



IT Essentials: PC Hardware and Software Version 4.0 Spanish
Capítulo 8

Redes



8.0 **Introducción**

En este capítulo, se presenta una descripción general de los principios, estándares y propósitos de la red. Se analizarán los siguientes tipos de red:

- * Red de área local (LAN)
- * Red de área extensa (WAN)
- * LAN inalámbrica (WLAN)

También se analizarán los diversos tipos de topologías, protocolos y modelos lógicos de red, y el hardware necesario para crear una red. Se abarcarán la configuración, la resolución de problemas y el mantenimiento preventivo. Además, se hablará sobre software de red, métodos de comunicación y relaciones de hardware.

Al completar este capítulo, alcanzará los siguientes objetivos:

- * Explicar los principios de networking.
- * Describir los tipos de redes.
- * Describir las tecnologías y los conceptos básicos de networking.
- * Describir los componentes físicos de una red.
- * Describir las arquitecturas y topologías de red LAN.
- * Identificar las organizaciones de estándares.
- * Identificar los estándares de Ethernet.
- * Explicar los modelos de datos OSI y TCP/IP.
- * Describir la forma en que se configuran una tarjeta NIC y un módem.
- * Identificar nombres, propósitos y características de otras tecnologías que se utilizan para establecer la conectividad.
- * Identificar y aplicar las técnicas comunes de mantenimiento preventivo utilizadas para las redes.
- * Resolver problemas en una red.

8.1 **Explicación de los principios de networking**

Las redes constituyen sistemas formados por enlaces. Los sitios Web que permiten que las personas creen enlaces entre sí con sus páginas se denominan sitios de redes sociales. Un conjunto de ideas relacionadas se puede denominar red conceptual. Las conexiones que usted tiene con todos sus amigos pueden denominarse su red personal.

Todos los días se utilizan las siguientes redes:

- * Sistema de entrega de correo
- * Sistema de telefonía
- * Sistema de transporte público
- * Red corporativa de computadoras
- * Internet

Las computadoras pueden estar conectadas por redes para compartir datos y recursos. Una red puede ser tan simple como dos computadoras conectadas por un único cable o tan compleja como cientos de computadoras conectadas a dispositivos que controlan el flujo de la información. Las redes de datos convergentes pueden incluir computadoras con propósitos generales, como computadoras

personales y servidores, así como dispositivos con funciones más específicas, tales como impresoras, teléfonos, televisores y consolas de juegos.

Todas las redes convergentes, de datos, voz y vídeo comparten información y emplean diversos métodos para dirigir el flujo de la información. La información en la red se traslada de un lugar a otro, a veces mediante rutas distintas, para llegar al destino correcto.

El sistema de transporte público es similar a una red de datos. Los automóviles, los camiones y otros vehículos son como los mensajes que viajan en la red. Cada conductor define el punto de partida (origen) y el punto final (destino). En este sistema, existen normas, como las señales de detención y los semáforos, que controlan la circulación desde el origen hasta el destino.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Definir las redes de computadoras.
- * Explicar los beneficios de networking.

Las redes están en todas partes



- 8.1 Explicación de los principios de networking
 - 8.1.1 Definición de las redes de computadoras

Una red de datos consiste en un conjunto de hosts conectados por dispositivos de red. Un host es cualquier dispositivo que envía y recibe información en la red. Los periféricos son dispositivos que están conectados a los hosts. Algunos dispositivos pueden actuar como hosts y periféricos. Por ejemplo, una impresora conectada a una computadora portátil que está en una red actúa como un periférico. Si la impresora está conectada directamente a un dispositivo de red, como un hub, un switch o un router, actúa como host.

Las redes de computadoras se utilizan globalmente en empresas, hogares, escuelas y organismos gubernamentales. Muchas de las redes se conectan entre sí a través de Internet.

