica el octeto del datagrama que generó el error.

8.2 Mensajes de control del conjunto de protocolos TCP/IP

8.2.1 Introducción a los mensajes de control

El Protocolo de mensajes de control en Internet (ICMP) es una parte integral del conjunto de protocolos TCP/IP. De hecho, todas las implementaciones del IP deben incluir soporte al ICMP. La razón es muy sencilla. En primer lugar, dado que el IP no garantiza la entrega, no cuenta con ningún método incorporado para informar a los hosts que se ha producido un error. Además, el IP no cuenta con ningún método incorporado para suministrar mensajes de información o control a los hosts. El ICMP ejecuta estas funciones para el IP.

A diferencia de los mensajes de error, los mensajes de control no se presentan como el resultado de pérdida de paquetes o condiciones de error que puedan ocurrir durante la transmisión de los paquetes, sino que se utilizan para mantener a los hosts informados de eventos como congestión o la existencia de un mejor gateway a una red remota. ICMP usa el header IP básico para viajar a través de varias redes.

El ICMP usa múltiples tipos de mensajes de control. Algunos de los más comunes se muestran en la Figura 1. Muchos de ellos se tratan en esta sección.

Tipos de mensajes ICMP	
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen
5	Redireccionar/cambiar petición
8	Petición de eco
9	Publicación del router
10	Selección del router
11	Tiempo superado
12	Problema de parámetros
13	Petición de marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información
17	Petición de máscara de dirección
18	Respuesta de máscara de dirección

Figura 1

8.2.2 Peticiones ICMP de redireccionamiento/cambio

Un mensaje común de control del protocolo ICMP es la petición de redireccionamiento/cambio. Este tipo de mensaje sólo puede originarse de un gateway, que es un término que se usa comúnmente para describir un router. Todos los hosts que se comunican con múltiples redes IP deben tener configurado un gateway por defecto. Este gateway por defecto es la dirección del puerto del router conectado a la misma red que el host. La Figura 1 muestra un host conectado a un router que tiene acceso a la Internet. Una vez configurado con la dirección IP de la interfaz Fa 0/0 como su gateway por defecto, el host B usa esa dirección de IP para llegar a cualquier red a la cual no esté conectado directamente. Normalmente, el host B está conectado sólo a un gateway. Sin embargo, en algunos casos, el host está conectado a un segmento de red el cual tiene dos o más routers conectados directamente. En este caso, es posible que el gateway por defecto del host deba utilizar una petición de redireccionamiento/cambio para informar al host cuál es la mejor ruta hacia una red determinada.

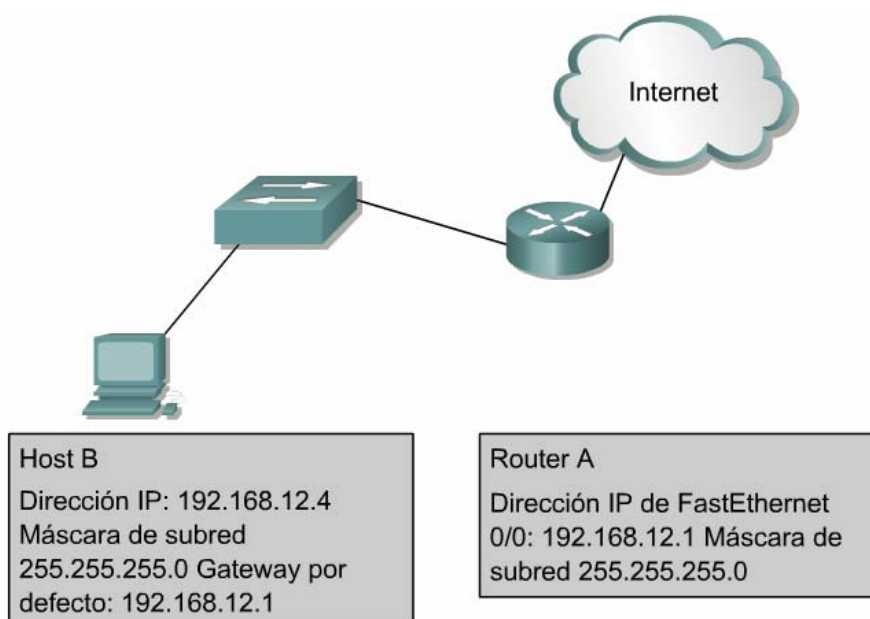


Figura 1

La Figura 2 muestra una red donde podría ocurrir el redireccionamiento ICMP. El host B envía un paquete al host C en la red 10.0.0.0/8. Dado que el host B no está directamente conectado a la misma red, envía el paquete a su gateway por defecto, el router A. El router A encuentra la ruta correcta hacia la red 10.0.0.0/8 en su tabla de enrutamiento, y determina que la ruta hacia la red es a través de la misma interfaz de la que provino la petición para enviar el paquete. Envía el paquete y hace una petición ICMP de redireccionamiento/cambio al host B, en la cual le indica que debe usar el router B como gateway para enviar todas las peticiones futuras para la red 10.0.0.0/8.

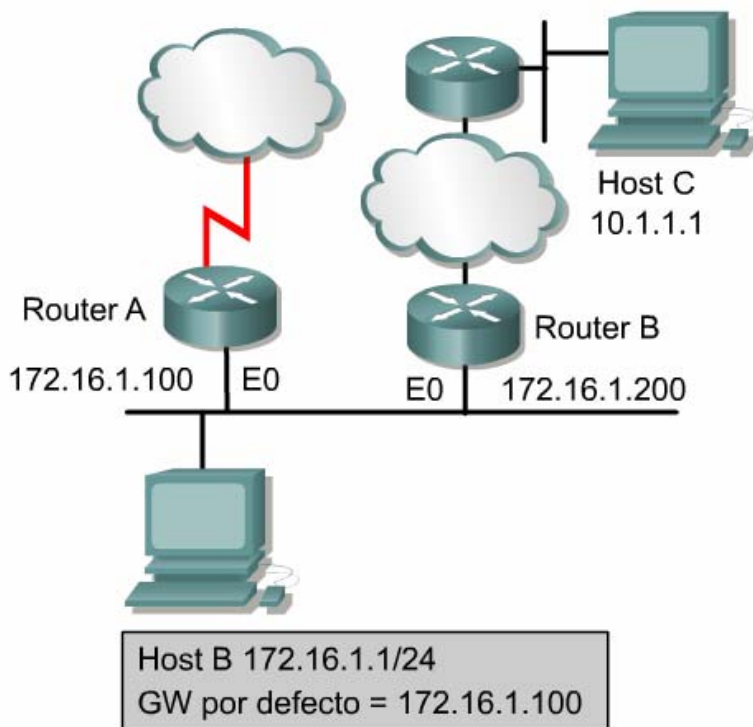


Figura 2

Los gateway por defecto envían mensajes ICMP de peticiones de redireccionamiento/cambio sólo si se cumplen las siguientes condiciones:

- La interfaz a través de la cual el paquete ingresa al router es la misma a través de la cual sale el paquete enrutado.
- La subred/red de la dirección de IP de origen es la misma red/subred de la dirección de IP del salto siguiente del paquete enrutado.
- El datagrama no está enrutado desde el origen.
- La ruta para el redireccionamiento no es otro redireccionamiento ICMP ni otra ruta por defecto.
- El router está configurado para enviar redireccionamientos. (Por defecto, los routers Cisco envían redireccionamientos ICMP. El subcomando de interfaces **no ip redirects** inhabilita todos los redireccionamientos ICMP).

0	8	16	31
Tipo (5)	Código (0-3)	Checksum	
Dirección de Internet del router			
Encabezado de Internet+ Primeros 64 bits de datagrama			
...			

Figura 3

La petición ICMP de redireccionamiento/cambio utiliza el formato que se muestra en la Figura 3. Tiene un código ICMP de tipo 5. Además, puede tener valores de código de 0, 1, 2 ó 3. 4

Valor del código	Acción requerida
0	Datagramas redireccionados para la red.
1	Datagramas redireccionados para el host.
2	Datagramas redireccionados para el tipo de servicios y redes.
3	Datagramas redireccionados para el tipo de servicios y host.

Figura 4

El campo Router Internet Address (Dirección Internet del router) del redireccionamiento ICMP es la dirección de IP a ser usada como gateway por defecto para una red en particular. En el ejemplo que aparece en la Figura 2, el redireccionamiento ICMP que se envía desde el router A al host B tiene un valor de campo del Router Internet Address de 172.16.1.200, el cual es la dirección IP de la interfaz E0 en el router B.

8.2.3 Sincronización de relojes y estimación del tiempo de tránsito

El conjunto de protocolos TCP/IP permite que los sistemas se conecten entre sí a través de amplias distancias por múltiples redes. Cada una de estas redes individuales hace su sincronización de reloj de una manera particular. Como resultado de ello, puede haber problemas en el caso de hosts en redes distintas que tratan de comunicarse mediante software que requiere de sincronización de reloj. El mensaje ICMP de tipo "timestamp" (de marca horaria) está diseñado para ayudar a resolver este problema.

El mensaje ICMP de petición de marca horaria permite que un host solicite la hora actual que observa el host remoto. El host remoto usa un mensaje ICMP de respuesta de marca horaria para responder a la petición. 1

0		8		16		31	
Tipo (13 ó 14)		Código (0)		Checksum			
Identificador				Número de secuencia			
Originar marca horaria							
Recibir marca horaria							
Transmitir marca horaria							

Figura 1

El campo de tipo de un mensaje ICMP de marca horaria puede ser 13 (timestamp request/petición de marca horaria) o 14 (timestamp reply/respuesta de marca horaria). El valor del campo de código se fija siempre en 0 dado que no hay ningún parámetro adicional disponible. La petición de marca horaria ICMP contiene una marca horaria de origen, que es la hora en el host solicitante al momento de enviar la petición de marca horaria. La marca horaria de recepción es la hora en que el host destino recibe la petición de marca horaria. La marca horaria de transmisión se completa justo antes de que se devuelva la respuesta de marca horaria. Las marcas horarias de origen, recepción y transmisión se calculan según la cantidad de milisegundos que transcurrieron desde la medianoche de la Hora Universal (UT).

Todos los mensajes ICMP de respuesta de marca horaria contienen las marcas horarias de origen, recepción y transmisión. Usando estos tres marca de tiempo, el cliente puede determinar el tiempo de tránsito a través de la red mediante la resta del tiempo de llegada y el tiempo de salida. O también en la dirección contraria restando el tiempo de transmisión del tiempo actual. El host que originó la petición de marca horaria también puede estimar la hora local en la computadora remota.

Aunque los mensajes ICMP de marca horaria suministran una forma sencilla para estimar la hora en un host remoto y el tiempo de tránsito total de una red, no es la mejor manera de obtener esta información. En lugar de ello, existen protocolos más sólidos como por ejemplo el Protocolo de hora de red (NTP), perteneciente a las capas superiores de la pila del protocolo TCP/IP, el cual realiza la sincronización de relojes de un modo más confiable.

8.2.4 Formatos de los mensajes de petición de información y de respuesta

Los mensajes ICMP de petición de información y de respuesta fueron concebidos originalmente para permitir que el host determine su número de red. La Figura 1 muestra el formato de un mensaje ICMP de petición de información y de respuesta.

0	8	16	31
Tipo (15 ó 16)	Código (0)	Checksum	
Identificador		Número de secuencia	

Figura 1

Hay dos códigos de tipo disponibles para estos mensajes. El tipo 15 indica un mensaje de petición de información y el tipo 16 señala un mensaje de respuesta de información. Este tipo de mensaje ICMP en particular se considera obsoleto. En la actualidad se usan otros protocolos como, por ejemplo el BOOTP, Reverse Address Resolution Protocol (RARP), y el Protocolo de configuración dinámica del host (DHCP), para que los hosts obtengan sus números de red.

8.2.5 Solicitud de la máscara de dirección

Cuando un administrador de red emplea el proceso de división en subredes para dividir un grupo amplio de direcciones IP en múltiples subredes, se crea una nueva máscara de subred. Esta nueva máscara de subred es vital para identificar los bits correspondientes a la red, la subred y el host de una dirección de IP. Si un host no conoce su máscara de subred, puede enviar una petición de máscara al router local. Si se conoce la dirección del router, esta petición se puede enviar directamente al router. De otro modo, la petición será hecha como broadcast. Cuando el router recibe la petición, envía de vuelta una respuesta de máscara de dirección o "address mask reply". Esta respuesta de máscara de dirección indica la máscara de subred correcta. Por ejemplo, consideremos que el host se encuentra en una red Clase B y tiene una dirección de IP de 172.16.5.2. Este host desconoce su máscara de subred, por lo tanto hace una petición de la máscara de dirección como broadcast.

Dirección de origen: 172.16.5.2

Dirección de destino: 255.255.255.255

Protocolo: ICMP = 1

Tipo: Petición de máscara de dirección = AM1

Código: 0

Máscara: 255.255.255.0

Este broadcast se recibe en 172.16.5.1, el router local. El router responde enviando una respuesta de máscara de dirección o "address mask reply":

Dirección de origen: 172.16.5.1

Dirección de destino: 172.16.5.2

Protocolo: ICMP = 1

Tipo: Respuesta de máscara de dirección = AM2

Código: 0

Máscara: 255.255.255.0

Los formatos de la petición y respuesta de máscara de dirección se indican en la Figura 1. La Figura 2 muestra las descripciones de cada uno de los campos del mensaje de petición de máscara de dirección. Observe que se usa el mismo formato tanto para la petición como para la respuesta de máscara de dirección. Sin embargo, el número de tipo 17 se asigna a la petición y, el 18, a la respuesta.

0		8		16		31	
Tipo (17 ó 18)		Código (0)		Checksum			
Identificador				Número de secuencia			
Máscara de dirección							
...							

Figura 1

Campos IP	
Direcciones	La dirección en un mensaje de requerimiento de máscara de direcciones será el destino del mensaje de respuesta de máscara de direcciones. Para formar un mensaje de respuesta de máscara de dirección, la dirección origen de la petición se convierte en la dirección destino de la respuesta, la dirección origen de la respuesta se pone como la dirección del respondedor. El tipo de código cambiado es AM2, el valor de la máscara de dirección se inserta en la máscara de dirección y la checksum se vuelve a calcular. Sin embargo, si la dirección de origen en el mensaje de requerimiento es cero, entonces la dirección de destino del mensaje de respuesta debería ser un broadcast.

Figura 2

8.2.6 Mensaje de descubrimiento de routers

Cuando arranca un host de la red, y su gateway por defecto no se ha configurado manualmente, puede aprender cuáles son los routers disponibles a través del proceso de descubrimiento de routers. Este proceso comienza cuando el host envía un mensaje de solicitud de routers a todos los routers. Para ello utiliza la dirección multicast 224.0.0.2 como la dirección destino. La Figura 1 muestra el mensaje ICMP de descubrimiento de routers o "router discovery". El mensaje de descubrimiento de router se puede enviar también como broadcast, para que incluya los routers que no se pueden configurar para multicast. Si se envía un mensaje de descubrimiento de router a un router que no maneja el proceso de descubrimiento, no se recibirá ninguna respuesta a dicho mensaje.

0		8		16		31	
Tipo (9)		Código (0)		Checksum			
Número de direcciones		Tamaño de la entrada de direcciones		Duración			
Dirección 1 del router							
Nivel de preferencias 1							
Dirección 2 del router							
Nivel de preferencias 2							

Figura 1

Si un router que permite el proceso de descubrimiento recibe un mensaje de descubrimiento de router, envía de vuelta una publicación o anuncio de router. El formato de la publicación de router se muestra en la Figura 1 y la Figura 2 da una explicación de cada uno de los campos.

Campos IP	
Dirección origen	Una dirección IP que pertenece a la interfaz desde la cual se ha enviado este mensaje.
Dirección destino	La dirección publicitaria configurada o la dirección IP de un host vecino.
Tiempo de existencia	1 si la dirección destino es una dirección IP multicast; al menos 1 de lo contrario.

Figura 2

8.2.7 Mensaje de solicitud de router

Un host genera un mensaje ICMP de solicitud de router en respuesta a la ausencia de un gateway por defecto. Este mensaje se envía mediante multicast y es el primer paso del proceso de descubrimiento de routers. El router local responde con una publicación de router, en la que se identifica el gateway por defecto para el host local. La Figura 2 identifica el formato de la publicación de router y la Figura 3 da una explicación de cada uno de los campos.

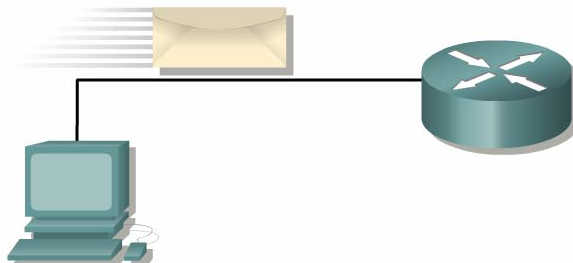


Figura 1

0	8	16	31
Tipo (10)	Código (0)	Checksum	
Reservado			

Figura 2

Campos IP	
Dirección origen	Una dirección IP que pertenece a la interfaz desde la cual se ha enviado este mensaje o 0.
Dirección destino	Dirección de solicitud configurada
Tiempo de existencia	Debe ser 1 si la dirección de destino es una dirección IP Multicast, De otra forma, debe ser al menos 1

Campos ICMP	
Tipo	10
Código	0
Checksum	Complemento a uno de 16 bits de la suma del complementos a uno del mensaje ICMP, comenzando por el tipo de ICMP. Para calcular la checksum, el campo de la checksum se pone a cero.
Reservado	Se envía un 0, se ignora en recepción.

Figura 3

8.2.8 Mensajes de congestión y control de flujo

Si varias computadoras tratan de tener acceso al mismo destino a la vez, la computadora de destino puede ser incapaz de manejar el alto tráfico. También se puede producir congestión cuando el tráfico de una LAN de alta velocidad llega a una conexión WAN más lenta. Cuando hay demasiada congestión en una red, los paquetes se pierden. Los mensajes ICMP source-quench (supresión en el origen) se usan para reducir la cantidad de datos perdidos. Los mensajes de supresión en el origen solicitan a los emisores reducir la velocidad a la que transmiten los paquetes. En la mayoría de los casos, la congestión se reduce luego de un corto período de tiempo, y el origen lentamente aumenta la velocidad de transmisión siempre y cuando no se reciba ningún otro mensaje de supresión en el origen. La mayoría de los routers Cisco por defecto no envían mensajes de supresión en el origen, dado que dichos mensajes pueden contribuir a la congestión de la red.

El caso de las oficinas pequeñas o oficinas en el hogar (SOHO) es uno en el que los mensajes ICMP de supresión en el origen se pueden usar de forma efectiva. Una red SOHO puede estar compuesta por cuatro computadoras conectadas en red mediante cable CAT-5 y que tienen una conexión Internet compartida a

través de un módem de 56K. Es muy fácil determinar que el ancho de banda de 10 ó 100 Mbps de la red local puede copar rápidamente el ancho de banda de 56Kbps del enlace WAN, lo que da como resultado la pérdida de datos y las retransmisiones. El host que actúa como gateway puede usar un mensaje ICMP "source quench" para solicitar que los otros hosts reduzcan sus velocidades de transmisión para prevenir la pérdida continua de datos. En la Figura 1 se muestra una red en la que la congestión del enlace WAN puede provocar problemas en la comunicación.

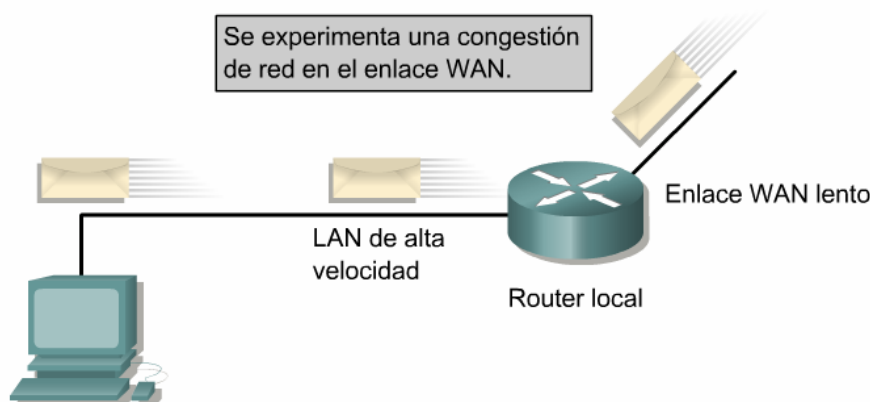


Figura 1

Resumen

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

- El IP es un método de entrega de mejor esfuerzo, el cual usa mensajes ICMP para alertar al emisor que los datos no llegaron a su destino.
- Los mensajes ICMP de petición de eco y de respuesta de eco permiten que el administrador de red pruebe la conectividad IP, para ayudar en el proceso de diagnóstico de fallas.
- Los mensajes ICMP se transmiten mediante el protocolo IP de modo que su entrega es poco confiable.
- Los paquetes ICMP tienen su propia información especial en el encabezado, la cual comienza con un campo de tipo y un campo de código.
- Identificar las causas potenciales de los mensajes específicos de error del protocolo ICMP
- Las funciones de los mensajes ICMP de control
- Los mensajes ICMP de petición de redireccionamiento/cambio
- Los mensajes de sincronización de reloj y estimación del tiempo de tránsito
- Los mensajes ICMP de petición de información y de respuesta de información
- Los mensajes ICMP de petición y respuesta de máscara de dirección
- El mensaje ICMP de descubrimiento de router
- El mensaje ICMP de solicitud de router
- Los mensajes ICMP de congestión y control de flujo

Módulo 9: Diagnóstico de fallas básico del router

Descripción general

Un router usa un protocolo de enrutamiento dinámico para aprender acerca de rutas a las redes destino. La mayoría de los routers usa una combinación de enrutamiento dinámico y rutas estáticas configuradas manualmente. Cualquiera sea el método utilizado, cuando un router determina que una ruta es el mejor camino hacia un destino, la instala en su tabla de enrutamiento. Este módulo describe los métodos para examinar e interpretar los contenidos de una tabla de enrutamiento.

La prueba y el diagnóstico de las fallas de una red son, tal vez, los componentes que demandan más tiempo entre las tareas que ejecuta un administrador de redes. Una prueba y diagnóstico de fallas eficientes deben llevarse a cabo de forma lógica, ordenada y bien documentada. De lo contrario, volverán a producirse los mismos problemas y el administrador de la red nunca podrá entender la red a ciencia cierta. Este módulo describe un enfoque estructurado respecto del diagnóstico de fallas y provee algunas herramientas que se utilizan en este proceso.

Para los administradores de redes, los problemas de enrutamiento son los más comunes y difíciles de diagnosticar. Identificar y resolver los problemas de enrutamiento puede no resultar tan sencillo, pero muchas son las herramientas que pueden hacer más fácil la tarea. Este módulo presenta varias de las herramientas más importantes y proporciona la práctica de su utilización.