Es posible conectar a una red diversos tipos de dispositivos:

- * Computadoras de escritorio
- * Computadoras portátiles
- * Impresoras
- * Escáneres
- * Asistentes digitales personales (PDA)
- * Teléfonos inteligentes
- * Servidores de impresión y de archivo

Una red puede compartir muchos tipos de recursos:

- * Servicios, como impresión o escaneo
- * Espacio de almacenamiento en dispositivos extraíbles, como discos duros o unidades ópticas
- * Aplicaciones, como bases de datos

Se pueden utilizar las redes para acceder a la información almacenada en otras computadoras, imprimir documentos mediante impresoras compartidas y sincronizar el calendario entre su computadora y su teléfono inteligente.

Los dispositivos de red se conectan entre sí mediante diversas conexiones:

- * Cableado de cobre: utiliza señales eléctricas para transmitir los datos entre los dispositivos.
- * Cableado de fibra óptica: utiliza cable de plástico o cristal, también denominado fibra, para transportar la información a medida que se emite luz.
- * Conexión inalámbrica: utiliza señales de radio, tecnología infrarroja (láser) o transmisiones por satélite.

Las redes de datos comparten muchos tipos de datos



- 8.1 Explicación de los principios de networking
- 8.1.2 Explicación de los beneficios de networking

Entre los beneficios de la conexión en red de computadoras y otros dispositivos, se incluyen costos bajos y mayor productividad. Gracias a las redes, se pueden compartir recursos, lo que permite reducir la duplicación y la corrupción de datos.

Se necesitan menos periféricos

La Figura 1 muestra que se pueden conectar muchos dispositivos en una red. Cada computadora en la red no necesita su propia impresora, escáner o dispositivo de copia de seguridad. Es posible configurar varias impresoras en una ubicación central y compartirlas entre los usuarios de la red. Todos los usuarios de la red envían los trabajos de impresión a un servidor de impresión central que administra las solicitudes de impresión. El servidor de impresión puede distribuir los trabajos de impresión entre las diversas impresoras o puede colocar en cola los trabajos que precisan una impresora determinada.

Mayores capacidades de comunicación

Las redes ofrecen diversas herramientas de colaboración que pueden utilizarse para establecer comunicaciones entre los usuarios de la red. Las herramientas de colaboración en línea incluyen correo electrónico, foros y chat, voz y vídeo, y mensajería instantánea. Con estas herramientas, los usuarios pueden comunicarse con amigos, familiares y colegas.

Se evitan la duplicación y la corrupción de los archivos

Un servidor administra los recursos de la red. Los servidores almacenan los datos y los comparten con los usuarios de una red. Los datos confidenciales o importantes se pueden proteger y se pueden compartir con los usuarios que tienen permiso para acceder a dichos datos. Se puede utilizar un software de seguimiento de documentos a fin de evitar que los usuarios sobrescriban o modifiquen archivos a los que otros usuarios están accediendo al mismo tiempo.

Menor costo en la adquisición de licencias

La adquisición de licencias de aplicaciones puede resultar costosa para computadoras individuales. Muchos proveedores de software ofrecen licencias de sitio para redes, lo que puede reducir considerablemente el costo de software. La licencia de sitio permite que un grupo de personas o toda una organización utilice la aplicación por una tarifa única.