Los estudiantes que completen este módulo deberán ser capaces de:

- Utilizar el comando **show ip route** para recopilar información detallada sobre las rutas instaladas en el router.
- Configurar un router o una red por defecto.
- Comprender la forma en que un router utiliza el direccionamiento de Capa 2 y de Capa 3 para transferir los datos a través de la red.
- Utilizar el comando **ping** para realizar las pruebas básicas de conectividad de la red.
- Utilizar el comando **telnet** para verificar el software de capa de aplicación entre las estaciones origen y destino.
- Diagnosticar las fallas por medio de pruebas secuenciales de las capas OSI.
- Utilizar el comando **show interfaces** para confirmar los problemas de Capa 1 y Capa 2.
- Utilizar los comandos **show ip route** y **show ip protocol** para identificar los problemas de enrutamiento.
- Utilizar el comando **show cdp** para verificar la conectividad de Capa 2.
- Utilizar el comando **traceroute** para identificar las rutas que los paquetes recorren entre las redes.
- Utilizar el comando **show controllers serial** para garantizar la conexión del cable apropiado.
- Utilizar los comandos básicos **debug** para monitorear la actividad del router.

9.1 Examen de la tabla de enrutamiento

9.1.1 El comando show ip route

Una de las funciones principales de un router es determinar la mejor ruta a un destino determinado. Un router averigua las rutas desde la configuración de un administrador o desde otros routers mediante los protocolos de enrutamiento. Los routers almacenan esta información en tablas de enrutamiento que se mantienen en la memoria de acceso aleatorio (RAM) del router. Una tabla de enrutamiento contiene una lista de las mejores rutas disponibles. El router usa la tabla de enrutamiento para tomar decisiones de envío de paquetes.

El comando **show ip route** muestra el contenido de una tabla de enrutamiento IP. Esta tabla contiene entradas para todas las redes y subredes conocidas, así como un código que indica de qué forma se obtuvo la información. Los siguientes son algunos comandos adicionales que se pueden utilizar con el comando **show ip route**:

- **show ip route connected**
- **show ip route address**
- **show ip route rip**
- **show ip route igrp**
- **show ip route static**

La tabla de enrutamiento mapea los prefijos de la red hacia la interfaz saliente. ¹ Cuando RTA recibe un paquete con destino a 192.168.4.46, busca el prefijo 192.168.4.0/24 en su tabla. RTA luego envía el paquete hacia una interfaz (Ethernet0) basándose en la entrada de la tabla de enrutamiento. Si RTA recibe un paquete con destino a 10.3.21.5, envía dicho paquete hacia Serial 0.

```

RTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic download static route
Gateway of last resort is not set
C    192.168.4.0/24 is directly connected, Ethernet0
     10.0.0.0/16 is subnetted, 3 subnets
C    10.3.0.0 is directly connected, Serial0
C    10.4.0.0 is directly connected, Serial1
C    10.5.0.0 is directly connected, Ethernet1
  
```

Figura 1

El ejemplo de tabla de enrutamiento muestra cuatro rutas para las redes directamente conectadas. Estas rutas, identificadas como C, se encuentran disponibles para las redes directamente conectadas. RTA descarta cualquier paquete destinado a una red que no se encuentre en la lista de la tabla de enrutamiento. A fin de efectuar el envío hacia otros destinos, la tabla de enrutamiento para RTA debe incluir más rutas. Estas nuevas rutas pueden agregarse utilizando uno de los dos siguientes métodos:

- **Enrutamiento estático:** el administrador define, de forma manual, las rutas hacia una o más redes destino.
- **Enrutamiento dinámico:** los router siguen reglas definidas por el protocolo de enrutamiento para intercambiar información de enrutamiento y seleccionar la mejor ruta de forma independiente.

Ventajas del enrutamiento estático	Desventajas del enrutamiento estático
Baja carga del procesador. Los routers no gastan ciclos valiosos de la CPU calculando la mejor ruta. Esto requiere menor potencia de procesamiento y menos memoria (y, por lo tanto, un router más económico).	Una configuración de alto mantenimiento. Los administradores deben configurar manualmente todas las rutas estáticas. Las redes complejas pueden necesitar una reconfiguración constante.
No usa el ancho de banda. Los routers no ocupan el ancho de banda enviando actualizaciones el uno al otro sobre las rutas estáticas.	No hay adaptabilidad. Las rutas configuradas estáticamente no se adaptan a los cambios en el estado de los enlaces.
Operación segura. Los routers que no envían actualizaciones no revelarán inadvertidamente información de red a una fuente no confiable. Los routers que no aceptan las actualizaciones de enrutamiento son menos vulnerables a los ataques.	
Facilidad de pronóstico. Las rutas estáticas permiten que un administrador controle de forma exacta la selección de rutas de un router. El enrutamiento dinámico a veces produce resultados inesperados, aun en las	

Figura 2

Se dice que las rutas definidas administrativamente son estáticas porque no cambian hasta que un administrador de red programe los cambios de forma manual. Las rutas obtenidas de otros routers son dinámicas porque pueden cambiar de forma automática a medida que los routers vecinos se actualizan entre sí con la nueva información. Cada método tiene ventajas y desventajas fundamentales. ² ³

Ventajas del enrutamiento dinámico	Desventajas del enrutamiento dinámico
Alto grado de adaptabilidad. Los routers pueden informarse el uno al otro acerca de enlaces que están inactivos o acerca de rutas nuevas que se han detectado. Los routers automáticamente "aprenden" la topología y seleccionan las mejores rutas.	Mayor carga del procesador y uso de memoria. Los procesos de enrutamiento dinámico requieren una cantidad significativa de tiempo de la CPU y memoria del sistema.
Configuración de bajo mantenimiento. Después de establecer correctamente los parámetros básicos de un protocolo de enrutamiento, no se requiere la intervención administrativa.	Elevado uso del ancho de banda. Los routers usan ancho de banda para enviar y recibir las actualizaciones de enrutamiento, lo que puede afectar de forma adversa el rendimiento de los enlaces WAN lentos.

Figura 3

9.1.2 Determinación del gateway de último recurso

No es factible, ni siquiera deseable, que un router mantenga rutas hacia cada posible destino. En su lugar, los routers guardan una ruta por defecto o un gateway de último recurso. Las rutas por defecto se utilizan cuando un router no es capaz de hacer coincidir una red destino con ninguna entrada de la tabla de enrutamiento. El router utiliza esta ruta por defecto para llegar al gateway de último recurso en un esfuerzo por enviar el paquete. ¹

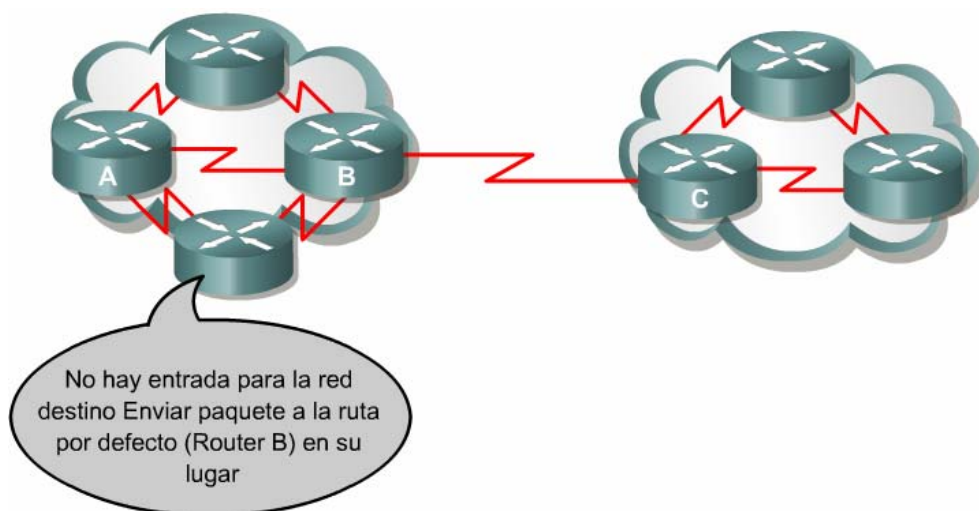


Figura 1

Una característica de escalabilidad clave es que las rutas por defecto mantienen las tablas de enrutamiento tan simples como es posible. Posibilitan que los routers envíen los paquetes destinados a cualquier host de Internet sin tener que mantener una entrada en la tabla para cada red de la Internet. El administrador puede ingresar estáticamente las rutas por defecto o es posible obtener información de las mismas de forma dinámica mediante un protocolo de enrutamiento.

El enrutamiento por defecto comienza en el administrador: Antes de que los routers puedan intercambiar la información de forma dinámica, el administrador debe configurar al menos un router con una ruta por defecto. Según los resultados deseados, el administrador puede utilizar alguno de los siguientes comandos para configurar una ruta por defecto de forma estática: ²

Comando

```
Router(config)#ip default-network [network number]
```

Figura 2

ip default-network

o

ip route 0.0.0.0 0.0.0.0

El comando **ip default-network** se usa para establecer una ruta predeterminada en redes que usan protocolos de enrutamiento dinámico. Este comando es con distinción de clase o classful, lo que quiere decir que una subred señalada por este comando instala la red mayor en la tabla de ruteo. El comando **ip default-network** se debe usar en la red mayor, para marcar la subred candidata a ser la ruta predeterminada.

El comando **ip default-network** establece una ruta por defecto en las redes que utilizan protocolos de enrutamiento dinámico. ³El comando global **ip default-network 192.168.17.0** define la red Clase C 192.168.17.0 como la ruta destino para paquetes que no poseen entradas en la tabla de enrutamiento. Para cada red configurada con el comando **ip default-network**, si un router cuenta con una ruta hacia la red, dicha ruta queda señalada como candidata a ser la ruta por defecto. ⁴

Argumento	Descripción
network-number	El número de la posible red o subred IP por defecto.

Figura 3

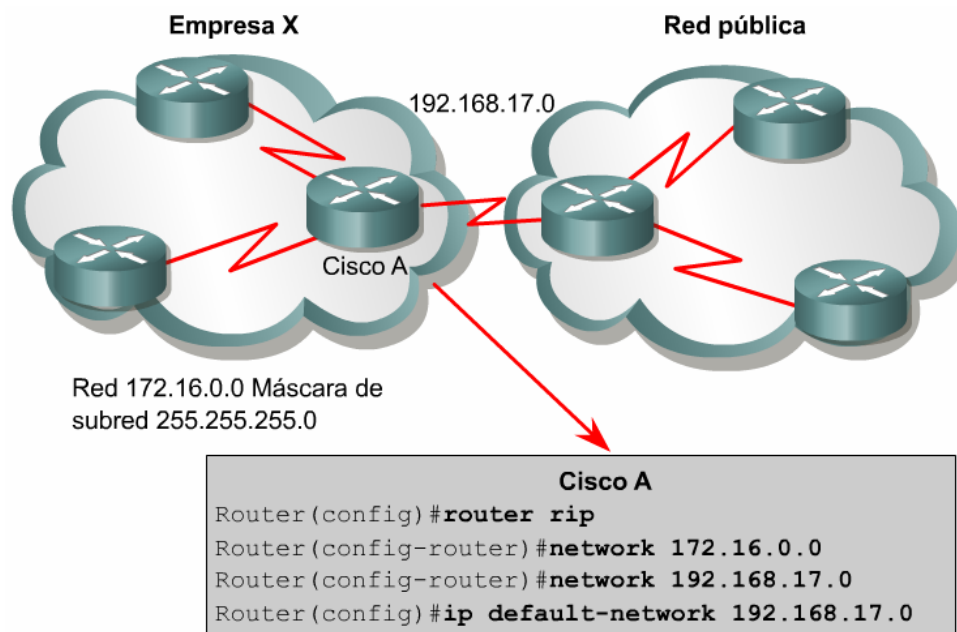


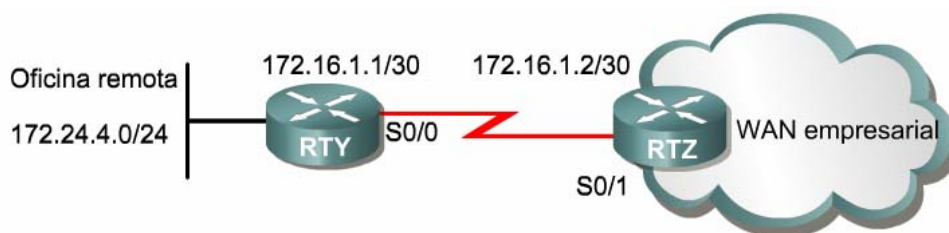
Figura 4

Crear un **ip route** hacia 0.0.0.0/0 es otra forma de configurar una ruta por defecto. ⁵

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [address | interface]
```

Después de configurar una ruta o una red por defecto, el comando **show ip route** mostrará lo siguiente:

Gateway of last resort is 172.16.1.2 to network 0.0.0.0 ⁶



```
RTY(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

Figura 5

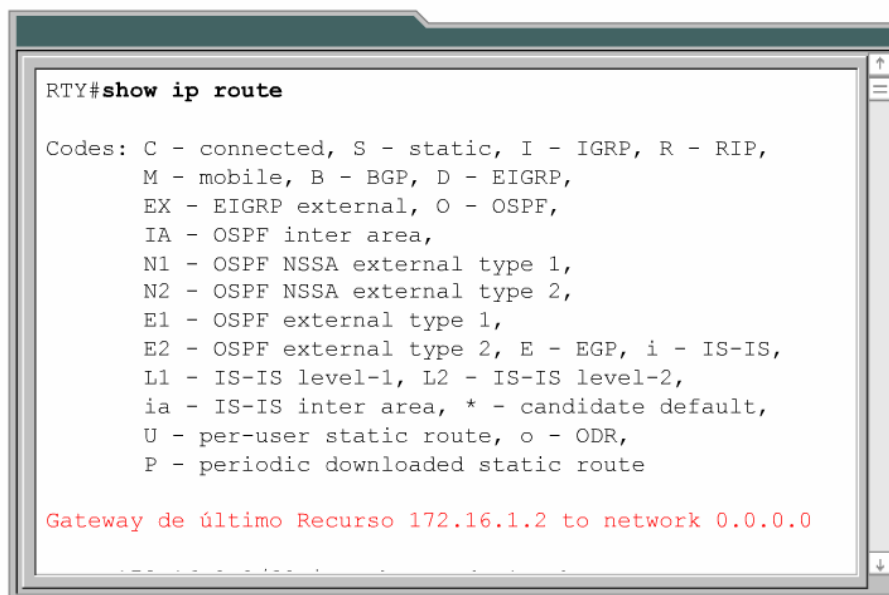


Figura 6

9.1.3 Determinación del origen y destino de una ruta

En el tráfico que fluye a través de la nube de la red, la determinación de la ruta se produce en la capa de red. La función de determinación de ruta permite al router evaluar las rutas disponibles hacia un destino y establecer el mejor manejo de un paquete. Los servicios de enrutamiento utilizan la información de topología de red al evaluar las rutas de red. Esta información la puede configurar el administrador de red o se puede recopilar a través de procesos dinámicos ejecutados en la red.

La capa de red proporciona entrega de paquetes de mejor esfuerzo y de extremo a extremo a través de redes interconectadas. La capa de red utiliza la tabla de enrutamiento IP para enviar paquetes desde la red origen a la red destino. Una vez que el router determina cuál es la ruta a utilizar, toma el paquete proveniente de una interfaz y lo envía hacia otra interfaz o puerto que refleje la mejor ruta hacia su destino.

1 2

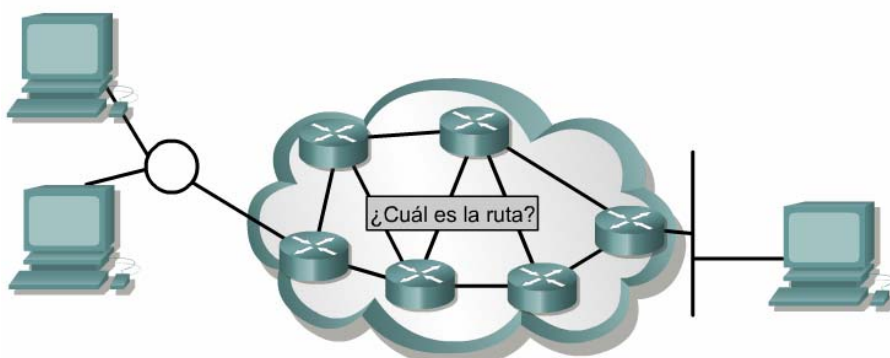


Figura 1

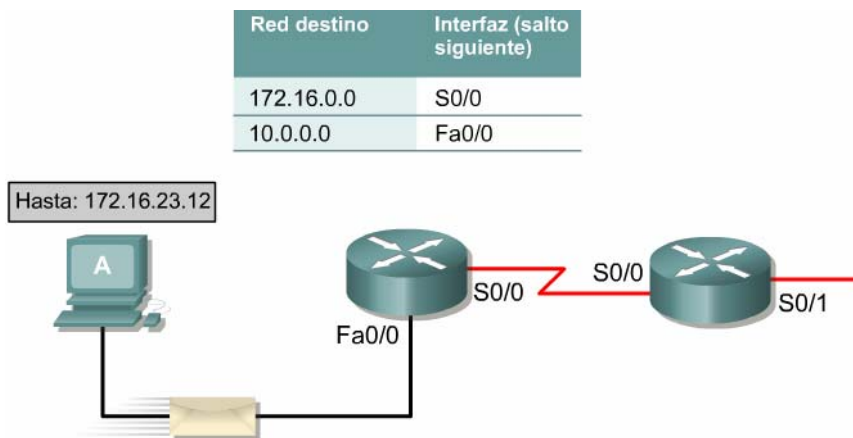
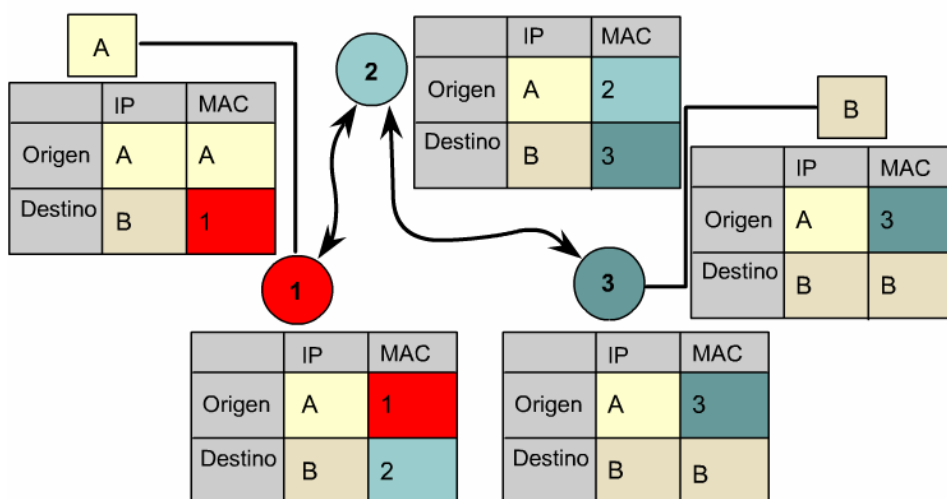


Figura 2

9.1.4 Determinación de las direcciones L2 y L3

Mientras las direcciones de capa de red se utilizan para que los paquetes viajen desde el origen hacia el destino, es importante comprender que se utiliza un tipo de dirección diferente para que los paquetes se transmitan desde un router hacia el siguiente. Para que un paquete se transmita desde un origen hacia su destino, se utiliza tanto las direcciones de Capa 2 como de Capa 3. Como se muestra en la Figura 1, en cada interfaz, a medida que el paquete se desplaza por la red, se examina la tabla de enrutamiento y el router determina el salto siguiente. El paquete se envía entonces utilizando la dirección MAC del salto siguiente. Los encabezados origen y destino IP no cambian en ningún momento.



En cada interfaz, a medida que el paquete se desplaza por la red, se examina la tabla de enrutamiento y el router determina el salto siguiente. El paquete se envía entonces mediante la dirección MAC del salto siguiente. Los encabezados origen y destino IP no cambian en ningún momento.

Figura 1

La dirección de Capa 3 se utiliza para enrutar el paquete desde la red origen hacia la red destino. Las direcciones IP de origen y destino no cambian. La dirección MAC cambia en cada salto o router. La dirección de capa de enlace de datos resulta necesaria porque la entrega dentro de la red está determinada por la dirección del encabezado de la trama de Capa 2 y no por el encabezado del paquete de Capa 3.

9.1.5 Determinación de la distancia administrativa de la ruta.

Un router puede descubrir rutas utilizando protocolos de enrutamiento dinámico o rutas que el administrador configura de forma manual en el router. Una vez descubiertas o configuradas, el router debe elegir cuáles son las mejores rutas hacia una red dada.

La distancia administrativa de la ruta es la información clave que el router utiliza para decidir cuál es el mejor camino hacia un destino en particular. La distancia administrativa es un número que mide la

confiabilidad del origen de la información de la ruta. Cuanto menor es la distancia administrativa, mayor la confiabilidad del origen.

Diferentes protocolos de enrutamiento presentan diferentes distancias administrativas por defecto. ¹ Si un camino tiene la menor distancia administrativa, se incluye en la tabla de enrutamiento. La tabla de enrutamiento no incluye una ruta si la distancia administrativa desde otro origen es menor.

Protocolos	Distancias administrativas por defecto
Conectado	0
Estática	1
Resumen de ruta EIGRP	5
eBGP	20
EIGRP (Interno)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (Externo)	170
iBGP (Externo)	200

Figura 1

9.1.6 Determinación de la métrica de la ruta

Los protocolos de enrutamiento utilizan la métrica para determinar la mejor ruta hacia un destino. La métrica es un valor que mide la conveniencia de una ruta. Algunos protocolos de enrutamiento sólo utilizan un factor para calcular una métrica. Por ejemplo, RIP versión 1 (RIP v1) utiliza el recuento de saltos como único factor para determinar la métrica de una ruta. Otros protocolos basan su métrica en el recuento de saltos, ancho de banda, retardo, carga, confiabilidad, y costo. ¹

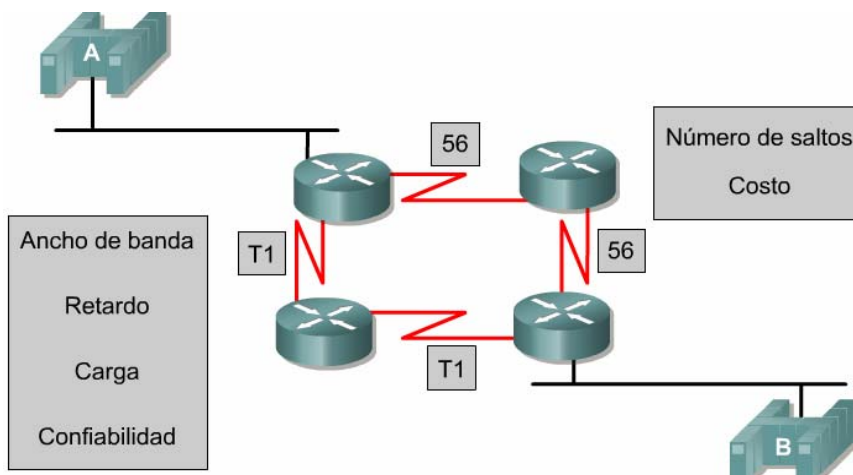


Figura 1

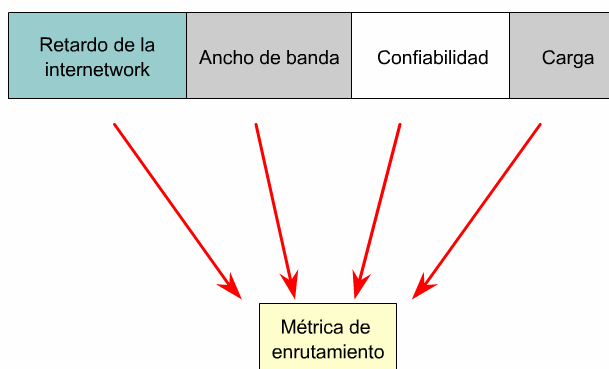


Figura 2

Cada algoritmo de enrutamiento interpreta lo que es mejor a su manera. El algoritmo genera un número, denominado métrica, para cada ruta a través de la red. Normalmente, cuanto menor es el valor de la métrica, mejor es la ruta.

Factores tales como ancho de banda y retardo son estáticos porque permanecen inalterables para cada interfaz hasta que se cambie la configuración del router o se rediseñe la red. Factores tales como carga y confiabilidad son dinámicos porque el router los calcula para cada interfaz en tiempo real. ²

Cuanto más factores compongan una métrica, mayor la flexibilidad para adaptar las operaciones de la red a las necesidades específicas. Por defecto, IGRP utiliza los factores estáticos ancho de banda y retardo para calcular el valor de la métrica. Estos dos factores pueden configurarse de forma manual, permitiendo un control preciso sobre cuál es la ruta que elige el router. IGRP también puede configurarse para incluir los factores dinámicos: carga y confiabilidad, en el cálculo de la métrica. Utilizando los factores dinámicos, los routers IGRP pueden tomar decisiones basándose en las condiciones del momento. Si un enlace está muy cargado o es no confiable, IGRP aumentará la métrica de las rutas que utilizan dicho enlace. En estas circunstancias, las rutas alternativas pueden presentar una métrica menor que las rutas cuya métrica aumentó y se utilizarán como reemplazo.

IGRP calcula la métrica agregando los valores ponderados de las diferentes características del enlace con la red en cuestión. En el siguiente ejemplo, los valores: ancho de banda, ancho de banda dividido por la carga y el retardo se ponderan con las constantes K1, K2, y K3.

Métrica = $[K1 * \text{Ancho de banda} + (K2 * \text{Ancho de banda}) / (256 - \text{Carga}) + K3 * \text{Retardo}] * [K5 / (\text{Confiabilidad} + K4)]$

Los valores por defecto de las constantes son K1 = K3 = 1 y K2 = K4 = K5 = 0.

Si K5=0, el término $[K5 / (\text{Confiabilidad} + K4)]$ no se utiliza. Dados los valores por defecto para las constantes K1 a K5, el cálculo de la métrica compuesta usado por IGRP se reduce a Métrica = Ancho de banda + Retardo.

9.1.7 Determinación del salto siguiente en la ruta

Los algoritmos de enrutamiento pueblan las tablas de enrutamiento con una amplia variedad de información. Las asociaciones entre el destino/salto siguiente le dicen al router que la mejor forma de alcanzar un destino en particular es enviar el paquete hacia un router en particular. Este router representa el siguiente salto en el camino hacia el destino final. ¹

```

rtl#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
R 200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14, Serial0/0
C 192.168.10.0/24 is directly connected, Serial0/0
C 192.168.0.0/24 is directly connected, Loopback0
rtl#show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.10.2 on Serial0/0, 00:00:11 ago
  Routing Descriptor Blocks:
    * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via Serial0/0
      Route metric is 1, traffic share count is 1

```

Figura 1

Cuando un router recibe un paquete entrante, lee la dirección destino e intenta asociar esta dirección con el salto siguiente. ²

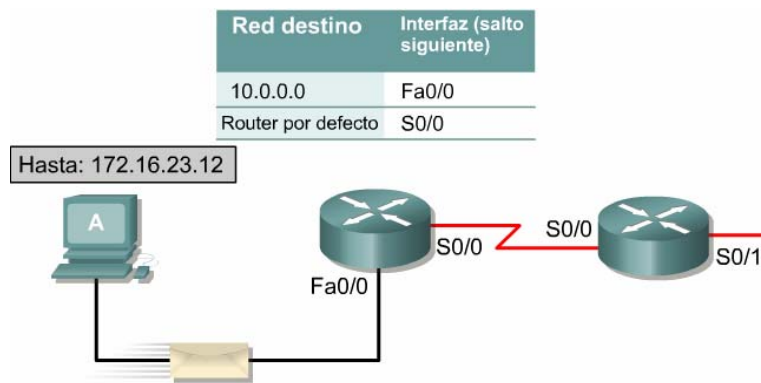


Figura 2

9.1.8 Determinación de la última actualización de enrutamiento

Utilice los siguientes comandos para encontrar la última actualización de enrutamiento:

- **show ip route** 1
- **show ip route** *address* 1
- **show ip protocols**
- **show ip rip database** 2

```

rtl#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set
R 200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14, Serial0/0
C 192.168.10.0/24 is directly connected, Serial0/0
C 192.168.0.0/24 is directly connected, Loopback0

rtl#show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.10.2 on Serial0/0, 00:00:11 ago
  Routing Descriptor Blocks:
  * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via Serial0/0
    Route metric is 1, traffic share count is 1

```

Figura 1

```
rt1#show ip rip database
192.168.0.0/24    auto-summary
192.168.0.0/24    directly connected, Loopback0
192.168.10.0/24   auto-summary
192.168.10.0/24   directly connected, Serial0/0
200.200.200.0/24  auto-summary
200.200.200.0/24
[1] via 192.168.10.2, 00:00:20, Serial0/0
```

Figura 2

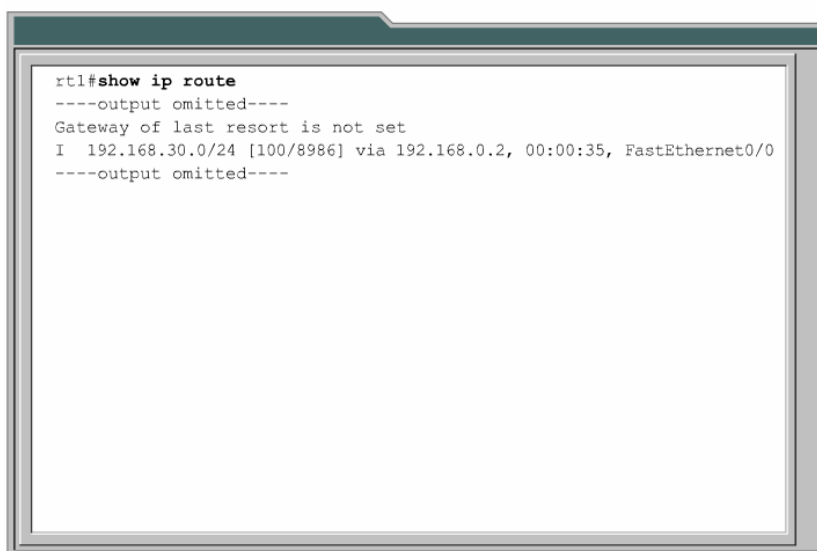
9.1.9 Observación de las múltiples rutas hacia un destino

Algunos protocolos de enrutamiento soportan múltiples rutas hacia un mismo destino. A diferencia de los algoritmos de ruta única, estos algoritmos de rutas múltiples permiten el tráfico a través de múltiples líneas, proporcionan un mejor rendimiento y son más confiables.

IGRP soporta balanceo de carga asimétrico, el cual se conoce como **variance**. El comando **variance** instruye al router a incluir rutas con métricas menores a n veces la métrica mínima para esa ruta, donde n es el número especificado por el comando **variance**. La variable n puede tomar valores entre 1 y 128, con el valor por defecto igual a 1, lo cual significa balanceo de carga simétrico.

Rt1 tiene dos rutas a la red 192.168.30.0. El comando Variance se fija en Rt1 para asegurar que ambas rutas se utilicen.

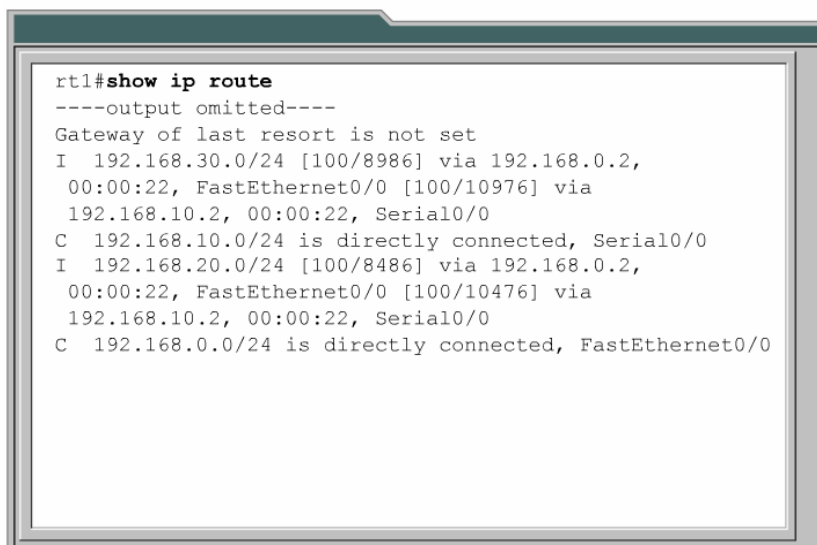
La Figura 1 muestra el resultado del comando **show ip route** ejecutado en Rt1 antes de configurada la variancia. La interfaz FastEthernet 0/0 es la única ruta a la red 192.168.30.0. Esta ruta tiene una distancia administrativa de 100 y un amétrica de 8986.



```
rt1#show ip route
----output omitted----
Gateway of last resort is not set
I 192.168.30.0/24 [100/8986] via 192.168.0.2, 00:00:35, FastEthernet0/0
----output omitted----
```

Figura 1

La Figura 2 muestra el resultado de **show ip route** ejecutado en Rt1 después de configurada la variancia. La mejor ruta es la interfaz FastEthernet 0/0, pero también se utiliza la interfaz Serial 0/0. Para verificar el balanceo de la carga, ejecute el comando **ping 192.168.30.1**.



```
rt1#show ip route
----output omitted----
Gateway of last resort is not set
I 192.168.30.0/24 [100/8986] via 192.168.0.2,
00:00:22, FastEthernet0/0 [100/10976] via
192.168.10.2, 00:00:22, Serial0/0
C 192.168.10.0/24 is directly connected, Serial0/0
I 192.168.20.0/24 [100/8486] via 192.168.0.2,
00:00:22, FastEthernet0/0 [100/10476] via
192.168.10.2, 00:00:22, Serial0/0
C 192.168.0.0/24 is directly connected, FastEthernet0/0
```