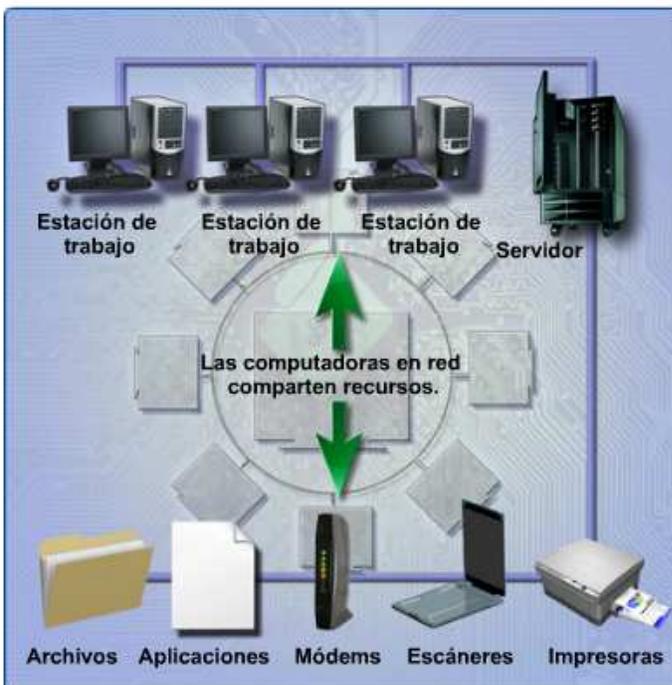
Administración centralizada

La administración centralizada reduce la cantidad de personas que se necesita para administrar los dispositivos y los datos en la red, lo que permite que la empresa ahorre tiempo y dinero. Los usuarios individuales de la red no necesitan administrar sus propios datos y dispositivos. Un administrador puede controlar los datos, dispositivos y permisos de los usuarios de la red. La creación de copias de seguridad de los datos resulta más sencilla ya que los datos se almacenan en una ubicación central.

Se conservan los recursos

Es posible distribuir el procesamiento de datos entre muchas computadoras para evitar que una computadora se sobrecargue con tareas de procesamiento.

Recursos compartidos



Ventajas y desventajas de networking

Ventajas y desventajas de la actividad de networking

Para seleccionar una respuesta, arrastre las opciones a la posición y haga clic en Verificar.

DESVENTAJA

Las redes deben administrarse.

La resolución de problemas puede resultar difícil.

Copia de seguridad de datos centralizada.

VENTAJA

Las redes permiten el acceso de grupos a documentos.

Los periféricos pueden compartirse.

¡Correcto!

Verificar

Reinicializar

8.2 Descripción de los tipos de redes

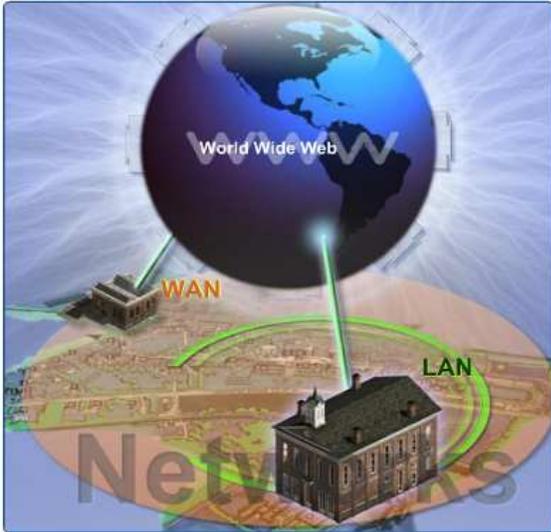
Las redes de datos evolucionan en cuanto a complejidad, uso y diseño. Para que sea posible hablar sobre redes, los diversos tipos de redes reciben nombres descriptivos distintos. Una red de computadoras se identifica en función de las siguientes características específicas:

- * El área a la que sirve.
- * El modo en que se almacenan los datos.
- * El modo en que se administran los recursos.
- * El modo en que se organiza la red.
- * El tipo de dispositivos de red empleados.
- * El tipo de medios que se utilizan para conectar los dispositivos.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Describir una LAN.
- * Describir una WAN.
- * Describir una WLAN.
- * Explicar las redes peer-to-peer.
- * Explicar las redes cliente/servidor.

Tipos de red



8.2 Descripción de los tipos de redes

8.2.1 Descripción de una LAN

Una red de área local (LAN) se refiere a un grupo de dispositivos interconectados que se encuentran bajo el mismo control administrativo. Antes, las redes LAN se consideraban redes pequeñas que existían en una única ubicación física. A pesar de que las redes LAN pueden ser tan pequeñas como una única red local instalada en un hogar o una oficina pequeña, con el paso del tiempo, la definición de LAN ha evolucionado hasta incluir las redes locales interconectadas que comprenden cientos de dispositivos, instalados en varios edificios y ubicaciones.