Figura 2

Una vez ejecutado **ping**, la mejor ruta es utilizando la interfaz Serial 0/0. IGRP utilizará balanceo de carga entre los dos enlaces. ³

```
rtl#show ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "igrp 1", distance 100, metric 8986
  Redistributing via igrp 1
  Advertised by igrp 1 (self originated)
  Last update from 192.168.10.2 on Serial0/0, 00:00:35 ago
  Routing Descriptor Blocks:
    192.168.0.2, from 192.168.0.2, 00:00:35 ago, via FastEthernet0/0
      Route metric is 8986, traffic share count is 1
      Total delay is 25100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.10.2, from 192.168.10.2, 00:00:36 ago, via Serial0/0
      Route metric is 10976, traffic share count is 1
      Total delay is 45000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Figura 3

9.2 Pruebas de red

9.2.1 Introducción a las pruebas de red

Las pruebas básicas de una red deben desarrollarse en secuencia comenzando desde una capa del modelo de referencia OSI a la siguiente. ¹ Se recomienda comenzar con la Capa 1 y continuar hasta llegar a la Capa 7, si fuera necesario. Comenzando con la Capa 1, busque problemas simples tales como cables de suministro conectados a la pared. Los problemas más frecuentes que se producen en las redes IP son causados por errores en el esquema de direccionamiento. Es importante verificar la configuración de direcciones antes de continuar con los siguientes pasos de configuración.

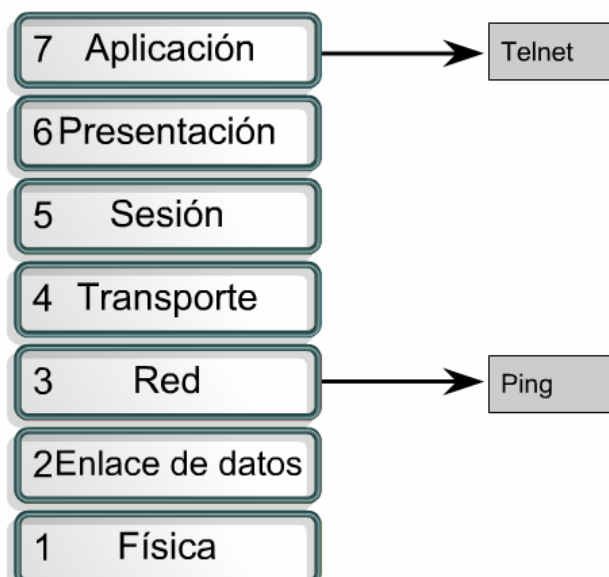


Figura 1

Cada prueba presentada en esta sección se ocupa de las operaciones de red en una capa específica del modelo de referencia OSI. Los comandos **telnet** y **ping** son dos comandos fundamentales que se utilizan para probar la red.

9.2.2 Uso de un enfoque estructurado en el diagnóstico de fallas

El diagnóstico de fallas es un proceso que permite que el usuario encuentre los problemas en una red. Debe existir un proceso ordenado para diagnosticar fallas basado en los estándares de networking establecidos

por un administrador de red. La documentación es una parte muy importante del proceso de diagnóstico de fallas. ¹

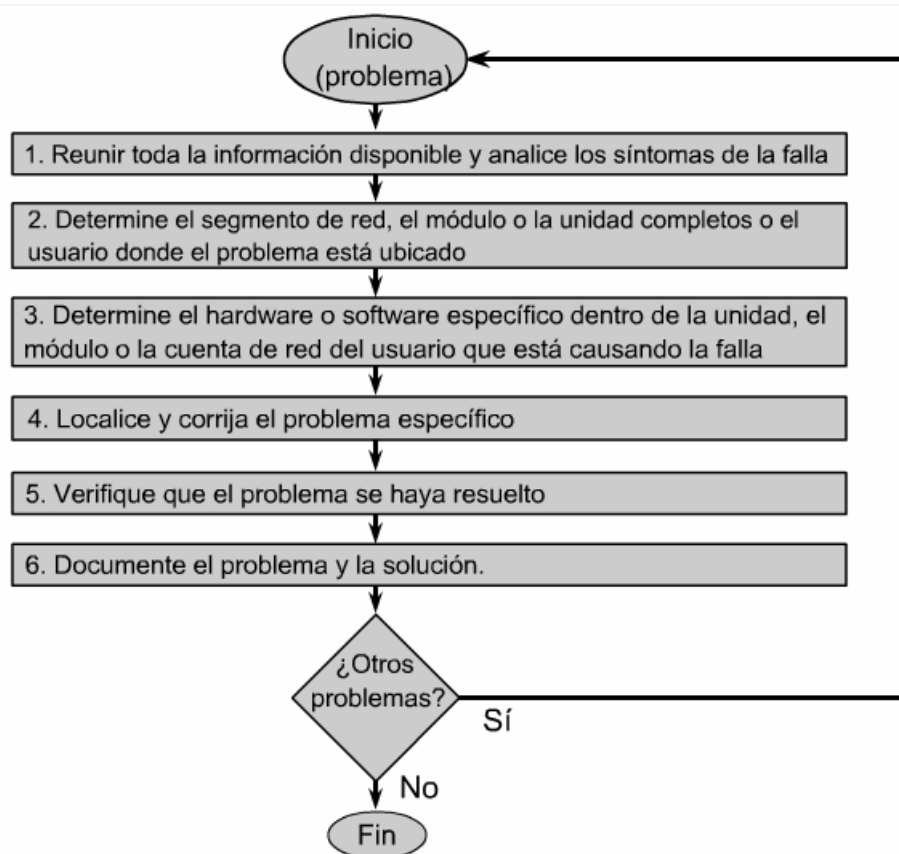


Figura 1

Los pasos de este modelo son:

Paso 1: Obtener toda la información disponible y analizar los síntomas de la falla

Paso 2: Circunscribir el problema a un segmento de la red, a un módulo o unidad completos o a un usuario.

Paso 3: Aislar la falla a un hardware o software específico dentro de la unidad, el módulo o la cuenta de red del usuario.

Paso 4: Localizar y corregir el problema específico.

Paso 5: Verificar si el problema se ha resuelto.

Paso 6: Documente el problema y la solución.

Un proceso ordenado es de fundamental importancia a fin de mantener la red en funcionamiento uniforme y eficiente.

Utilizando un enfoque estructurado para diagnosticar fallas, cada miembro de un equipo de asistencia técnica de redes puede saber cuáles son los pasos que cada miembro del grupo ha llevado a cabo para resolver el problema. Si se intenta llevar a cabo una variedad de ideas para el diagnóstico de fallas sin organización o documentación, la forma de solucionar los problemas no es efectiva. Aun si se resuelve el problema en un entorno no estructurado, probablemente resulte imposible repetir la solución en problemas similares en el futuro.

9.2.3 Prueba capa por capa OSI

La prueba debe comenzar con la Capa 1 del modelo OSI y continuar hasta la Capa 7 si fuera necesario.

Los errores de Capa 1 incluyen: ¹

- Cables defectuosos.

- Cables desconectados.
- Cables conectados a los puertos incorrectos.
- Conexión de cable intermitente.
- Cables inadecuados para la tarea (se deben usar los cables rollover, de conexión cruzada y de conexión directa (straight-through) correctamente).
- Problemas en el transceptor.
- Problemas en el cable del DCE.
- Problemas en el cable del DTE.
- Dispositivos apagados.



Figura 1



Figura 2



Figura 3

Los errores de Capa 2 incluyen: **2**

- Interfaces seriales incorrectamente configuradas.
- Interfaces Ethernet incorrectamente configuradas.
- Encapsulamiento incorrecto (HDLC es el encapsulamiento por defecto para las interfaces seriales).
- Configuraciones de temporización incorrectas en las interfaces seriales
- Problemas en la tarjeta de interfaz de red (NIC).

Los errores de Capa 3 incluyen: **3**

- Protocolo de enrutamiento no habilitado.
- Protocolo de enrutamiento incorrecto habilitado.
- Direcciones IP incorrectas.
- Máscaras de subredes incorrectas.

Si se producen errores en la red, debe iniciarse el proceso de prueba a través de las capas de OSI. El comando **ping** se utiliza en la Capa 3 para probar la conectividad. En la Capa 7, es posible utilizar el comando **telnet** para verificar el software de capa de aplicación entre las estaciones origen y destino. Ambos comandos se tratarán en mayor detalle en una sección posterior.

9.2.4 Diagnóstico de fallas en la Capa 1 utilizando indicadores

Las luces indicadoras constituyen una herramienta útil para el diagnóstico de fallas. La mayoría de las interfaces o NICs cuentan con luces indicadoras que muestran si la conexión es válida. A menudo, esta luz recibe el nombre "link". La interfaz también puede contar con luces que indican si se transmite (TX) o recibe (RX) tráfico. Si la interfaz cuenta con luces indicadoras que no muestran una conexión válida, apague el dispositivo y vuelva a colocar la tarjeta de la interfaz. Un cable no apropiado o defectuoso también puede hacer que la luz de enlace indique una mala conexión o la ausencia de enlace.

Verifique que todos los cables se conecten a los puertos correctos. Asegúrese de que todas las conexiones cruzadas realicen una adecuada conexión con la ubicación correcta utilizando el cable y método apropiados. Verifique que todos los puertos del hub o del switch se encuentren en la VLAN o en el dominio de colisión correctos y que se hayan configurado las opciones correctas para el spanning tres y demás consideraciones.

Verifique que se use el cable correcto. Puede resultar necesario el uso de un cable de interconexión cruzada para realizar conexiones directas entre dos switches o hubs o entre dos host, por ejemplo: PCs o routers. Verifique la correcta conexión del cable proveniente de la interfaz origen y su buen estado. Si

hubiera alguna duda de que la conexión es buena, vuelva a colocar el cable y controle que la conexión sea segura. Pruebe reemplazar el cable con otro que usted sepa que funciona. Si este cable se conecta a un toma de pared, utilice el analizador de cables para garantizar que la conexión esté bien cableada.

Además, controle todos los transceptores para garantizar que sean del tipo correcto y que estén bien conectados y configurados. Si reemplazar el cable no resuelve el problema, pruebe reemplazar el transceptor, si hubiera uno en uso.

Asegúrese siempre de que el dispositivo se encuentre encendido. Controle siempre los principios básicos antes de efectuar el diagnóstico o de intentar un diagnóstico de fallas complejo. ¹

Problemas comunes de la Capa 1
• Cables rotos • Cables desconectados • Cables conectados a los puertos incorrectos • Conexión de cable intermitente • Cables incorrectos para la tarea (se deben usar los cables de consola, de conexión cruzada y de conexión directa correctamente) • Problemas con el transceptor • Problemas del cable DCE • Problemas del cable DTE • Dispositivos apagados

Figura 1

9.2.5 Diagnóstico de fallas en la Capa 3 utilizando el comando ping

Ping se utiliza para verificar la conectividad de la red. Como ayuda para diagnosticar la conectividad básica de red, muchos protocolos de red admiten un protocolo de eco. Los protocolos de eco se utilizan para verificar el enrutamiento de los paquetes de protocolo. El comando **ping** envía un paquete al host destino y luego espera un paquete de respuesta de ese host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de ruta hacia el host, las demoras en la ruta y si se puede acceder al host o si este funciona. El resultado del comando **ping** muestra los tiempos mínimo, promedio y máximo que tarda un paquete ping en encontrar un sistema especificado y regresar. El comando **ping** utiliza el Protocolo de mensajes de control en Internet (ICMP) para verificar la conexión de hardware y la dirección lógica de la capa de red. La Figura ¹ es una tabla que muestra los distintos tipos de mensajes de ICMP. Este es un mecanismo de prueba sumamente básico para la conectividad de la red.

Mensaje	Propósito
Destination unreachable (Destino inalcanzable)	Esto indica al host origen que hay un problema para entregar un paquete.
Time exceeded (Tiempo superado)	Se ha tardado demasiado en entregar el paquete; el paquete se ha descartado.
Source quench (Disminución de velocidad en origen)	El origen está enviando datos más rápido que lo que pueden reenviarse. Este mensaje es una petición para que el remitente envíe los paquetes más lentamente.
Redirect (Redirigir)	El router que envía este mensaje ha recibido un paquete para el cual otro router puede tener una ruta mejor. El mensaje indica al remitente que debe usar la mejor ruta.
Echo (Eco)	El comando ping utiliza esto para verificar la conectividad.
Parameter problem (Problema de parámetros)	Esto se utiliza para identificar un parámetro que es incorrecto.
Timestamp (Marca horaria)	Esto se utiliza para medir el tiempo de recorrido de ida y vuelta a hosts específicos.
Petición/ respuesta de máscara de dirección	Esto se utiliza para consultar y conocer cuál es la máscara de subred correcta que se debe utilizar.
Publicación y selección del router	Esto se utiliza para permitir que los hosts averigüen de forma dinámica las direcciones IP de los routers conectados a la subred.

Figura 1

En la figura 2, el destino de ping 172.16.1.5 respondió con éxito a los cinco datagramas enviados. Los signos de exclamación (!) indican cada eco exitoso. Si se visualizan uno o más puntos (.) en lugar de signos de exclamación, significa que se venció el tiempo de espera de la aplicación en el router mientras se esperaba un eco de paquete proveniente del objetivo de **ping**.

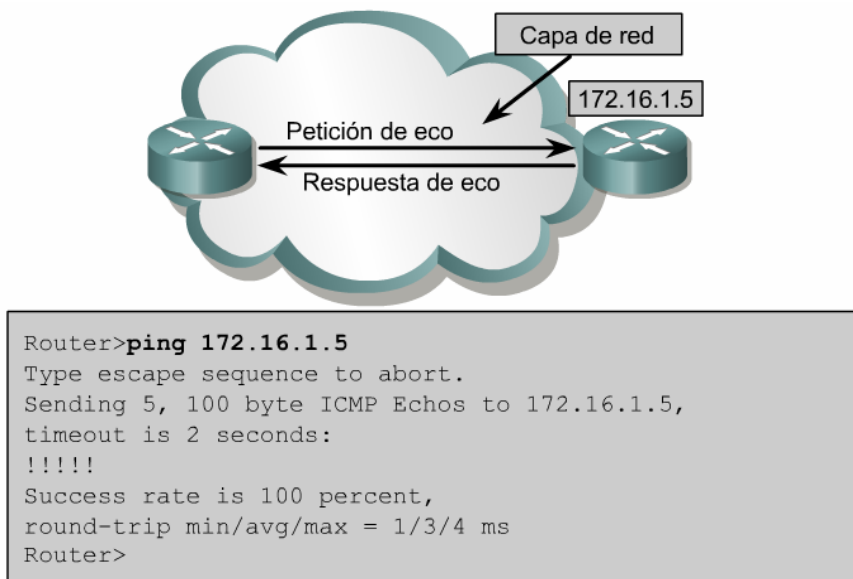


Figura 2

El siguiente comando activa una herramienta de diagnóstico que se usa para probar la conectividad.

Router#ping [protocol] {host | address}

El comando **ping** prueba las conexiones de red enviando peticiones de eco ICMP hacia un host objetivo y controla el tiempo de respuesta. El comando ping registra el número de paquetes enviados, el número de respuestas recibidas y el porcentaje de paquetes perdidos. También registra la cantidad de tiempo que tardan los paquetes en llegar al destino y las respuestas en ser recibidas. Esta información permite verificar la comunicación entre una estación de trabajo y otros host, y si se perdió información. 2

Es posible invocar el comando **ping** desde el modo EXEC del usuario y desde el modo EXEC privilegiado. El comando **ping** se puede utilizar para confirmar la conectividad básica de una red en AppleTalk, Servicio de red no orientado a la conexión ISO (CLNS), IP, Novell, Apollo, VINES, DECnet, o redes XNS.

El uso de un comando **ping** extendido hace que el router ejecute una variedad más extensa de opciones de prueba. Para utilizar **ping** extendido, escriba **ping** en la línea de comando, luego presione la tecla **Intro** sin ingresar una dirección IP. Aparecerán indicadores cada vez que se presiona la tecla **Intro**. Estos indicadores proporcionan muchas más opciones que el comando **ping** estándar.

Es una buena idea utilizar el comando **ping** cuando la red funciona correctamente para ver cómo funciona el comando en condiciones normales y de modo que sea posible compararlo cuando se ejecuta el diagnóstico de fallas.

9.2.6 Diagnóstico de fallas en la Capa 7 utilizando Telnet

Telnet es un protocolo de terminal virtual que forma parte del conjunto de protocolos TCP/IP. Permite la verificación del software de capa de aplicación entre las estaciones origen y destino. Es el mecanismo de prueba más completo disponible. La aplicación de telnet se utiliza generalmente para conectar dispositivos remotos, recopilar información y ejecutar programas.

La aplicación Telnet proporciona una terminal virtual para conectarse a routers que ejecutan TCP/IP. A los fines del diagnóstico de fallas, resulta de utilidad verificar que se pueda realizar la conexión utilizando Telnet. Esto prueba que, al menos, una aplicación TCP/IP es capaz de conectarse de extremo a extremo. Una conexión exitosa de Telnet indica que la aplicación de capa superior y los servicios de las capas inferiores funcionan correctamente. 1

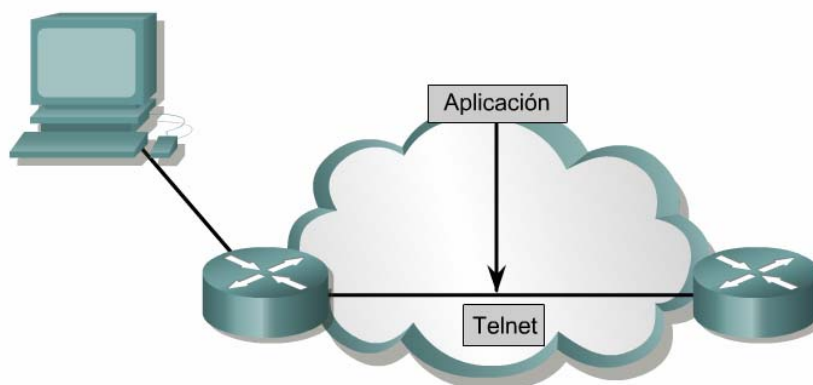


Figura 1

Si un administrador puede conectarse por Telnet con un router pero no con otro, verifique la conectividad de la capa inferior. Si se ha verificado la conectividad, probablemente la falla de Telnet se deba a problemas de permiso de acceso, denominación o direccionamiento específicos. Estos problemas pueden producirse en el router del administrador o en el router que falló como objetivo de Telnet.

Si la conexión Telnet con un servidor particular falla desde un host, pruebe conectarse desde un router y desde otros dispositivos diferentes. Cuando trate de conectarse por Telnet, si no aparece el indicador de conexión, verifique lo siguiente:

- ¿Se puede realizar una verificación DNS inversa de la dirección del cliente? Muchos servidores Telnet no permiten conexiones desde direcciones IP que no tienen entrada DNS. Este es un problema frecuente de las direcciones asignadas por DHCP en que el administrador no ha agregado entradas DNS adicionales para los grupos DHCP.
- Es posible que la aplicación Telnet no pueda negociar las opciones adecuadas y, por lo tanto, no se produce la conexión. En un router Cisco, este proceso de negociación se puede visualizar utilizando el comando **debugtelnet**.
- Es posible que el servicio Telnet esté desactivado o que se haya trasladado a un puerto diferente al 23 en el servidor destino.

9.3 Descripción general del diagnóstico de fallas del router

9.3.1 Diagnóstico de fallas de la Capa 1 utilizando el comando **show interfaces**

Cisco IOS contiene un conjunto de comandos completo para el diagnóstico de fallas. Entre los más usados se encuentran los comandos **show**. Cada aspecto del router puede visualizarse con uno o más comandos **show**.

El comando **show** utilizado para verificar el estado y las estadísticas de las interfaces es el comando **show interfaces**. El comando **show interfaces** sin argumentos entrega el estado y las estadísticas de todas las interfaces del router. El comando **show interfaces <interface name>** entrega el estado y las estadísticas del puerto indicado. Para ver el estado de la interfaz serial 0/0, use el comando **show interfaces serial 0/0**.

El estado de dos porciones importantes de las interfaces se muestra con el comando **show interfaces**. Son la porción física (hardware) y la porción lógica (software). Pueden estar relacionadas con las funciones de Capa 1 y Capa 2.

El hardware incluye a los cables, conectores e interfaces que muestran el estado de la conexión física entre los dispositivos. El estado del software muestra el estado de los mensajes, por ejemplo: mensajes de actividad, información de control e información del usuario que se transmiten entre los dispositivos adyacentes. Esto se relaciona con el estado del protocolo de Capa 2 que se transfiere entre dos interfaces de router conectadas.

Estos elementos fundamentales del resultado del comando **show interfaces serial** se muestran como estado del protocolo de enlace de datos y de la línea. ¹

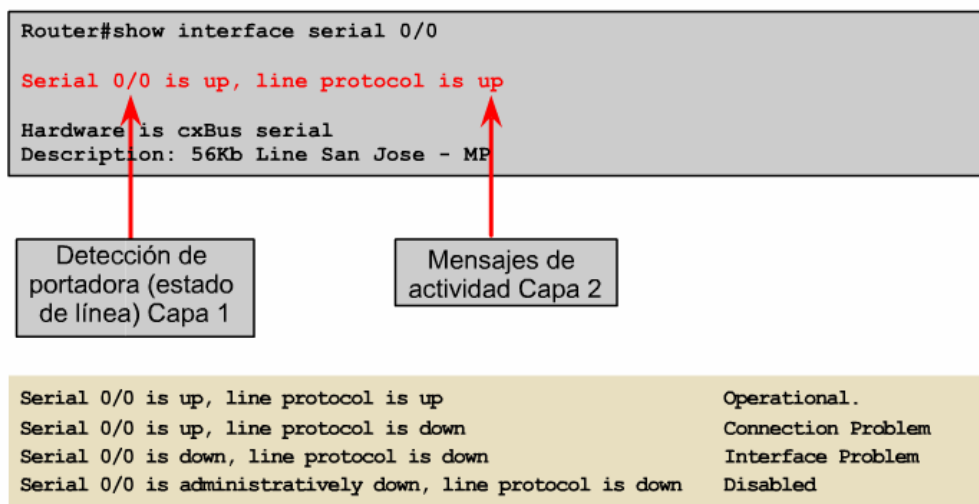


Figura 1

El primer parámetro se refiere a la capa de hardware y básicamente refleja si la interfaz recibe la señal de detección de portadora (CD) proveniente del otro extremo de la conexión. Si la línea está desactivada, hay un problema con el cableado, el equipo puede estar apagado en alguna parte del circuito o puede estar funcionando mal, o puede haber sido administrativamente desactivada. Si la interfaz está en el estado administrativamente desactivada, ha sido manualmente desactivada en la configuración.

El comando **show interfaces serial** también proporciona información de ayuda para el diagnóstico de otros problemas de la Capa 1 que no resultan fáciles de determinar. Un número creciente de recuentos de transiciones de portadora en un enlace serial puede indicar uno o más de los siguientes problemas:

- Interrupciones en la línea debido a problemas en la red del proveedor de servicios de red.
- Switch, DSU o hardware del router defectuosos.

Si aparece un número creciente de errores de entrada en el resultado del comando **show interfaces serial**, varios son las causas posibles de estos errores. Algunos son problemas relacionados con la Capa 1, a saber.

- Equipo de la compañía de telefonía defectuoso.
- Línea serial con ruidos.
- Cable o longitud de cable incorrectos.
- Cable o conexión dañados.
- CSU o DSU defectuosas.
- Hardware del router defectuoso.

Otra área a examinar es el número de reinicios de las interfaces. Son el resultado de la pérdida de demasiados mensajes de actividad. Los siguientes problemas de Capa 1 pueden ser causa de los reinicios de las interfaces:

- Línea inadecuada que produce transiciones de la portadora.
- Posible problema de hardware en la CSU, DSU, o en el switch

Si las transiciones de portadora y los reinicios de las interfaces aumentan o si los errores de entrada son muchos a medida que aumentan los reinicios de la interfaz, el problema probablemente sea un enlace inadecuado o CSU o DSU defectuosas.

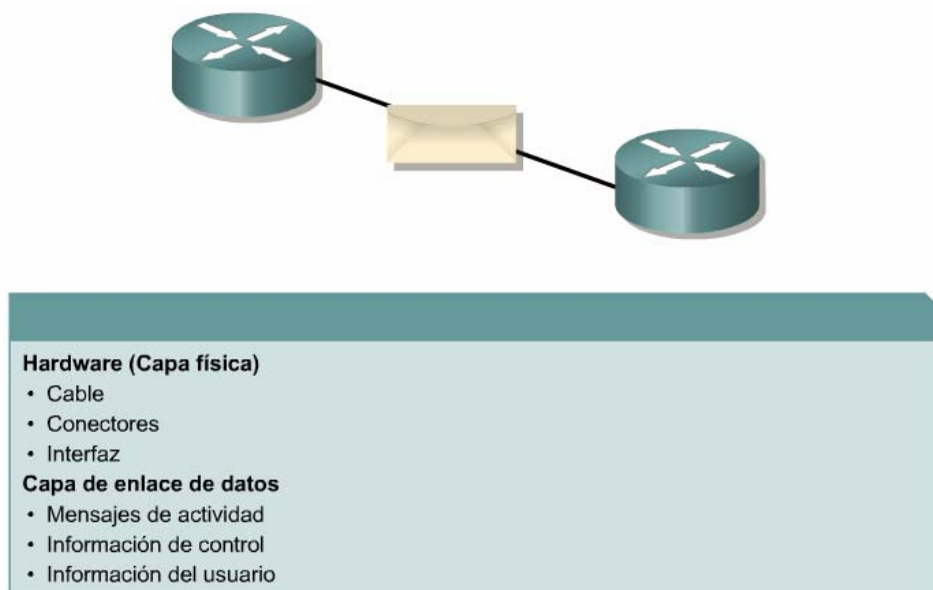
El número de errores debe interpretarse en relación a la cantidad de tráfico que ha procesado el router y la cantidad de tiempo durante el cual las estadísticas han sido capturadas. El router registra estadísticas que suministran información acerca de la interfaz. Las estadísticas reflejan el funcionamiento de un router desde que se puso en marcha o desde la última vez que se reiniciaron los contadores.

Si el resultado del comando **show interfaces** muestra que nunca se reiniciaron los contadores, utilice el comando **show version** para saber cuánto hace que el router se encuentra en funcionamiento.

Utilice el comando **clear counters** para poner los contadores en cero. Siempre es necesario reiniciar los contadores después de la corrección de un problema en la interfaz. Comenzar desde cero brinda un mejor cuadro sobre el estado actual de la red y ayuda a verificar que la corrección del problema sea real.

9.3.2 Diagnóstico de fallas de la Capa 2 utilizando el comando show interfaces

El comando **show interfaces** es tal vez la única herramienta de importancia para descubrir problemas de Capa 1 y de Capa 2 con el router. El primer parámetro (línea) se refiere a la capa física. El segundo parámetro (protocolo) indica si los procesos del IOS que controlan el protocolo de la línea consideran utilizable la interfaz o no. Esto está determinado por la recepción exitosa de los mensajes de actividad. Se entiende por mensajes de actividad a los mensajes enviados por un dispositivo de red para informar a otro que el circuito virtual entre ambos sigue estando activo. Si la interfaz pierde tres mensajes de actividad consecutivos, el protocolo de línea se marca como desactivado.



Siempre que la línea esté desactivada, el protocolo también lo está porque no existe un medio utilizable para el protocolo de Capa 2. Esto se aplica cuando la interfaz se encuentra desactivada debido a un problema de hardware y cuando esté desactivada por el administrador.

Si la interfaz está activada y el protocolo de línea no, existe un problema en la Capa 2. Las posibles causas son:

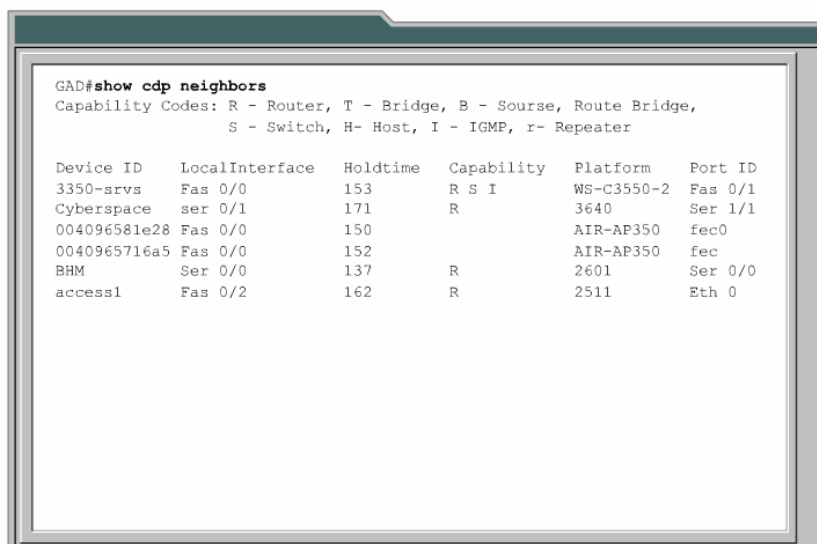
- Falta de mensajes de actividad.
- Falta de velocidad de reloj.
- Falta de concordancia en el tiempo de encapsulamiento.

El comando **show interfaces serial** debe utilizarse después de configurar una interfaz serial a fin de verificar los cambios y que la interfaz se encuentre operando.

9.3.3 Diagnóstico de fallas utilizando el comando show cdp

Cisco Discovery Protocol (CDP) divulga la información sobre el dispositivo a sus vecinos directos incluyendo direcciones IP y MAC e interfaces salientes.

El resultado del comando **show cdp neighbors** muestra información sobre los dispositivos Cisco vecinos que se conectan de forma directa. ¹Esta información es de utilidad para la depuración de los temas relacionados con la conectividad. Si se sospecha que el problema es de cableado, habilite las interfaces con el comando **no shutdown** y luego ejecute el comando **show cdp neighbors detail** antes de cualquier configuración. Este comando muestra el detalle del dispositivo específico, por ejemplo: interfaces, ID del puerto y el dispositivo. También muestra la versión del Cisco IOS que se ejecuta en los dispositivos remotos.



```
GAD#show cdp neighbors
Capability Codes: R - Router, T - Bridge, B - Source, Route Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	LocalInterface	Holdtime	Capability	Platform	Port ID
3350-srvs	Fas 0/0	153	R S I	WS-C3550-2	Fas 0/1
Cyberspace	ser 0/1	171	R	3640	Ser 1/1
004096581e28	Fas 0/0	150		AIR-AP350	fec0
0040965716a5	Fas 0/0	152		AIR-AP350	fec
BHM	Ser 0/0	137	R	2601	Ser 0/0
access1	Fas 0/2	162	R	2511	Eth 0

Figura 1

Si la capa física funciona correctamente, entonces también se muestran todos los restantes dispositivos Cisco directamente conectados. Si no aparece un dispositivo conocido, probablemente el problema sea de Capa 1.

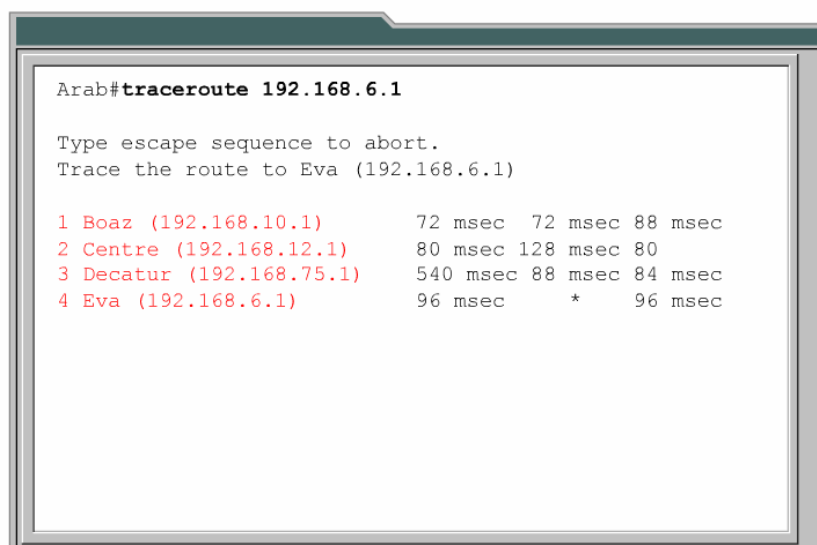
Un área problemática para CDP es la seguridad. La cantidad de información que CDP proporciona es tan inmensa que puede ser un potencial agujero en la seguridad. Por razones de seguridad, CDP debe configurarse sólo en enlaces entre dispositivos Cisco y inhabilitarse en puertos o enlaces de usuario no administrados a nivel local.

9.3.4 Diagnóstico de fallas utilizando el comando traceroute

El comando **traceroute** se utiliza para descubrir las rutas que toman los paquetes cuando viajan hacia su destino. Traceroute también puede utilizarse para ayudar a verificar la capa de red (Capa 3) teniendo en cuenta salto por salto y para proporcionar puntos de referencia para el desempeño.

El comando **traceroute** a menudo se refiere como comando **trace** en los materiales de referencia. Sin embargo, la sintaxis correcta del comando es **traceroute**.

El resultado del comando **traceroute** genera una lista de saltos alcanzados de forma exitosa. Si los datos finalmente llegan a su destino, entonces el resultado indica cada router por el que pasa el datagrama. Es posible capturar y utilizar este resultado para futuros diagnósticos de fallas en internetwork.



```
Arab#traceroute 192.168.6.1

Type escape sequence to abort.
Trace the route to Eva (192.168.6.1)
```

Hop	Router (IP)	1st	2nd	3rd	4th
1	Boaz (192.168.10.1)	72 msec	72 msec	88 msec	
2	Centre (192.168.12.1)	80 msec	128 msec	80	
3	Decatur (192.168.75.1)	540 msec	88 msec	84 msec	
4	Eva (192.168.6.1)	96 msec	*	96 msec	

Figura 1

El resultado de **traceroute** también indica el salto específico donde se produce la falla. Para cada router de la ruta se genera una línea de resultado en la terminal que indica la dirección IP de la interfaz que ingresó los datos. Si aparece un asterisco (*), el paquete falló. Si se obtiene el último salto exitoso del resultado de **traceroute** y se lo compara con el diagrama de internetwork, es posible aislar el área del problema.

Traceroute también brinda información que indica el desempeño relativo de los enlaces. El tiempo de ida y vuelta (RTT) es el tiempo necesario para enviar un paquete de eco y obtener una respuesta. ¹ Esto es útil para tener una idea aproximada del retardo del enlace. Estos valores no son suficientemente precisos como para ser utilizados para una evaluación exacta del desempeño. Sin embargo, es posible capturar y utilizar este resultado para futuros diagnósticos de fallas en el desempeño de la internetwork.

Tenga en cuenta que el dispositivo que recibe el **traceroute** también tiene que saber cómo enviar la respuesta nuevamente hacia el origen del **traceroute**. Para que los datos del comando **traceroute** o **ping** completen el recorrido con éxito entre los routers, debe haber rutas conocidas en ambas direcciones. Una falla en la respuesta no siempre indica un problema ya que los mensajes ICMP pueden estar limitados por la velocidad o filtrados en el sitio del host. Esto se aplica en especial a Internet.

Traceroute envía una secuencia de datagramas de Protocolo de datagramas de usuario (UDP) desde el router hacia una dirección de puerto inválida en el host remoto. Para la primera secuencia de tres datagramas enviada, el valor de campo de Tiempo de existencia (TTL) se establece en uno. El valor de TTL de 1 hace que el datagrama expire el tiempo de espera en el primer router de la ruta. Este router entonces responde con un Mensaje ICMP de tiempo excedido (TEM) que indica que ha caducado el datagrama.

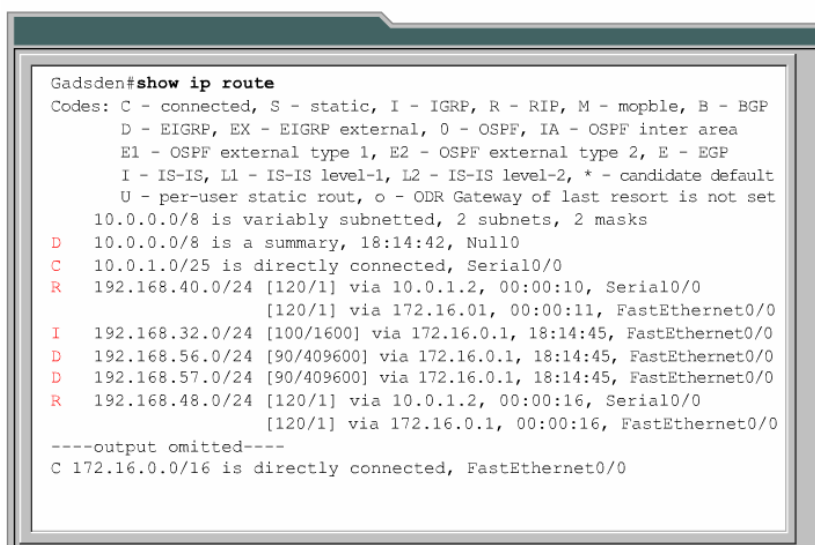
Luego, se envían tres mensajes UDP adicionales, esta vez con un valor de TTL de 2. Esto hace que el segundo router devuelva los TEM ICMP. Este proceso continúa hasta que los paquetes alcanzan su destino o se ha alcanzado el valor TTL máximo. El valor TTL máximo por defecto para el comando **traceroute** es 30.

Como estos datagramas tratan de acceder a un puerto inválido en el host destino, los mensajes que vuelven son ICMP de puerto inalcanzable y no ICMP de tiempo excedido. Esto indica un puerto inalcanzable y señala que el programa **traceroute** da por terminado el proceso.

9.3.5 Diagnóstico de los problemas relacionados con el enrutamiento

Los comandos **show ip protocols** y **show ip route** muestran información sobre los protocolos de enrutamiento y la tabla de enrutamiento. El resultado de estos comandos puede utilizarse para verificar la configuración del protocolo de enrutamiento.

El comando **show ip route** es tal vez el único comando fundamental para el diagnóstico de problemas relacionados con el enrutamiento. Este comando muestra el contenido de la tabla de enrutamiento IP. El resultado del comando **show ip route** muestra las entradas para todas las redes y subredes conocidas y de qué forma se obtuvo la información. ¹



```
Gadsden#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mospble, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static rout, o - ODR Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D 10.0.0.0/8 is a summary, 18:14:42, Null0
C 10.0.1.0/25 is directly connected, Serial0/0
R 192.168.40.0/24 [120/1] via 10.0.1.2, 00:00:10, Serial0/0
   [120/1] via 172.16.0.1, 00:00:11, FastEthernet0/0
I 192.168.32.0/24 [100/1600] via 172.16.0.1, 18:14:45, FastEthernet0/0
D 192.168.56.0/24 [90/409600] via 172.16.0.1, 18:14:45, FastEthernet0/0
D 192.168.57.0/24 [90/409600] via 172.16.0.1, 18:14:45, FastEthernet0/0
R 192.168.48.0/24 [120/1] via 10.0.1.2, 00:00:16, Serial0/0
   [120/1] via 172.16.0.1, 00:00:16, FastEthernet0/0
----output omitted----
C 172.16.0.0/16 is directly connected, FastEthernet0/0
```

Figura 1

Si el problema se produce al llegar al host de una red en particular, entonces es posible utilizar el resultado del comando **show ip route** para verificar que el router tenga una ruta hacia dicha red.

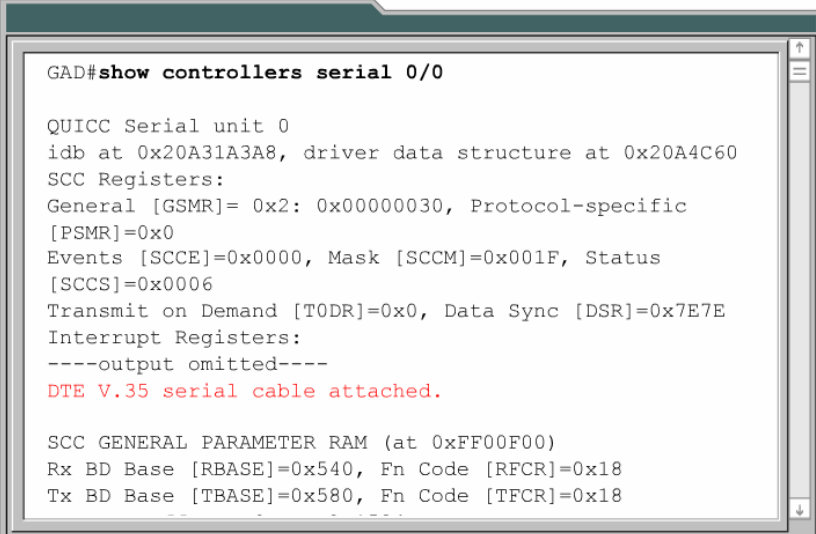
Si el resultado del comando **show ip route** no muestra que se tomaron las rutas aprendidas esperadas o que no hay rutas aprendidas, entonces el problema posiblemente sea la falta de intercambio en la información de enrutamiento. En este caso, utilice el comando **show ip protocols** en el router para verificar el error de configuración del protocolo de enrutamiento.

El comando **show ip protocols** muestra los valores sobre la información del protocolo IP de enrutamiento de todo el router. Este comando se puede utilizar para confirmar cuáles son los protocolos configurados, cuáles son las redes divulgadas, cuáles son las interfaces que envían actualizaciones y las actualizaciones de los orígenes del enrutamiento. El resultado del comando **show ip protocols** también muestra los temporizadores, los filtros, el resumen de las rutas, la redistribución de las rutas y otros parámetros que son específicos para cada protocolo de enrutamiento que se habilita en el router. Cuando se configuran múltiples protocolos de enrutamiento, la información sobre cada protocolo se enumera en una lista por separado.

El resultado del comando **show ip protocols** se puede utilizar para diagnosticar una gran variedad de problemas de enrutamiento, incluyendo la identificación de un router del que se sospecha envía información incorrecta sobre un router. Puede utilizarse para confirmar la presencia de los protocolos esperados, las redes divulgadas y los vecinos de enrutamiento. Como sucede con cualquier proceso de diagnóstico de fallas, identificar el problema es difícil pero no imposible si no se dispone de documentación que indique lo esperado.

9.3.6 Diagnóstico de fallas utilizando el comando show controllers

Muy a menudo, la configuración y el diagnóstico de fallas de los routers se realiza de forma remota, cuando no es posible inspeccionar físicamente las conexiones del router. El comando **show controllers** es de utilidad para determinar el tipo de cable conectado sin inspeccionar los cables. ¹



```
GAD#show controllers serial 0/0

QUICC Serial unit 0
idb at 0x20A31A3A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]= 0x2: 0x00000030, Protocol-specific
[PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x0006
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
----output omitted----
DTE V.35 serial cable attached.

SCC GENERAL PARAMETER RAM (at 0xFF00F00)
Rx BD Base [RBASE]=0x540, Fn Code [RFCR]=0x18
Tx BD Base [TBASE]=0x580, Fn Code [TFCR]=0x18
```

Figura 1

Examinando el resultado del comando **show controllers**, es posible determinar el tipo de cable que el controlador detecta. Resulta útil para encontrar una interfaz serial sin cable, el tipo de cable inadecuado o un cable defectuoso.

El comando **show controllers serial 0/0** interroga al circuito integrado (chip) que controla las interfaces seriales y muestra información acerca de la interfaz física serial 0/0. Incluso dentro de un tipo de router, pueden utilizarse chips de controlador distintos.

Sin tener en cuenta el tipo de controlador, el comando **show controllers serial** genera un resultado impresionante. Excepto por el tipo de cable, la mayor parte de este resultado es detalle técnico interno relacionado con el estado del chip del controlador. Sin conocimiento específico del circuito integrado, esta información carece de utilidad.

9.3.7 Introducción al comando debug

El comando **debug** ayuda a aislar los problemas de configuración y de protocolo. El comando **debug** se utiliza para mostrar los sucesos y datos dinámicos. Como los comandos **show** sólo muestran información estática, brindan un cuadro histórico de la operación del router. Con el comando **debug**, el resultado brinda una visión interna de los sucesos que se producen en el router. Estos sucesos pueden ser tráfico en una interfaz, mensajes de error generados por los nodos de una red, paquetes de diagnóstico específicos del protocolo y otros datos útiles para el diagnóstico de fallas. ¹El resultado dinámico del comando **debug** se genera a costa del desempeño, produciendo un mayor encabezado en el procesador que puede interrumpir el funcionamiento normal del router. Por este motivo, **debug** sólo debe utilizarse de forma moderada. Utilice los comandos **debug** para examinar los tipos de tráfico o problemas específicos una vez que los problemas potenciales se circunscriban a unas pocas causas.

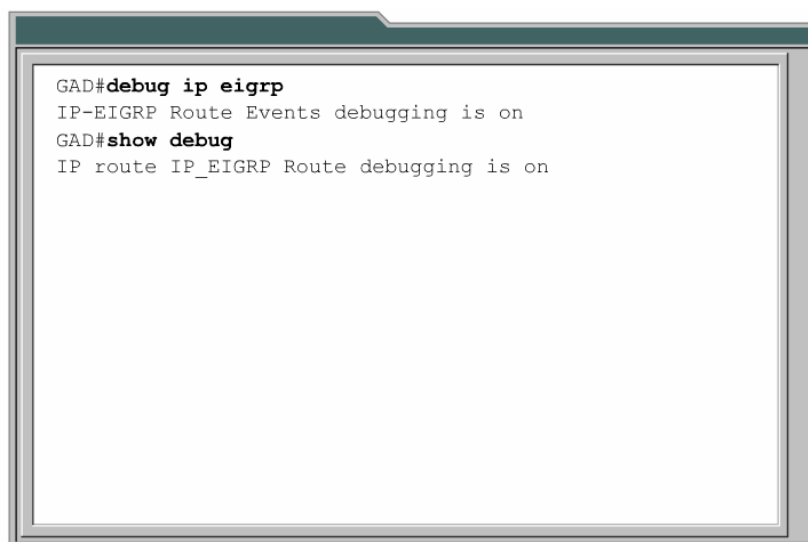


Figura 1

ADVERTENCIA:

El comando **debug** **all** se debe utilizar moderadamente ya que puede interrumpir las operaciones del router.

Por defecto, el router envía el resultado de **debug** y los mensajes del sistema a la consola. Si se utiliza una sesión por telnet para examinar el router, entonces, es posible redirigir el resultado de **debug** y los mensajes del sistema hacia a terminal remota. Esto se hace a través de la sesión por telnet emitiendo el comando **terminal monitor**. Es necesario tener sumo cuidado al seleccionar los comandos **debug** a partir de una sesión por telnet. No se debe elegir ningún comando que haga que el resultado de **debug** cree un tráfico adicional que, a su vez, cree un resultado de **debug**. Si esto sucede, la sesión por telnet rápidamente saturará el enlace con tráfico o el router agotará uno o más recursos. Una buena regla a seguir para evitar esta repetición de tráfico es "Nunca debug (depurar) ninguna actividad en el puerto donde se establece la sesión".

El resultado de los distintos comandos **debug** varía. Con frecuencia, algunos pueden generar muchas líneas mientras que otros producen una o dos líneas de resultado cada pocos minutos.

Otro servicio del IOS que mejorará la utilidad de la salida del comando **debug** es el comando **timestamps**. Este comando pondrá una marca de tiempo en el mensaje del comando **debug**. Esta información proporciona la hora de ocurrencia del evento de depuración y el tiempo transcurrido entre eventos.

Esto es a menudo muy útil para el diagnóstico de fallas de problemas intermitentes. Poniendo marcas de tiempo en la salida, a menudo se puede reconocer un patrón de ocurrencia. Esto ayuda a aislar la fuente del problema. El siguiente comando configura una marca de tiempo que mostrará las horas:minutos:segundos de la salida, la cantidad de tiempo transcurrido desde que el router se encendió por última vez o desde que se ejecutó un comando reload:

```
GAD(config)#service timestamps debug uptime
```

La salida de este comando es útil para determinar el tiempo transcurrido entre eventos. Para determinar cuanto tiempo ha pasado desde la última ocurrencia del evento debug, se tiene que usar como referencia el

tiempo desde la última reinicialización del router. Este tiempo se puede encontrar con el comando **show version**.

Un uso más práctico de las marcas de tiempo es que muestren la fecha y hora en la que el evento ocurrió. Esto simplificará el proceso de determinar la última ocurrencia del evento debug. Esto se hace con la opción **datetime**:

GAD(config)#**service timestamps debug datetime localtime**

Se debe notar que este comando es útil solamente si el reloj se encuentra configurado en el router. De otra manera, la marca de tiempo mostrada en la salida del comando debug no es un tiempo preciso. Para asegurar que las marcas de tiempo sean correctas, el reloj del router se debe configurar con la hora y fecha correcta desde el modo EXEC privilegiado usando el siguiente comando:

GAD#**clock set 15:46:00 3 May 2004**

NOTA:

En algunas plataformas Cisco, el reloj del router no se respalda con una batería, de manera que la hora del sistema se borrará después de una reinicialización del router o una falla de energía.

El comando **no debug all** o el comando **undebg all** desactivan el resultado de diagnóstico. Para inhabilitar un comando **debug** en particular, utilice la forma no del comando. Por ejemplo: si se habilita debug para monitorear RIP con el comando **debug ip rip**, es posible inhabilitarlo con **no debug ip rip**. Para visualizar lo que se está examinando con el comando **debug**, utilice el comando **show debugging**.

Resumen

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

- Comando **show ip route**.
- Determinación del gateway de último recurso.
- Determinación la dirección origen y destino de una ruta
- Determinación de la distancia administrativa de la ruta
- Determinación de la métrica de una ruta.
- Determinación del salto siguiente en la ruta.
- Determinación de la última actualización de la ruta.
- Observación de las múltiples rutas hacia un destino
- Uso de un enfoque estructurado en el diagnóstico de fallas
- Prueba capa por capa OSI
- Diagnóstico de fallas en la Capa 1 utilizando indicadores.
- Diagnóstico de fallas en la Capa 3 utilizando el comando ping.
- Diagnóstico de fallas en la Capa 7 utilizando Telnet.
- Diagnóstico de fallas de la Capa 1 utilizando el comando **show interfaces**.
- Diagnóstico de fallas de la Capa 2 utilizando el comando **show interfaces**.
- Diagnóstico de fallas utilizando el comando **cdp**.
- Diagnóstico de fallas utilizando el comando **traceroute** .
- Diagnóstico de problemas de enrutamiento con los comandos **show ip route** y **show ip protocols**.
- Diagnóstico de fallas utilizando el comando **show controllers**.
- Diagnóstico de fallas utilizando los comandos **debug**.

Módulo 10: TCP/IP intermedio

Descripción general

Los routers utilizan información de la dirección del Protocolo de Internet (IP) en un encabezado IP del paquete para determinar cuál es la interfaz hacia la que se conmutará el paquete para que llegue lo más cerca posible de su destino. Como IP no brinda ningún servicio que ayude a asegurar que el paquete realmente llegue a destino, se describe como un protocolo no confiable, no orientado a conexión que hace uso de entregas de mejor esfuerzo. Si los paquetes se descartan en la ruta, llegan en el orden incorrecto o se transmiten a una velocidad mayor a la que el receptor puede aceptar, IP, por si mismo, no puede corregir el problema. Para resolver los problemas, IP confía en el Protocolo de control de transmisión (TCP). Este módulo describe el TCP y sus funciones e introduce el UDP, otro importante protocolo de Capa 4.

Cada capa del modelo de networking de OSI cumple varias funciones. Estas funciones son independientes de las otras capas. Cada capa espera recibir servicios de la capa inferior y cada una provee ciertos servicios a su capa superior. Las capas de aplicación, presentación y de sesión del modelo OSI son todas parte de la capa de aplicación del modelo TCP/IP, acceden a los servicios de la capa de transporte a través de entidades lógicas llamadas puertos. Este módulo presenta el concepto de puertos y explica su fundamental importancia y la de los números de puerto en el networking con datos.

Los estudiantes que completen este módulo deberán ser capaces de:

- Describir TCP y sus funciones.
- Describir sincronización y control de flujo de TCP.
- Describir operación y procesos de UDP.
- Identificar los números de puerto comunes.
- Describir las múltiples conversaciones entre los host.
- Identificar los puertos que se utilizan para servicios y clientes.
- Describir la numeración de los puertos y los puertos conocidos.
- Comprender las diferencias y la relación entre las direcciones MAC, direcciones IP y los números de los puertos.

10.1 Operación del TCP

10.1.1 Operación del TCP

Las direcciones IP permiten el enrutamiento de los paquetes entre las redes. Sin embargo, IP no garantiza la entrega. La capa de transporte es responsable del transporte confiable y de la regulación del flujo de datos desde el origen hacia el destino. Esto se logra utilizando ventanas deslizantes y números de secuencia junto con un proceso de sincronización que garantiza que cada host se encuentra listo y desea comunicarse. ¹



Figura 1

Para comprender la confiabilidad y el control de flujo, piense en un estudiante que ha estudiado un idioma extranjero durante un año. Ahora imagine que este estudiante visita un país donde se habla ese idioma. Durante las conversaciones, deberá pedirle a la gente que repita lo que ha dicho (para confiabilidad) y que hable despacio, para que pueda entender las palabras (control de flujo). La capa de transporte, la Capa 4 del modelo OSI, provee estos servicios a la capa 5 por medio de TCP.

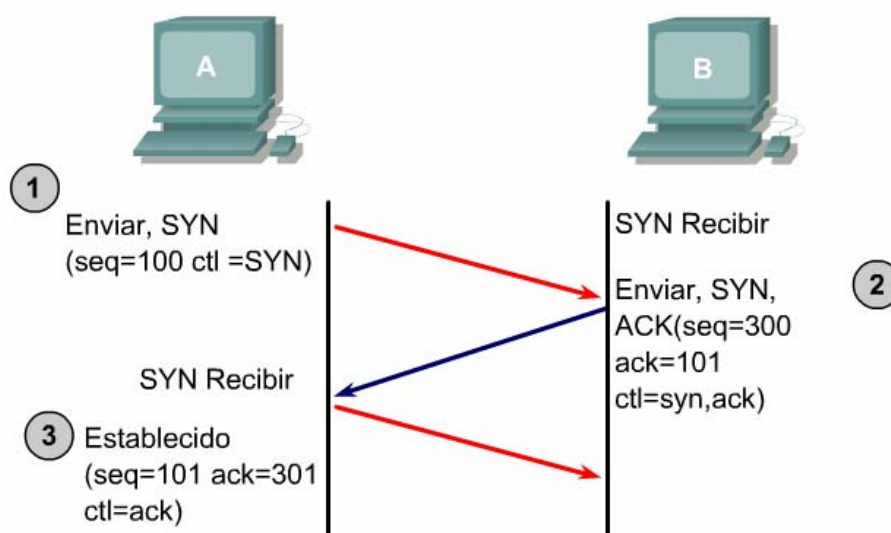
10.1.2 Sincronización del intercambio de señales de 3 vías

TCP es un protocolo orientado a conexión. Antes de transmitir datos, los dos clientes que desean comunicarse deben llevar a cabo un proceso de sincronización para establecer una conexión virtual para cada sesión entre ellos. Este proceso de sincronización asegura que ambas partes estén listas para la transmisión y permite que los dispositivos determinen los números de la secuencia inicial de dicha sesión. Este proceso se llama saludo de tres vías, es un proceso de tres pasos para establecer una conexión virtual entre dos dispositivos. Es muy importante saber que este proceso lo inicia un cliente. Para establecer la sesión TCP, el cliente usa un puerto conocido del servicio que desea contactar.

0	4	10	16	24	31
Puerto origen			Puerto destino		
Número de secuencia					
Número de acuse de recibo					
Hlen	Reservado	Bits de código	Ventana		
Checksum			Puntero urgente		
Opciones (de haberlas)				Relleno	
Datos					
...					

En el paso uno, el cliente inicia la sincronización enviando un paquete SYN para iniciar la conexión. Esto indica que el paquete tiene un Número secuencial Válido. El bit de SYN se encuentra en el campo de código del encabezado del segmento.

En el paso dos, el otro host recibe el paquete, graba el Número Secuencial x del cliente, y responde con un Acuse de Recibo (ACK). El bit de control del ACK indica que el campo de Acuse de Recibo contiene un número válido. el ACK es un bit en el campo de código del encabezado del segmento TCP, y el número ACK es un campo de 32 bits en el mismo encabezado. Una vez hecha la conexión, la bandera de ACK se fija para todos los segmentos durante la sesión. El campo de Número de ACK contiene el siguiente Número Secuencial que se espera recibir ($x + 1$). El número ACK $x + 1$ significa que el host ya recibió todos los bytes incluyendo x , y espera recibir el byte $x + 1$. El host también inicia un regreso de sesión, esto incluye un segmento TCP con su propio Número Secuencial y bandera de sincronización.



En el paso tres, el host que inició la conversación responde con un Número de ACK de $y + 1$, el cual es el Número Secuencial del valor del Host B + 1. Esto indica que recibió el ACK anterior y finaliza el proceso de conexión para esta sesión.

Es importante entender que los números secuenciales iniciales se usan sólo para comenzar la comunicación entre dos dispositivos. Actúan como referencia entre los dos dispositivos. Dichos números le dan a cada host la posibilidad de mandar acuses de recibo.

10.1.3 Ataques de denegación de servicio

Esta página enseñará a los estudiantes acerca de los ataques de negación de Servicio (DoS). Estos ataques están diseñados para denegar servicios a host legítimos que tratan de establecer conexiones. Los ataques DoS son muy comunes entre hackers para anular las respuestas de los sistemas. Un tipo de DoS es el inundamiento de SYN o SYN flooding. SYN flooding explota el saludo de tres vías y causa que los dispositivos manden un ACK a direcciones origen que no completarán el saludo.