Es importante recordar que todas las redes locales dentro de una LAN se encuentran bajo un grupo de control administrativo que administra las políticas de seguridad y control de acceso que se aplican a la red. Dentro de este contexto, la palabra "local" en el término "red de área local" se refiere al control sistemático local y no significa que los dispositivos se encuentran físicamente cerca uno del otro. Los dispositivos que se encuentran en una LAN pueden estar cerca físicamente, pero esto no es obligatorio.

Red de área local (LAN, Local Area Network)

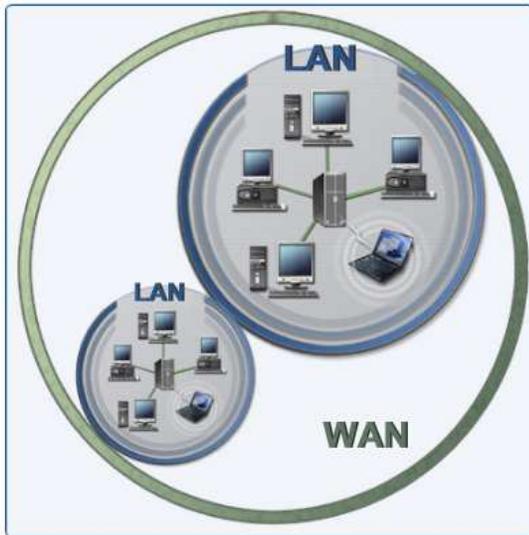


8.2 Descripción de los tipos de redes

8.2.2 Descripción de una WAN

Las redes de área extensa (WAN) constituyen redes que conectan redes LAN en ubicaciones que se encuentran geográficamente separadas. Internet es el ejemplo más común de una WAN. Internet es una red WAN grande que se compone de millones de redes LAN interconectadas. Se utilizan proveedores de servicios de telecomunicaciones (TSP) para interconectar estas redes LAN en ubicaciones diferentes.

Red de área extensa (WAN)



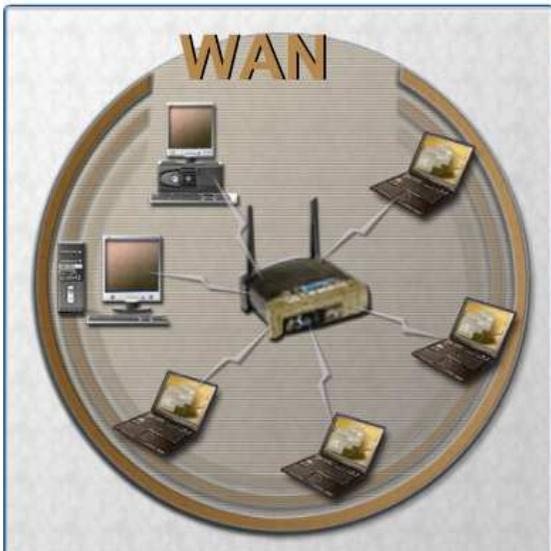
8.2 Descripción de los tipos de redes

8.2.3 Descripción de una WLAN

En una red LAN tradicional, los dispositivos se conectan entre sí mediante cables de cobre. En algunos entornos, es posible que la instalación de cables de cobre resulte poco práctica, no deseable o incluso imposible. En estos casos, se utilizan dispositivos inalámbricos para transmitir y recibir datos mediante ondas de radio. Estas redes se denominan redes LAN inalámbricas o WLAN. Al igual que en las redes LAN, en una WLAN es posible compartir recursos, como archivos e impresoras, y acceder a Internet.

En una WLAN, los dispositivos inalámbricos se conectan a puntos de acceso dentro de una área determinada. Por lo general, los puntos de acceso se conectan a la red mediante un cableado de cobre. En lugar de proporcionar cableado de cobre a todos los hosts de red, sólo el punto de acceso inalámbrico se conecta a la red con cables de cobre. La cobertura de WLAN puede ser pequeña y estar limitada al área de una sala, o puede contar con un alcance mayor.

Red de área local inalámbrica (WLAN)



Tipos de red

Actividad de tipos de red

Para seleccionar una respuesta, arrastre las opciones a la posición y haga clic en Verificar.

LAN	Este tipo de red utiliza las conexiones de cable en un solo grupo administrativo.
WAN	Este tipo de red utiliza muchas tecnologías para conectar redes lejanas.
WLAN	Este tipo de red utiliza puntos de acceso y NIC inalámbricas para la conectividad.

8.2 Descripción de los tipos de redes

8.2.4 Explicación de las redes peer-to-peer

En una red peer-to-peer, los dispositivos están conectados directamente entre sí, sin necesidad de contar con ningún dispositivo de red entre ellos. En este tipo de red, cada dispositivo tiene funciones y tareas equivalentes. Los usuarios individuales son responsables de sus propios recursos y pueden decidir qué datos y dispositivos desean compartir. Dado que los usuarios individuales son responsables de sus propias computadoras, no hay una administración o un punto central de control en la red.

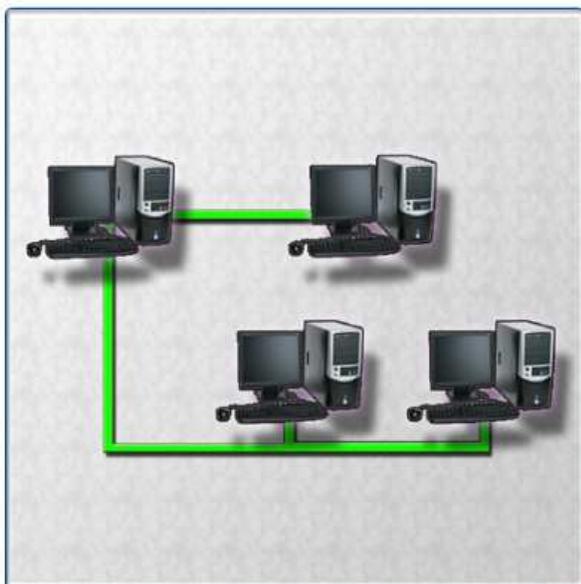
Las redes peer-to-peer funcionan mejor en entornos con diez computadoras o menos. Dado que los usuarios individuales controlan sus propias computadoras, no se necesita contratar un administrador de red dedicado.

Las redes peer-to-peer presentan varias desventajas:

- * No existe una administración de red centralizada, lo que dificulta determinar quién controla los recursos de la red.
- * No hay seguridad centralizada. Cada computadora debe utilizar medidas de seguridad individuales para la protección de los datos.
- * La red resulta más compleja y difícil de administrar a medida que aumenta la cantidad de computadoras en la red.
- * Es posible que no haya un almacenamiento centralizado de los datos. Se deben conservar individualmente copias de seguridad de los datos. Esta responsabilidad recae en los usuarios individuales.

En la actualidad, aún existen redes peer-to-peer dentro de redes más grandes. Incluso en una red cliente grande, los usuarios pueden compartir recursos directamente con otros usuarios, sin usar un servidor de red. En su hogar, si tiene más de una computadora, puede instalar una red peer-to-peer. Puede compartir archivos con otras computadoras, enviar mensajes entre las computadoras e imprimir documentos en una impresora compartida.

Red entre pares



8.2 Descripción de los tipos de redes

8.2.5 Explicación de las redes cliente/servidor

En una red cliente/servidor, el cliente solicita información o servicios del servidor. El servidor proporciona al cliente la información o los servicios solicitados. Los servidores en una red cliente/servidor suelen realizar parte del trabajo de procesamiento para los equipos cliente; por ejemplo, la clasificación dentro de una base de datos antes de proporcionar sólo los registros que solicita el cliente.