El saludo de tres vías empieza al mandar un paquete SYN, el cual incluye las IP origen y destino. Ambas direcciones se utilizan para mandar ACK.¹

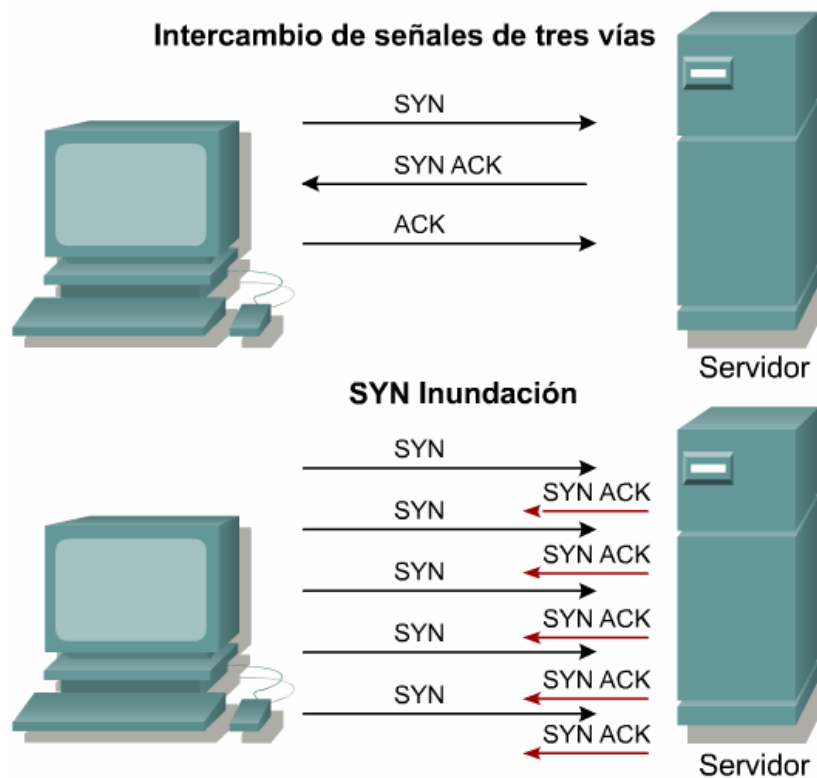


Figura 1

En un ataque DoS, el hacker inicia un SYN pero falsifica la IP, es decir hace un Spoofing. Spoofing es un término usado cuando el cliente destino responde a una dirección origen que no existe, o no se puede alcanzar y entonces se va a estado de espera hasta que recibe un ACK del origen. La solicitud de espera se coloca en una cola en la conexión o en un área de memoria de espera. Este estado de espera requiere el uso de recursos del sistema que se está atacando, tal como memoria, hasta que el temporizador de la conexión expira. Los hackers inundarán el host con falsos SYN para usar sus recursos en la conexión y no dejarlo contestar para poder legitimizar los requisitos de la conexión.

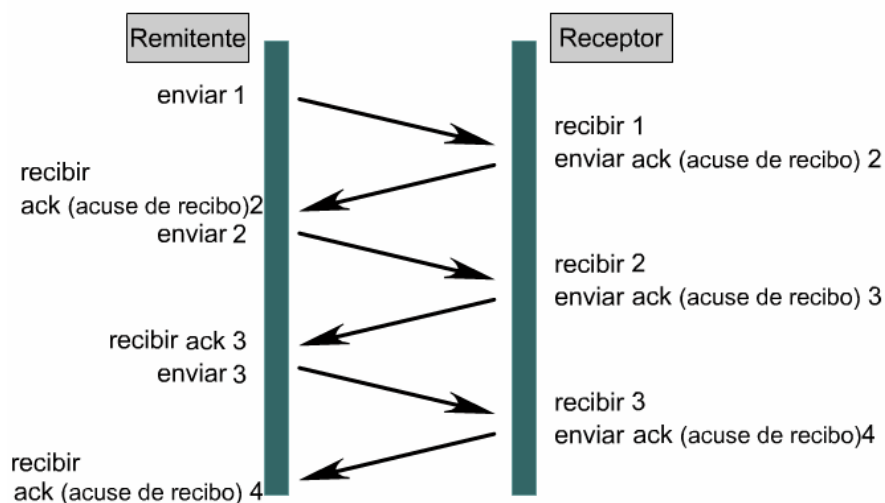
Para defenderse de estos ataques, los administradores del sistema pueden reducir el período de espera de desconexión y aumentar el tamaño de la cola de conexión. También existe software que puede detectar estos tipos de ataques e iniciar medidas de defensa.

10.1.4 Uso de ventanas y tamaño de las ventanas

A menudo, la cantidad de datos que se necesita transmitir es demasiado grande como para ser enviada en un solo segmento de datos. En este caso, los datos deben dividirse en porciones de menor tamaño para permitir su correcta transmisión. TCP tiene la responsabilidad de dividir los datos en segmentos. Esto se puede comparar con la forma en que son alimentados los niños pequeños. Su comida se corta en pedazos más pequeños que sus bocas pueden acomodar. Además, es posible que las máquinas receptoras no sean capaces de recibir datos con la rapidez que el origen los envía, tal vez, porque el dispositivo receptor está ocupado con otras tareas o porque el transmisor simplemente es un dispositivo más robusto.

Una vez segmentados los datos, deben transmitirse hacia el dispositivo destino. Uno de los servicios que provee TCP es el control de flujo que regula la cantidad de datos enviada durante un período de transmisión dado. Este proceso de control de flujo se conoce como uso de ventanas.

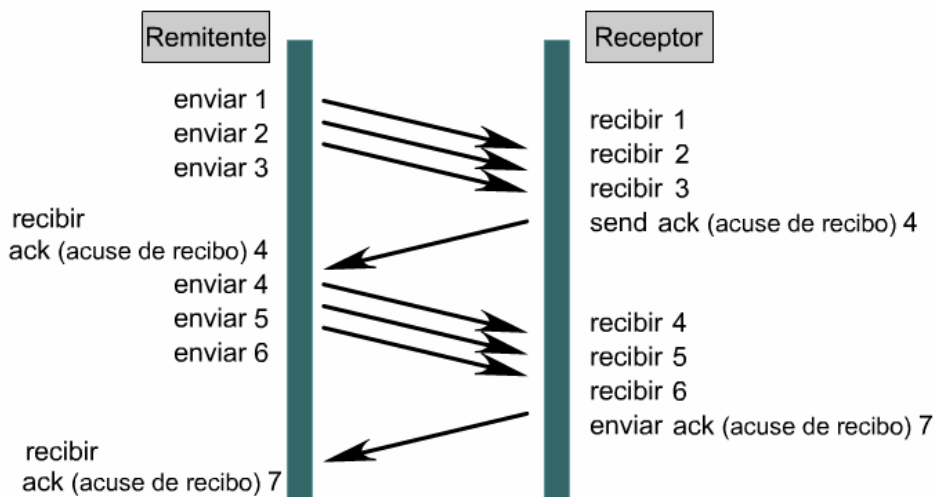
El tamaño de la ventana determina la cantidad de datos que se pueden transmitir simultáneamente antes que el destino responda con un Acuse de recibo (ACK). Después que un host transmite el tamaño de ventana en bytes, el host debe recibir un ACK indicando que la información se recibió antes de poder enviar más información. Por ejemplo, si la ventana es de 1, se debe generar un ACK por cada byte antes de enviar el siguiente ¹.



Esto se ha simplificado para el ejemplo. Las ventanas reales son de un tamaño mucho mayor, generalmente de miles de bytes

Figura 1

TCP usa las ventanas para determinar de forma dinámica el tamaño de la transmisión. Los dispositivos negocian el tamaño de la ventana a un número específico de bytes para transmitir antes del ACK ².



Esto se ha simplificado para el ejemplo. Las ventanas reales son de un tamaño mucho mayor, generalmente de miles de bytes

Figura 2

Este proceso de variación dinámica del tamaño de la ventana incrementa la confiabilidad. El tamaño de la ventana se puede basar en los ACKs.

10.1.5 Números de secuencia

TCP divide los datos en segmentos. Los segmentos de datos viajan entonces desde el transmisor hacia el receptor después del proceso de sincronización y la negociación del tamaño de ventana que dicta el número

de bytes que es posible transmitir por vez. Los segmentos de datos que se transmiten deben reensamblarse una vez recibidos. No hay garantía alguna de que los datos llegarán en el orden en que se transmitieron. TCP aplica los números de secuencia a los segmentos de datos que transmite de modo que el receptor pueda reensamblar adecuadamente los bytes en su orden original. Si los segmentos TCP llegan desordenados, los segmentos se pueden reensamblar de forma incorrecta. Los números de secuencia le indican al dispositivo destino cómo ordenar correctamente los bytes a medida que arriban.

Estos números de secuencia también actúan como números de referencia de modo que el receptor sabe si ha recibido todos los datos. También identifican las porciones de datos perdidos y así el transmisor puede retransmitir los datos faltantes. ¹Esto ofrece una mayor eficiencia ya que el transmisor sólo necesita retransmitir los segmentos faltantes en lugar de todo el grupo de datos.

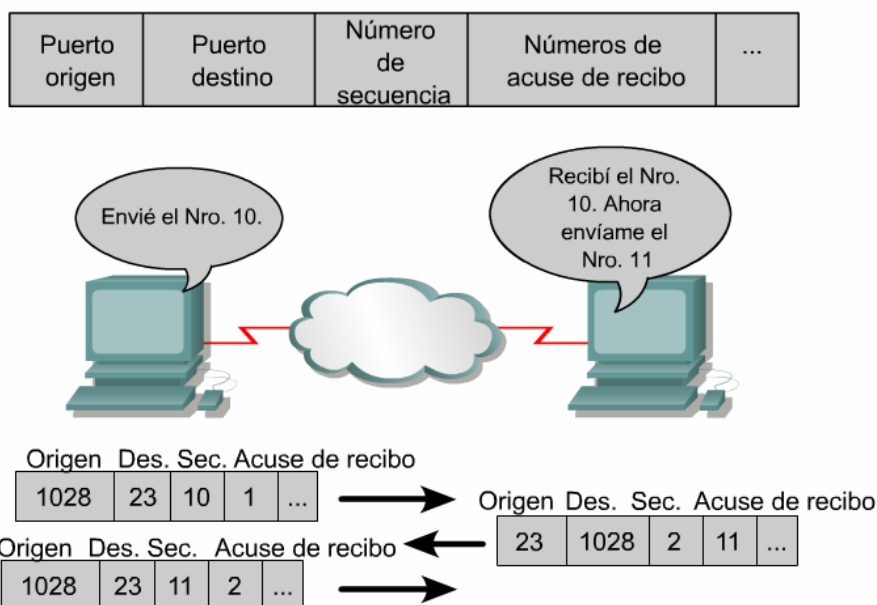


Figura 1

Cada segmento TCP se numera antes de su transmisión. ²Tenga en cuenta que después del puerto destino en el formato del segmento se encuentra la porción del número de secuencia. En la estación receptora, TCP usa los números de secuencia para reensamblar los segmentos hasta formar un mensaje completo. Si falta algún número de secuencia en la serie, ese segmento se vuelve a transmitir.

0	4	10	16	24	31
Puerto origen			Puerto destino		
Número de secuencia					
Número de acuse de recibo					
Hlen	Reservado	Bits de código	Ventana		
Checksum			Señalador urgente		
Opciones (de haberlas)				Relleno	
Datos					
...					

Figura 2

10.1.6 ACK positivo

El acuse de recibo es un paso frecuente del proceso de sincronización que incluye ventanas deslizantes y secuenciación de datos. En un segmento TCP, el campo número de secuencia está seguido por el campo número de acuse de recibo, también conocido como el campo código. ¹

0	4	10	16	24	31
Puerto origen			Puerto destino		
Número de secuencia					
Número de acuse de recibo					
Hlen	Reservado	Bits de código	Ventana		
checksum			Señalador urgente		
Opciones (de haberlas)				Relleno	
Datos					
...					

Figura 1

Uno de los problemas con el protocolo IP no confiable es que no cuenta con un método de verificación para determinar que los segmentos de datos realmente llegan a destino. Por lo tanto, los segmentos de datos pueden enviarse de forma constante sin saber si realmente se recibieron o no. TCP utiliza acuse de recibo positivo y retransmisión para controlar el flujo de datos y confirmar la entrega de los datos.

El acuse de recibo positivo y retransmisión (PAR) es una técnica frecuente que muchos protocolos utilizan para proporcionar confiabilidad. Con PAR, el origen envía un paquete, inicia un temporizador y espera un acuse de recibo antes de enviar el siguiente paquete. Si el temporizador expira antes de que el origen reciba un acuse de recibo, el origen retransmite el paquete y reinicia el temporizador. TCP utiliza acuses de recibo de expectativa, lo que significa que el número de acuse de recibo se refiere al siguiente octeto esperado.

El uso de ventanas es un mecanismo de control de flujo que requiere que el dispositivo origen reciba un acuse de recibo desde el destino después de transmitir una cantidad determinada de datos. Con un tamaño de ventana de tres, el dispositivo origen puede enviar tres octetos al destino. Entonces debe esperar un acuse de recibo. Si el destino recibe los tres octetos, envía un acuse de recibo al dispositivo origen, que ahora puede transmitir otros tres octetos. Si, por algún motivo, el destino no recibe los tres octetos, posiblemente debido a búferes cuya capacidad se ha excedido, no envía un acuse de recibo. Debido a que el origen no recibe un acuse de recibo, sabe que los octetos se deben retransmitir, y que la velocidad de transmisión debe reducirse. ²

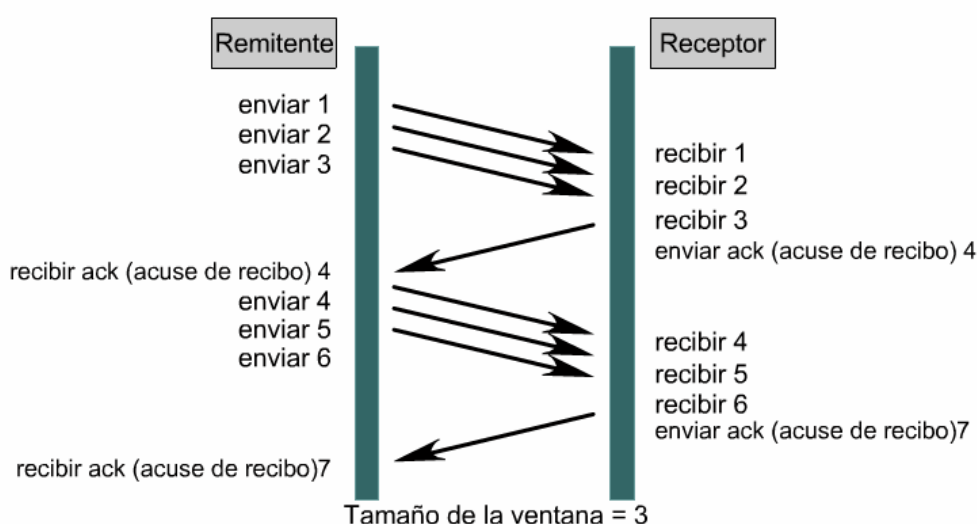


Figura 2

10.1.7 Operación de UDP

La pila del protocolo TCP/IP contiene muchos protocolos diferentes, cada uno diseñado para realizar una tarea determinada. IP provee transporte de Capa 3 no orientado a conexión a través de una internetwork. TCP permite la transmisión confiable, orientada a conexión de los paquetes en la Capa 4 del modelo OSI. UDP proporciona la transmisión de paquetes no orientado a conexión y no confiable de los paquetes en la Capa 4 del modelo OSI.

Tanto TCP como UDP utilizan IP como protocolo subyacente de Capa 3. Además, distintos protocolos de capa de aplicación utilizan TCP y UDP. TCP provee servicios para aplicaciones tales como FTP, HTTP, SMTP y DNS. UDP es el protocolo de capa de transporte utilizado por DNS, TFTP, SNMP y DHCP. ¹

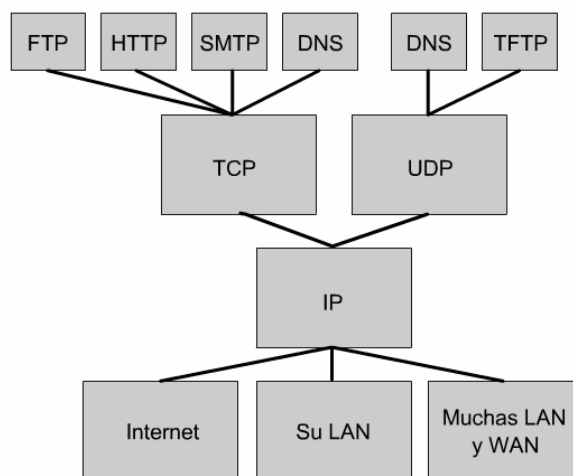


Figura 1

TCP debe utilizarse cuando las aplicaciones requieren la garantía de que un paquete llegue intacto, en secuencia y sin duplicar. El encabezado que se asocia con garantizar la entrega del paquete, a veces, se convierte en un problema al utilizar TCP. No todas las aplicaciones necesitan garantizar la entrega del paquete de datos, por lo tanto, utilizan un mecanismo de entrega no orientado a conexión, más rápido, que aporta el UDP. El estándar del protocolo UDP, que se describe en RFC 768, es un protocolo simple que intercambia segmentos sin acuses de recibo ni entrega garantizada.

UDP no hace uso de ventanas ni acuses de recibo de modo que los protocolos de capa de aplicación deben brindar la detección de errores. ²El campo Puerto de origen es un campo optativo que sólo se utiliza si la información debe regresar al host transmisor. Cuando un router destino recibe una actualización de enrutamiento, el router origen no solicita nada, de modo que nada debe regresar a la fuente. No existe intercambio de información o datos alguno. El campo Puerto destino especifica la aplicación a la que UDP necesita pasar el protocolo. Una petición DNS proveniente de un host hacia un servidor DNS suele tener un campo Puerto destino de 53, el número de puerto de UDP para DNS. El campo Longitud identifica el número de octetos de un segmento UDP. El checksum de UDP es optativo pero debería utilizarse para garantizar que no se han dañado los datos durante la transmisión. Para el transporte a través de la red, UDP se encapsula en el paquete IP.

Número de Bits	16	16	16	16	16
	Puerto origen	Puerto destino	Longitud	Checksum	Datos...

Figura 2

Una vez que el segmento UDP llega a la dirección IP destino, debe haber un mecanismo que permita que el host receptor determine la exacta aplicación en destino. Para este fin se utilizan los puertos destino. Si un host provee servicios de TFTP y DNS, debe ser capaz de determinar cuál es el servicio que necesitan los segmentos UDP que llegan. El campo del Puerto destino del encabezado UDP determina la aplicación hacia la que se enviará el segmento UDP.

10.2 Descripción general de los puertos de la capa de transporte

10.2.1 Múltiples conversaciones entre hosts

En un momento dado, miles de paquetes que proveen cientos de servicios distintos atraviesan una red moderna. En muchos casos, los servidores proveen una gran cantidad de servicios lo que causa problemas singulares para el direccionamiento de los paquetes. Si un servidor ofrece servicios SMTP y HTTP, utiliza el campo puerto destino para determinar cuál es el servicio que solicita el origen. El origen no puede construir un paquete destinado sólo a la dirección IP del servidor porque el destino no sabría cuál es el servicio que

se solicita. **1** Un número de puerto debe asociarse a la conversación entre hosts para garantizar que el paquete alcance el servicio adecuado en el servidor. Sin una forma de distinguir entre las distintas conversaciones, el cliente sería incapaz de enviar un mensaje electrónico y navegar una página web utilizando un servidor al mismo tiempo. Debe utilizarse un método para separar las conversaciones de la capa de transporte.

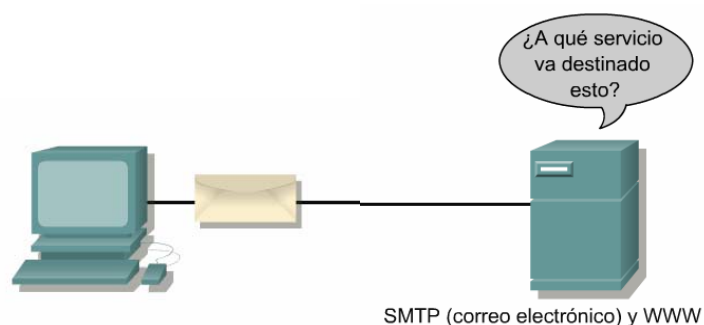


Figura 1

Los hosts que corren TCP/IP asocian los puertos de la capa de transporte con determinadas aplicaciones. Los números de puerto se usan para realizar el seguimiento de las distintas conversaciones que atraviesan la red al mismo tiempo. Los números de puerto son necesarios cuando un host se comunica con un servidor que provee múltiples servicios. Tanto TCP como UDP utilizan números de puerto o socket para enviar información a las capas superiores.

Los fabricantes de software de aplicación han acordado utilizar los números de puerto bien conocidos que se definen en la RFC1700. Toda conversación dirigida a la aplicación FTP utiliza el número de puerto estándar 21. **2** Las conversaciones que no involucran aplicaciones con números de puerto bien conocidos reciben números de puerto elegidos de forma aleatoria de un rango específico. Estos números de puerto se usan como direcciones origen y destino en el segmento TCP. **3**

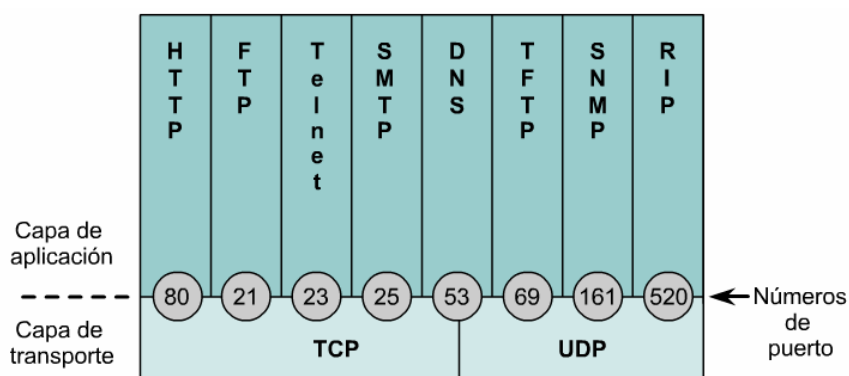


Figura 2

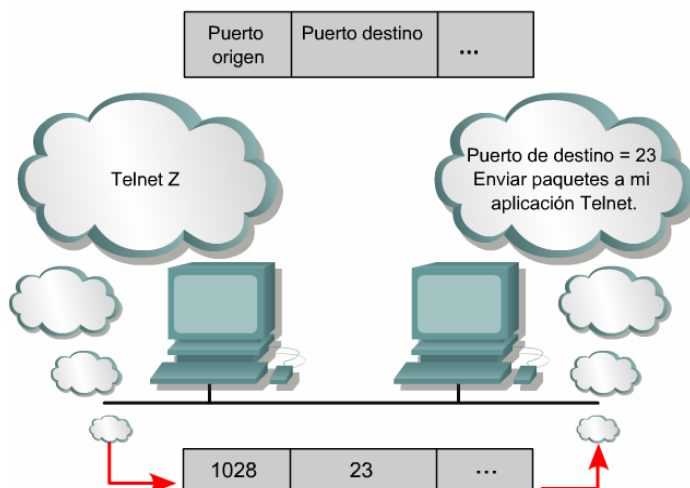


Figura 3

Los números de puerto tienen los siguientes intervalos asignados:

- Los puertos bien conocidos son aquellos desde 0 a 1.023.
- Los puertos registrados son aquellos desde 1.024 a 49.151.
- Los puertos dinámicos y/o privados son aquellos desde el 49.152 al 65.535.

Los sistemas que inician solicitudes de comunicación usan números de puerto para seleccionar las aplicaciones adecuadas. El host que origina la transferencia asigna dinámicamente los números del puerto de origen para estas solicitudes y, en general, son números mayores a 1023. Los números de puerto en el rango de 0 a 1023 se consideran números de puerto públicos y son controlados por la Autoridad de Asignación de Números de Internet (IANA, por sus siglas en inglés). Los números de las casillas de correo postal son una buena analogía de los números de puerto. Es posible enviar una carga postal a un código postal, ciudad y casilla de correo. El código postal y la ciudad dirigen la correspondencia hacia las instalaciones postales correctas mientras que la casilla de correo garantiza la entrega a la persona a quien va dirigida la carta. De igual forma, la dirección IP lleva al paquete hacia el servidor correcto, pero el número de puerto TCP o UDP garantiza que el paquete pase a la aplicación correspondiente.

10.2.2 Puertos para servicios

Los servicios que funcionan en los host deben contar con un número de puerto asignado para que la comunicación se produzca. Un host remoto que intenta conectarse con un servicio espera que el servicio utilice puertos y protocolos de capa de transporte específicos. Algunos puertos, definidos en la RFC 1700, se conocen como puertos bien conocidos y reservados tanto en TCP como UDP.

Estos puertos bien conocidos definen las aplicaciones que se ejecutan sobre los protocolos de la capa de transporte. Por ejemplo, un servidor que provee servicio FTP enviará las conexiones TCP que utilizan los puertos 20 y 21 provenientes de los clientes hacia su aplicación FTP. De esta forma, el servidor puede determinar con exactitud cuál es el servicio que solicita el cliente. TCP y UDP utilizan los números de puerto para determinar el servicio adecuado a las peticiones enviadas.

10.2.3 Puertos para los clientes

Cada vez que un cliente se conecta a un servicio de un servidor, es necesario especificar el puerto de origen y destino. Los segmentos de TCP y UDP contienen campos para los puertos de origen y destino. ¹
² Los puertos destino o los puertos para servicios, generalmente, se definen utilizando los puertos conocidos. Los puertos de origen configurados por el cliente se determinan de forma dinámica.

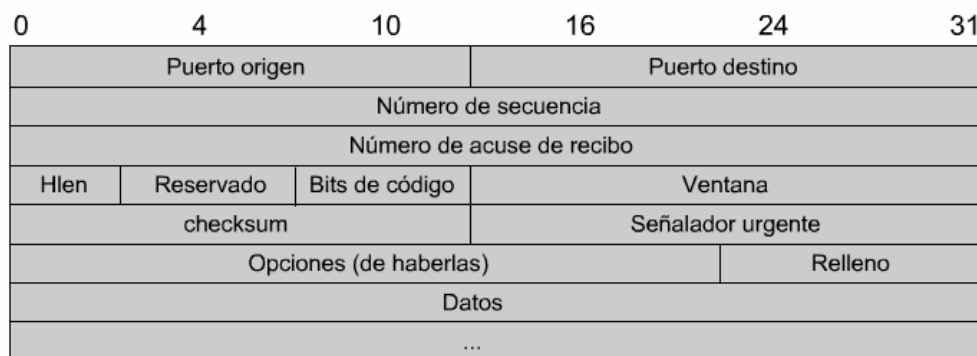


Figura 1

Número de Bits	16	16	16	16	16
	Puerto origen	Puerto destino	Longitud	Checksum	Datos...

Figura 2

En general, un cliente determina el puerto de origen asignando un número mayor a 1023 de forma aleatoria. Por ejemplo, un cliente que intenta comunicarse con un servidor web utiliza TCP y asigna el puerto destino con el número 80 y el puerto origen con 1045. Cuando el paquete llega al servidor, pasa hacia la capa de transporte superior y eventualmente al servicio HTTP que opera en el puerto 80. El servidor HTTP responde a las peticiones del cliente con un segmento que utiliza el puerto 80 como origen y 1045 como destino. De

esta manera, los clientes y servidores utilizan los puertos para diferenciar el proceso al que se asocia el segmento.

10.2.4 Numeración de los puertos y números de puerto conocidos

Los números de puerto se representan con 2 bytes en el encabezado del segmento TCP o UDP. Este valor de 16 bits puede hacer que los números de puerto varíen de 0 a 65535. Estos números de puerto se dividen en tres categorías diferentes: puertos bien conocidos, puertos registrados y puertos dinámicos o privados. Los primeros 1023 puertos son puertos bien conocidos. Como su nombre indica, estos puertos se utilizan para los servicios de red bien conocidos, por ejemplo; FTP, Telnet, o DNS. Los puertos registrados varían de 1024 a 49151. Los puertos entre 49152 y 65535 se conocen como puertos dinámicos o privados.

10.2.5 Ejemplo de múltiples sesiones entre hosts

Se usan números de puerto para rastrear múltiples sesiones que pueden ocurrir entre hosts. Los números de puerto de origen y destino se combinan con la dirección de red para formar un socket. Un par de sockets, uno en cada host, forman una única conexión. Por ejemplo, un host puede tener una conexión telnet, puerto 23 mientras que, al mismo tiempo, puede navegar la red, puerto 80. Las direcciones IP y MAC son las mismas porque los paquetes provienen del mismo host. Por lo tanto, cada conversación en el extremo origen necesita su propio número de puerto y cada servicio solicitado necesita de su propio número de puerto.

10.2.6 Comparación de direcciones MAC, direcciones IP y números de puerto

Estos tres métodos de direccionamiento resultan a menudo confusos, pero es posible evitar la confusión si se explican las direcciones haciendo referencia al modelo OSI. Los números de puerto se encuentran en la capa de transporte y la capa de red les brinda servicio. La capa de red asigna una dirección lógica (dirección IP) y recibe servicios de la capa de enlace de datos quien le asigna una dirección física (dirección MAC).

Una clara analogía podría ser la de una carta normal. La dirección de la carta consta de nombre, calle, ciudad y estado. Estos pueden compararse con el puerto, la dirección MAC y la dirección IP que se utilizan para los datos de red. El nombre en el sobre equivale al número de puerto, la calle es la dirección MAC, y la ciudad y estado son la dirección IP. Es posible enviar varias cartas a la misma calle, ciudad y estado pero incluye distintos nombres. Por ejemplo, se podrían enviar dos cartas a la misma casa, una dirigida a John Doe y la otra a Jane Doe. Esto es análogo a múltiples sesiones con diferentes números de puerto.

Resumen

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

- Descripción de la operación de TCP.
- Proceso de sincronización (intercambio de señales de tres vías).
- Ataques de servicio denegado
- Uso de ventanas y tamaño de las ventanas
- Números de secuencia
- ACK positivo
- Operación de UDP
- Múltiples conversaciones entre hosts
- Puertos para servicios
- Puertos para los clientes
- Numeración de los puertos y números de puertos conocidos
- Ejemplo de múltiples sesiones entre hosts
- Comparación de direcciones MAC, direcciones IP y números de puertos.

Módulo 11: Listas de control de acceso (ACL)

Descripción general

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos. Aunque las herramientas de seguridad, como por ejemplo: las contraseñas, equipos de callback y dispositivos de seguridad física, son de ayuda, a menudo carecen de la flexibilidad del filtrado básico de tráfico y de los controles específicos que la mayoría de los administradores prefieren. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero impedir a los usuarios externos el acceso telnet a la LAN.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior. Este módulo introduce las ACL estándar y extendidas como medio de control del tráfico de red y explica de qué manera se utilizan las ACL como parte de una solución de seguridad.

Además, este capítulo incluye consejos, consideraciones, recomendaciones y pautas generales acerca del uso de las ACL e incluye los comandos y configuraciones necesarias para crear las ACL. Finalmente, brinda ejemplos de ACL estándar y extendidas y su aplicación en las interfaces del router.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers. Aunque muchos de los usos avanzados de las ACL exceden el alcance de este curso, este módulo ofrece detalles sobre las ACL estándar y extendida, su ubicación adecuada y algunas de las aplicaciones especiales de las mismas.

Los estudiantes que completen este módulo deberán ser capaces de:

- Describir las diferencias entre las ACL estándar y extendida.
- Explicar las reglas para establecer las ACL.
- Crear y aplicar las ACL nombradas.
- Describir las funciones de los firewalls.
- Utilizar las ACL para restringir el acceso a la terminal virtual.

11.1 Aspectos fundamentales de las listas de control de acceso

11.1.1 ¿Qué son las ACL?

Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. ¹ Estas listas le informan al router qué tipo de paquetes aceptar o rechazar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas. Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red.

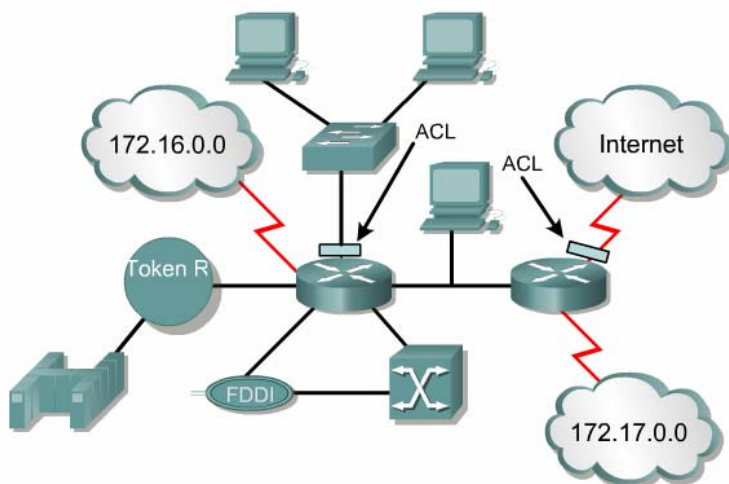


Figura 1

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. ²El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

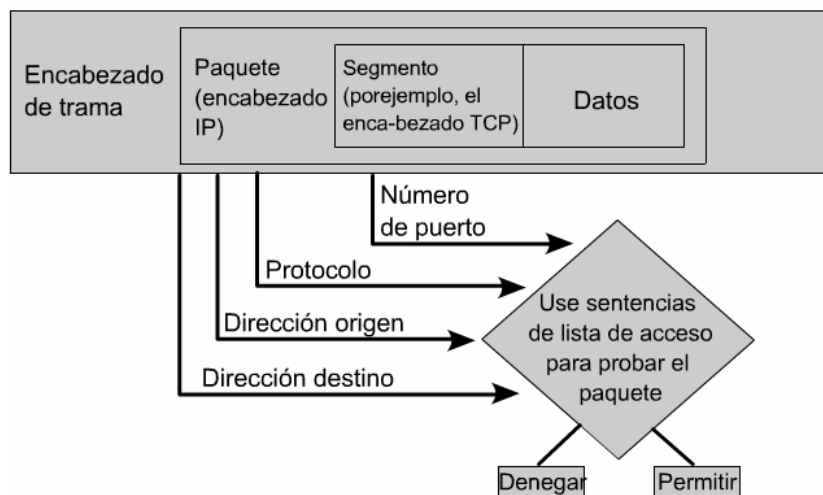


Figura 2

Las ACL se definen según el protocolo, la dirección o el puerto. ³Para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz. Las ACL controlan el tráfico en una dirección por vez, en una interfaz. Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente. Finalmente, cada interfaz puede contar con varios protocolos y direcciones definidas. Si el router tiene dos interfaces configuradas para IP, AppleTalk e IPX, se necesitan 12 ACLs separadas. Una ACL por cada protocolo, multiplicada por dos por dirección entrante y saliente, multiplicada por dos por el número de puertos.

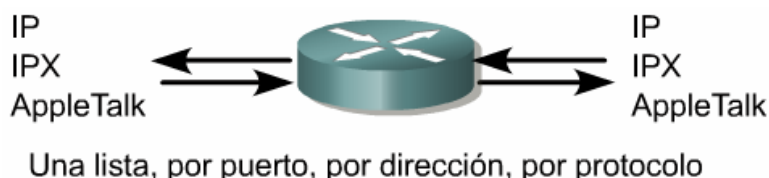


Figura 3

Estas son las razones principales para crear las ACL:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red. Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

Si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

11.1.2 Funcionamiento de las ACL

Una lista ACL es un grupo de sentencias que definen si se aceptan o rechazan los paquetes en interfaces entrantes o salientes. ¹Estas decisiones se toman haciendo coincidir una sentencia de condición en una lista de acceso y luego realizando la acción de aceptación o rechazo definida en la sentencia.

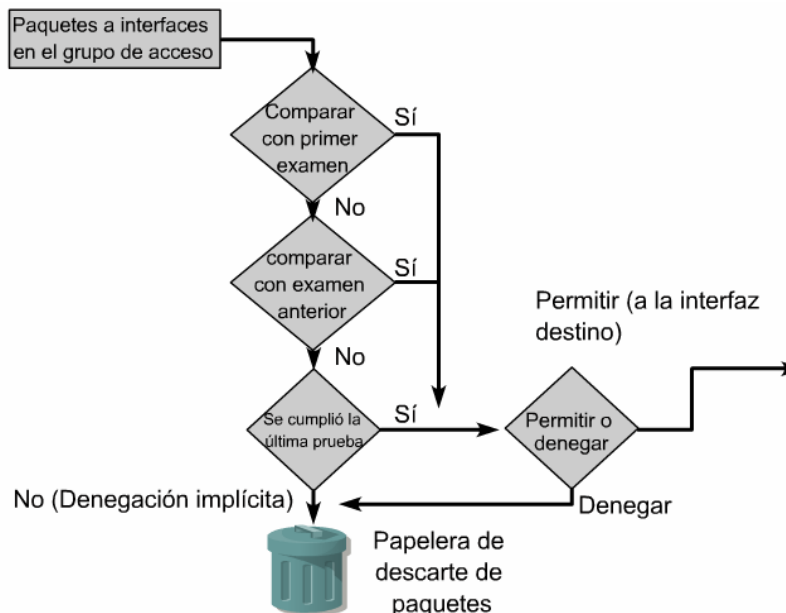


Figura 1

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición. ²Para que el proceso de revisión de una ACL sea más simple, es una buena idea utilizar un editor de textos como el Bloc de notas y pegar la ACL a la configuración del router.

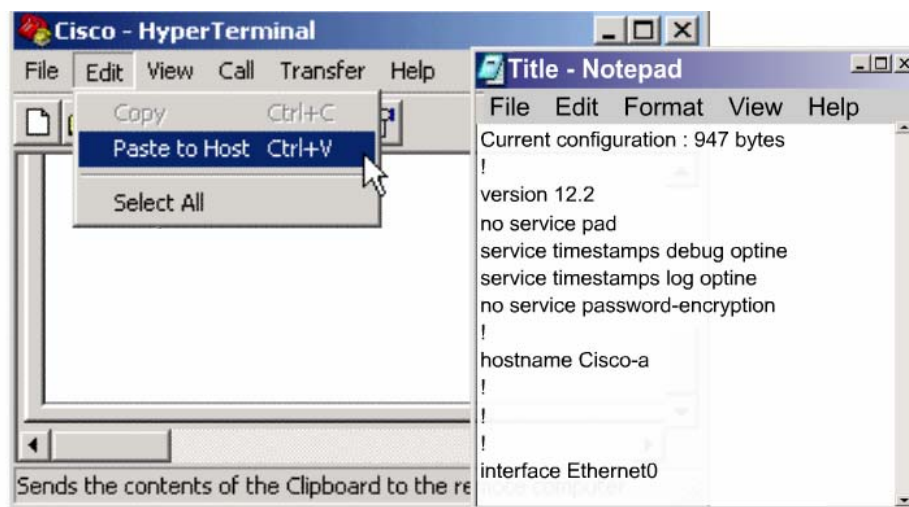


Figura 2

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. A medida que una trama ingresa a una interfaz, el router verifica si la dirección de Capa 2 concuerda o si es una trama de broadcast. Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante. Si existe una ACL, entonces se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete cumple las condiciones, se lleva a cabo la acción de aceptar o rechazar el paquete. Si se acepta el paquete en la interfaz, se lo compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. A continuación, el router verifica si la interfaz destino tiene una ACL. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se lleva a cabo la aceptación o el rechazo del paquete. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de Capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea **deny any** no sea visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el **deny any** al final de las ACL para reforzar la presencia dinámica de la prohibición implícita deny.

11.1.3 Creación de las ACL

Las ACL se crean en el modo de configuración global. ¹Existen varias clases diferentes de ACLs: estándar, extendidas, IPX, AppleTalk, entre otras. Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista. ²

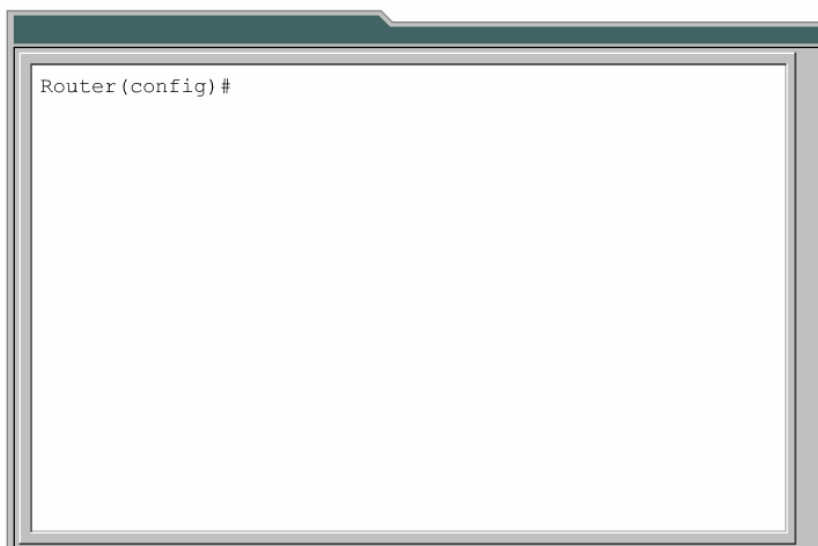


Figura 1

Protocolo	Intervalo
IP	1-99, 1300-1999
IP extendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

Figura 2

Después de ingresar al modo de comando apropiado y que se decide el número de tipo de lista, el usuario ingresa sentencias de lista de acceso utilizando el comando **access-list**, seguida de los parámetros necesarios. ³Estando en el modo de comandos adecuado y definido el tipo de número de lista, el usuario

tipea las condiciones usando el comando **access-list** seguido de los parámetros apropiados. Este es el primero de un proceso de dos pasos. El segundo paso consiste en asignar la lista a la interfaz apropiada.

Paso 1	Definir la ACL con el siguiente comando: <pre>Router(config)#access-list <i>access-list-number</i> {permit deny} {<i>test-conditions</i>}</pre> Una sentencia global identifica la ACL. Específicamente, el intervalo 1-99 se reserva para IP estándar. Este número se refiere al tipo de ACL. En la versión 11.2 o posterior de Cisco IOS, las ACL también pueden usar un nombre ACL, como educación_grupo, en lugar de un número El término permit o deny (permitir o denegar) de la sentencia ACL global indica cuántos paquetes que cumplan con las condiciones de prueba maneja el software Cisco IOS. Permit generalmente significa que el paquete puede usar una o más interfaces que se especifican posteriormente. El (Los) último(s) término(s) especifican las condiciones de prueba que utiliza la sentencia ACL.
Paso 2	A continuación, es necesario aplicar las ACL en una interfaz mediante el comando access-group, como se muestra en el ejemplo. <pre>Router(config-if)#{<i>protocol</i>} access-group <i>access-list-number</i></pre> Todas las sentencias ACL identificadas con access-list-number están relacionadas con una o más interfaces. Cualquier paquete que pase las condiciones de prueba de la ACL tiene permiso de usar cualquier interfaz en el grupo de acceso de las interfaces.

Figura 3

En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando **ip access-group** en el modo de configuración de interfaz. ⁴Al asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Es posible establecer la dirección del filtro para verificar los paquetes que viajan hacia dentro o fuera de una interfaz. Para determinar si la ACL controla el tráfico entrante o saliente, el administrador de red necesita mirar las interfaces como si se observara desde dentro del router. Este es un concepto muy importante. Una lista de acceso entrante filtra el tráfico que entra por una interfaz y la lista de acceso saliente filtra el tráfico que sale por una interfaz. Después de crear una ACL numerada, se la debe asignar a una interfaz. Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando **no access-list list-number** y entonces proceder a recrearla. ⁵

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Figura 4

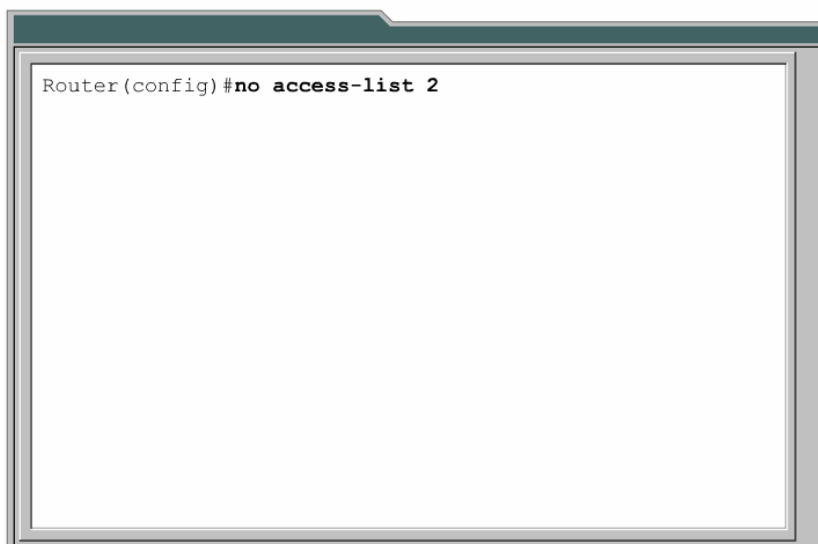


Figura 5

Es necesario utilizar estas reglas básicas a la hora de crear y aplicar las listas de acceso.

- Una lista de acceso por protocolo y por dirección.
- Se deben aplicar las listas de acceso estándar que se encuentran lo más cerca posible del destino.
- Se deben aplicar las listas de acceso extendidas que se encuentran lo más cerca posible del origen.
- Utilice la referencia de la interfaz entrante y saliente como si estuviera mirando el puerto desde adentro del router.
- Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
- Hay un **deny any** (denegar cualquiera) implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.
- Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específico y por último los grupos o filtros generales.
- Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
- Nunca trabaje con una lista de acceso que se utiliza de forma activa.
- Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
- Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando **no access-listx** elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.
- Una lista de acceso IP envía un mensaje ICMP llamado de host fuera de alcance al emisor del paquete rechazado y descarta el paquete en la papelera de bits.
- Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una deny any (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
- Los filtros salientes no afectan al tráfico que se origina en el router local.

11.1.4 Función de la máscara wildcard

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar cómo tratar los bits de la dirección IP correspondientes. El término máscara wildcard es la denominación aplicada al proceso de comparación de bits de máscara y proviene de una analogía con el "wildcard" (comodín) que equivale a cualquier otro naipe en un juego de póquer. Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas. Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP. Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

Durante el proceso de máscara wildcard, la dirección IP en la sentencia de la lista de acceso tiene la máscara wildcard aplicada a ella. Esto crea el valor de concordancia, que se utiliza para comparar y verificar si esta sentencia ACL debe procesar un paquete o enviarlo a la próxima sentencia para que se lo verifique. La segunda parte del proceso de ACL consiste en que toda dirección IP que una sentencia ACL en particular verifica, tiene la máscara wildcard de esa sentencia aplicada a ella. El resultado de la dirección IP y de la máscara debe ser igual al valor de concordancia de la ACL.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

Se puede escribir como:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Se puede escribir como:
Router(config)#access-list 1 permit host 172.30.16.29
```

Figura 1

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones **any** y **host**. ¹Para explicarlo de forma sencilla, la opción **any** reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción **host**. Esta máscara necesita todos los bits de la dirección ACL y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

11.1.5 Verificación de las ACL

Existen varios comandos **show** que verifican el contenido y ubicación de las ACL en el router.

El comando **show ip interface** muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando **show access-lists** muestra el contenido de todas las ACL en el router. ¹Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando **show running-config** también revela las listas de acceso en el router y la información de asignación de interfaz.

```
Router#show access-lists
Standard IP access list 2
deny 172.16.1.1
permit 172.16.1.0, wildcard bits 0.0.0.255
deny 172.16.0.0, wildcard bits 0.0.255.255
permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
permit tcp 192.168.6.0 0.0.0.255 any eq telnet
permit tcp 192.168.6.0 0.0.0.255 any eq ftp
permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Figura 1

Estos comandos **show** verifican los contenidos y ubicación de las listas. También se recomienda verificar las listas de acceso usando tráfico de ejemplo para asegurarse que la lógica de la lista de acceso sea correcta.

11.2 Listas de control de acceso (ACL)

11.2.1 ACL estándar

Las ACL estándar verifican la dirección origen de los paquetes IP que se deben enrutar. Con la comparación se permite o rechaza el acceso a todo un conjunto de protocolos, según las direcciones de red, subred y host. Por ejemplo, se verifican los paquetes que vienen en Fa0/0 para establecer la dirección origen y el protocolo. Si se les otorga el permiso, los paquetes se enrutan a través del router hacia una interfaz de salida. Si se les niega el permiso, se los descarta en la interfaz entrante.

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACLs estándar pudiendo así proveer un máximo posible de 798 ACLs estándar adicionales, a las cuales se les conoce como ACLs IP expandidas. (también entre 1300 y 1999 en IOS recientes) ¹En la primera sentencia ACL, cabe notar que no hay máscara wildcard. En este caso donde no se ve ninguna lista, se utiliza la máscara por defecto, que es la 0.0.0.0. Esto significa que toda la dirección debe concordar o que esta línea en la ACL no aplica y el router debe buscar una concordancia en la línea siguiente de la ACL.

```
access-list 2 deny 172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny 172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
```

- Intervalo de números de lista de acceso de 1-99 y 1300-1999
- Filtrar solamente en la dirección IP origen
- Máscaras wildcard
- Aplicado al puerto más cercano al destino

Figura 1

La sintaxis completa del comando ACL estándar es:

Router(config)#**access-list***access-list-number* {deny | permit | remark} source [*source-wildcard*] [**log**]

El uso de **remark** facilita el entendimiento de la lista de acceso. Cada **remark** está limitado a 100 caracteres. Por ejemplo, no es suficientemente claro cual es el propósito del siguiente comando: **access-list 1 permit 171.69.2.88**. Es mucho mas fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

access-list 1 remark Permit only Jones workstation through

access-list 1 permit 171.69.2.88

La forma no de este comando se utiliza para eliminar una ACL estándar. Ésta es la sintaxis:

Router(config)#**no access-list***access-list-number*

El comando **ip access-group** relaciona una ACL existente a una interface:

Router(config)#**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

La tabla muestra descripciones de los parámetros utilizados en esta sintaxis. ²

Parámetro	Descripción
<i>access-list-number</i>	Número de una ACL, el cual es un decimal de 1 a 99 (para ACLs IP estándar) y de 1300 a 1999 (para ACLs expandidas)
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Agrega un comentario acerca de las entradas de una lista de acceso IP para hacer que la lista sea más fácil de entender y recorrer.
<i>source</i>	Número de la red o del host desde el que se envía un paquete. Hay dos formas de especificar el origen: • Usar una cantidad de 32 bits en un formato de cuatro partes, decimal separado con puntos. • Usar la palabra clave any como una abreviatura del origen y source-wildcard de la 0.0.0.0 255.255.255.55
<i>source-wildcard</i>	(Opcional) Los bits wildcard para aplicar al origen. Hay dos formas de especificar el wildcard origen: • Utilizar una cantidad de 32 bits en un formato de cuatro partes, decimal separado con puntos. Coloca unos en las posiciones de bit que desea ignorar. • Usar la palabra clave any como una abreviatura del origen y source-wildcard de la 0.0.0.0 255.255.255.55
log	(Opcional) Genera un mensaje de registro informativo en la consola acerca del paquete que concuerda con la entrada. (La cantidad de los mensajes generados en la consola se controla con el comando <code>logging console</code>). El mensaje incluye el número ACL, si el paquete fue permitido o denegado, la dirección origen y la cantidad de paquetes. El mensaje se genera para el primer paquete que concuerda, y luego a intervalos de cinco minutos, incluyendo la cantidad de paquetes permitidos o denegados en el intervalo de cinco minutos anterior.

Figura 2

11.2.2 ACL extendidas

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar porque ofrecen un mayor control. Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mayor flexibilidad para establecer qué verifica la ACL. Se puede permitir o rechazar el acceso de los paquetes según el lugar donde se originó el paquete y su destino así como el tipo de protocolo y direcciones de puerto. Una ACL extendida puede permitir el tráfico de correo electrónico de Fa0/0 a destinos específicos S0/0, al mismo tiempo que deniega la transferencia de archivos y la navegación en la red. Una vez descartados los paquetes, algunos protocolos devuelven un paquete al emisor, indicando que el destino era inalcanzable.

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Rango de números de listas de acceso de 100 a 199 y de 2000 a 2699
- Dirección IP de origen y de destino
- Número de protocolo de Capa 4
- Aplicado al puerto más cercano al host origen

Figura 1

Es posible configurar múltiples sentencias en una sola ACL. ¹Cada una de estas sentencias debe tener el mismo número de lista de acceso, para poder relacionar las sentencias con la misma ACL. Puede haber tanta cantidad de sentencias de condición como sean necesarias, siendo la única limitación la memoria

disponible en el router. Por cierto, cuantas más sentencias se establezcan, mayor será la dificultad para comprender y administrar la ACL.

La sintaxis de una sentencia ACL extendida puede ser muy extensa y a menudo, se vuelve engorrosa en la ventana terminal. Las wildcards también tienen la opción de utilizar las palabras clave **host** o **any** en el comando. ²

```
access-list access-list-number [dynamic dynamic-name [timeout
minutes]] {deny | permit | remark} protocol source source-
wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log | log-input] [time-range time-
range-name] icmp-type icmp-code icmp-message igmp-type
[operator operand] [port port number or name] [established]
[fragments]
```

Figura 2

Al final de la sentencia de la ACL extendida, se obtiene más precisión con un campo que especifica el Protocolo para el control de la transmisión (TCP) o el número de puerto del Protocolo de datagrama del usuario (UDP). Las operaciones lógicas pueden especificarse como igual (eq), desigual (neq), mayor a (gt) y menor a (lt) aquellas que efectuarán las ACL extendidas en protocolos específicos. Las ACL extendidas utilizan el número de lista de acceso entre 100 y 199 (también entre 2000 y 2699 en IOS recientes).



Una lista, por puerto, por dirección, por protocolo

Figura 3

El comando **ip access-group** enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permite una ACL por interfaz por protocolo por dirección ³. El formato del comando es:

Router(config-if)#**ip access-group** access-list-number {in | out}

11.2.3 ACL nombradas

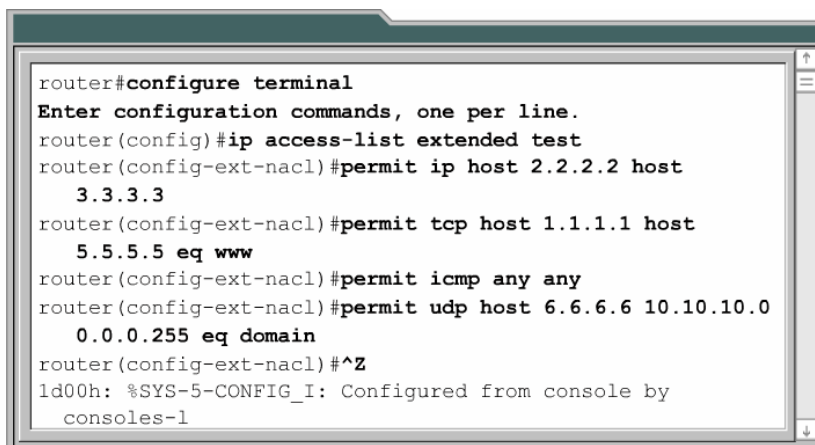
```
Rt1(config-ext-nacl)#remark (ACL para permitir acceso al correo y al servidor
DNS)
Rt1(config-ext-nacl)#permit tcp any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit udp any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#exit

Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

Figura 1

Las ACL nombradas IP se introdujeron en el software Cisco IOS Versión 11.2, permitiendo que las ACL extendidas y estándar tuvieran nombres en lugar de números. ¹ Las ventajas que ofrece una lista de acceso nombrada son las siguientes:

- Identifica intuitivamente las ACL usando un nombre alfanumérico.
- El IOS no limita el número de las ACL nombradas que se pueden configurar.
- Las ACL nombradas tienen la capacidad de modificar las ACL sin tener que eliminarlas y luego reconfigurarlas. Cabe notar que las listas de acceso nombradas permiten eliminar sentencias pero sólo permiten que las sentencias se agreguen al final de la lista. Aún con las ACL nombradas, se recomienda utilizar un editor de textos para crearlas. ²



```
router#configure terminal
Enter configuration commands, one per line.
router(config)#ip access-list extended test
router(config-ext-nacl)#permit ip host 2.2.2.2 host
3.3.3.3
router(config-ext-nacl)#permit tcp host 1.1.1.1 host
5.5.5.5 eq www
router(config-ext-nacl)#permit icmp any any
router(config-ext-nacl)#permit udp host 6.6.6.6 10.10.10.0
0.0.0.255 eq domain
router(config-ext-nacl)#^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by
consoles-1
```

Figura 2

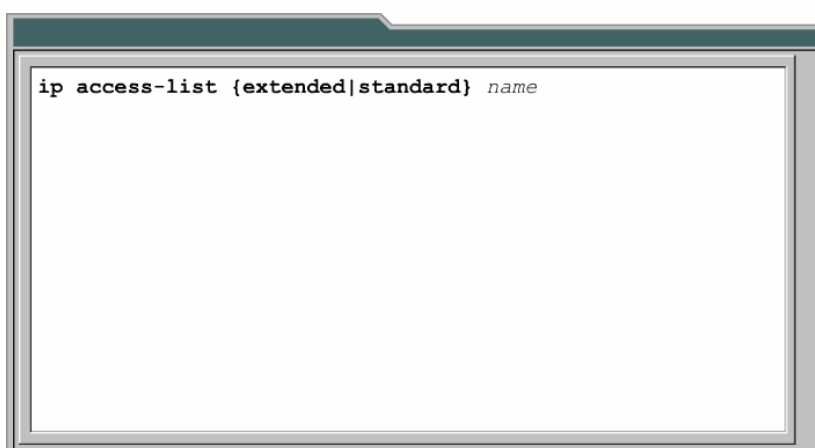
Tenga en cuenta lo siguiente antes de implementar las ACL nombradas:

Las ACL nombradas no son compatibles con las versiones de Cisco IOS anteriores a la versión 11.2.

No se puede utilizar el mismo nombre para varias ACL. Por ejemplo, no se permite da el nombre de George a ACL estándar y extendida.

Es importante conocer las listas de acceso nombradas debido a las ventajas antes mencionadas. Las operaciones de la lista de acceso avanzadas como las ACL nombradas se verán en el currículum CCNP.

Una ACL nombrada se crea con el comando **ip access-list**. ³ Esto coloca al usuario en el modo de configuración de ACL. En el modo de configuración de ACL, especifique una o más condiciones que se permitan o rechacen. ⁴ Esto determina si el paquete se envía o se descarta cuando hay concordancia con las sentencias de la ACL.



```
ip access-list {extended|standard} name
```

Figura 3

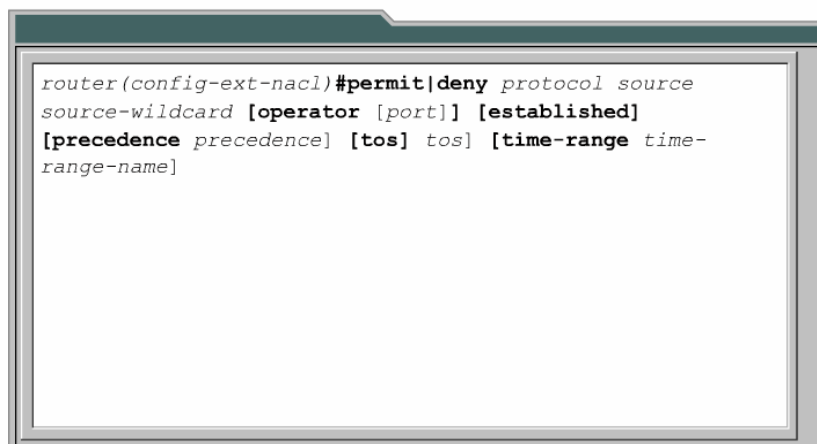


Figura 4

La configuración vista crea una ACL estándar llamada filtro de Internet y una ACL extendida llamada “grupo de marketing”. Esta figura 5 también muestra como las listas de acceso nombradas se aplican a una interfaz.

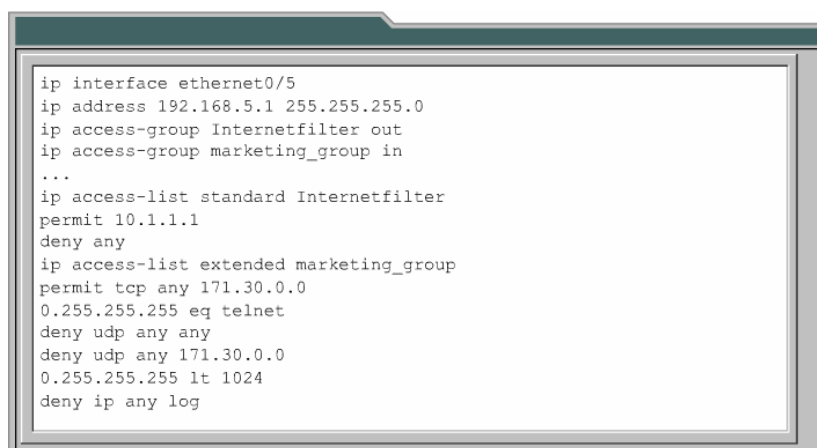


Figura 5

11.2.4 Ubicación de las ACL

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es dónde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente. Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

En la figura 1 el administrador quiere denegar el tráfico telnet o FTP del segmento LAN Ethernet del Router A al segmento LAN Ethernet conmutado Fa0/1 en el Router D, y al mismo tiempo permitir otros tipos de tráfico. Hay varias maneras de cumplir con esta política. La recomendación es utilizar ACL extendida, especificando las direcciones origen y destino. Se coloca esta ACL extendida en el Router A. Entonces los paquetes no atraviesan la Ethernet del Router A, no atraviesan las interfaces seriales de los Routers B y C, y no entran al Router D. El tráfico con direcciones de origen y destino diferentes todavía puede permitirse.

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

Un administrador solo puede colocar una lista de acceso en el dispositivo que controla. De este modo, la ubicación de la lista de acceso se determina según hasta dónde se extienda el control del administrador de la red.

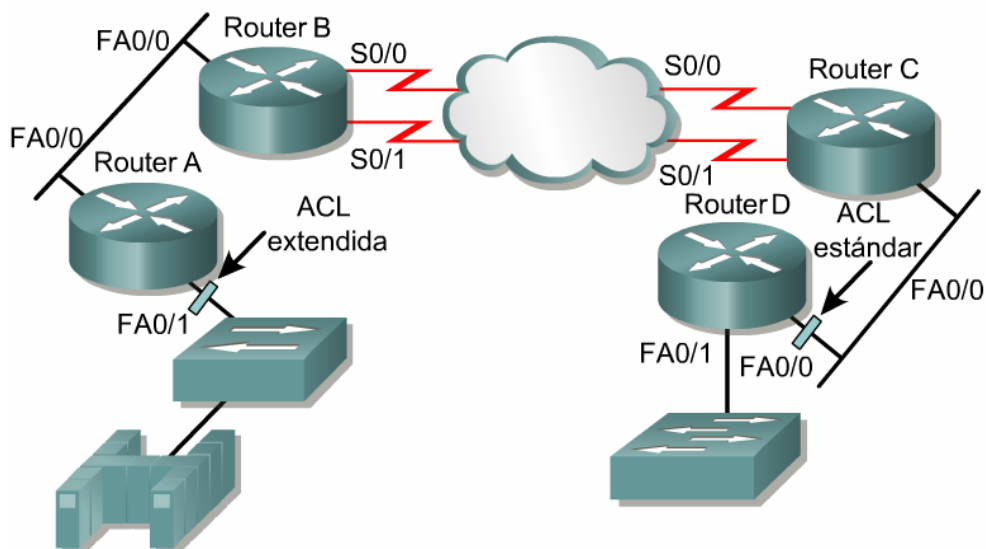
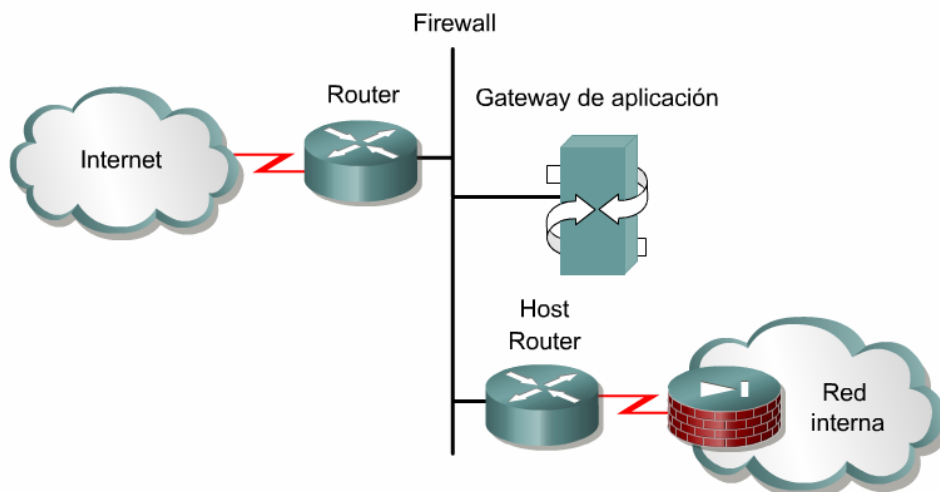


Figura 1

11.2.5 Firewalls

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.



En esta arquitectura, el router conectado a Internet, es decir el router exterior, obliga todo el tráfico entrante a pasar por el gateway de la aplicación. El router conectado a la red interna, es decir el router interior, acepta los paquetes provenientes sólo del gateway de aplicación. En efecto, el gateway controla la entrega de servicios basados en red que entran y salen de la red interna. Por ejemplo, sólo ciertos usuarios pueden estar autorizados a comunicarse con Internet o sólo a ciertas aplicaciones se les puede permitir establecer conexiones entre un host interior y exterior. Si la única aplicación que se permite es el correo electrónico, entonces sólo se permiten paquetes de correo electrónico a través del router. Esto protege el gateway de aplicación y evita que se supere su capacidad con paquetes que de otra manera se descartarían.

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna. El router firewall proporciona un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Se necesita configurar las ACL en routers fronterizos, que son aquellos situados en las fronteras de la red, para brindar mayor seguridad. Esto proporciona protección básica contra la red externa u otra parte menos controlada de la red, en un área más privada de la red. En estos routers fronterizos, es posible crear ACLs para cada protocolo de red configurado en las interfaces del router.

11.2.6 Cómo restringir el acceso de terminal virtual

Las listas de acceso extendidas y estándar se aplican a paquetes que viajan a través de un router. ¹No están diseñadas para bloquear paquetes que se originan dentro del router. Una lista de acceso extendida Telnet saliente, por defecto no impide las sesiones Telnet iniciadas por el router.

Del mismo modo que hay puertos físicos o interfaces, como Fa0/0 y S0/0 en el router, también hay puertos virtuales. Estos puertos virtuales se denominan líneas VTY. Existen cinco líneas vty, numeradas del 0 al 4, como se observa en la figura ¹. Por razones de seguridad, es posible negar o permitir, a los usuarios, el acceso a la terminal virtual del router, pero se les puede negar el acceso a destinos desde dicho router.

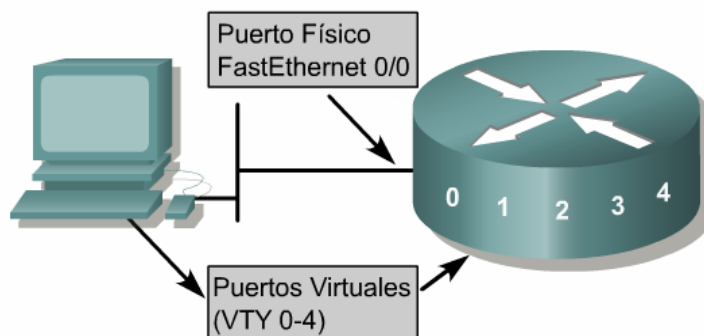


Figura 1

El objetivo de restringir el acceso vty es aumentar la seguridad de la red. También se logra el acceso a vty utilizando el protocolo Telnet para realizar una conexión no física con el router. Como resultado, hay solo un tipo de lista de acceso vty. Es necesario imponer idénticas restricciones a todas las líneas vty, ya que no es posible controlar a qué línea se conectará el usuario.

El proceso de creación de una lista de acceso vty es igual al descrito para una interfaz. Sin embargo, para aplicar la ACL a una línea terminal se necesita el comando **access-class** en vez del **access-group**. ²

```
Cisco - Hyperterminal

Creating the standard list:

Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Rt1(config)#access-list 2 permit 172.16.2.0 0.0.0.255
Rt1(config)#access-list 2 deny any

Applying the access list:

Rt1(config)#line vty 0 4
Rt1(config-line)#login
Rt1(config-line)#password secret
Rt1(config-line)#access-class 2 in
```

Figura 2

Cuando configure las listas de acceso en las líneas vty tenga en consideración lo siguiente:

- Cuando controle el acceso a una interfaz, es posible utilizar un número o un nombre.
- Sólo se pueden aplicar listas de acceso numeradas a las líneas virtuales.
- Imponga restricciones idénticas a todas las líneas de terminal virtual, porque el usuario puede querer conectarse a cualquiera de ellas.

Resumen

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

- Las ACL desempeñan varias funciones en un router, entre ellas la implementación de procedimientos de seguridad/acceso.
- Las ACL se utilizan para controlar y administrar el tráfico.
- En algunos protocolos, es posible aplicar dos ACL a una interfaz: una ACL entrante y una saliente.
- Mediante el uso de las ACL, una vez que un paquete ha sido asociado a una sentencia ACL, se le puede denegar o permitir el acceso al router.
- Los bits de máscara wildcard usan el número uno (1) y el número cero (0) para identificar la manera de tratar los bits de dirección IP correspondientes.
- Verificación de la creación y aplicación de las listas de acceso a través del uso de varios comandos show de IOS.
- Los dos tipos principales de ACL son: estándar y extendida.
- Las ACL nombradas permiten el uso de un nombre para identificar la lista de acceso en lugar de un número.
- Las ACL pueden configurarse para todos los protocolos de red enrutados.
- Las ACL se ubican en donde se pueda tener un control más eficiente.
- Las ACL, en general se usan en routers firewall.
- Las listas de acceso pueden también restringir el acceso de la terminal virtual al router.