Un ejemplo de una red cliente/servidor es un entorno corporativo en el que los empleados usan un servidor de correo electrónico de la empresa para enviar, recibir y guardar correo electrónico. El cliente de correo electrónico en la computadora de un empleado emite una solicitud al servidor de correo electrónico para todo el correo electrónico no leído. El servidor responde mediante el envío al cliente del correo electrónico solicitado.

En un modelo cliente/servidor, los administradores de red realizan el mantenimiento de los servidores. El administrador de red implementa las medidas de seguridad y las copias de seguridad de los datos. Asimismo, el administrador de red controla el acceso de los usuarios a los recursos de la red. Todos los datos que se encuentran en la red se almacenan en un servidor de archivo centralizado. Un servidor de impresión centralizado administra las impresoras compartidas de la red. Los usuarios de red con los permisos correspondientes pueden acceder a los datos y a las impresoras compartidas. Cada usuario debe proporcionar un nombre de usuario autorizado y una contraseña para poder acceder a los recursos de red para los cuales tiene autorización.

Para la protección de datos, un administrador crea una copia de seguridad de rutina de todos los archivos contenidos en los servidores. Si una computadora deja de funcionar, o si se pierden datos, el administrador puede recuperar los datos de una copia de seguridad reciente con facilidad.

Red cliente/servidor



8.3 Descripción de las tecnologías y los conceptos básicos de networking

En su carácter de técnico, deberá configurar y resolver problemas de las computadoras conectadas en una red. Para configurar correctamente una computadora en la red, debe comprender el direccionamiento IP, los protocolos y otros conceptos de red.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Explicar el ancho de banda y la transmisión de datos.
- * Describir el direccionamiento IP.
- * Definir DHCP.
- * Describir las aplicaciones y los protocolos de Internet.
- * Definir ICMP.

Conceptos básicos de red



8.3 Descripción de las tecnologías y los conceptos básicos de networking

8.3.1 Explicación del ancho de banda y la transmisión de datos

El ancho de banda es la cantidad de datos que se pueden transmitir en un período de tiempo determinado. Cuando se envían datos en una red, se dividen en pequeñas porciones denominadas paquetes. Cada paquete contiene encabezados. Un encabezado constituye información que se agrega en cada paquete que contiene el origen y el destino del paquete. Un encabezado también contiene información que describe cómo volver a integrar los paquetes en el destino. El tamaño del ancho de banda determina la cantidad de información que puede transmitirse.

El ancho de banda se mide en bits por segundo y generalmente se representa con cualquiera de las siguientes unidades de medida:

- * bps: bits por segundo
- * Kbps: kilobits por segundo
- * Mbps: megabits por segundo

NOTA: Un byte equivale a 8 bits y se abrevia con B mayúscula. Un MBps equivale a aproximadamente 8 Mbps.

En la Figura 1, se muestra cómo se puede comparar el ancho de banda con una autopista. En el ejemplo de la autopista, los automóviles y camiones representan los datos. La cantidad de carriles representa la cantidad de vehículos que pueden circular simultáneamente en la autopista. Por una autopista de ocho carriles, pueden circular el cuádruple de vehículos que por una autopista de dos carriles.

Los datos que se transmiten en la red pueden circular en uno de tres modos: simplex, half-duplex o full-duplex.

Simplex

El modo simplex, también denominado unidireccional, es una transmisión única, de una sola dirección. Un ejemplo de transmisión simplex es la señal que se envía de una estación de TV a la TV de su casa.

Half-Duplex

Cuando los datos circulan en una sola dirección por vez, la transmisión se denomina half-duplex. En la transmisión half-duplex, el canal de comunicaciones permite alternar la transmisión en dos direcciones, pero no en ambas direcciones simultáneamente. Las radios bidireccionales, como las radios móviles de comunicación de emergencias o de la policía, funcionan con transmisiones half-duplex. Cuando presiona el botón del micrófono para transmitir, no puede oír a la persona que se encuentra en el otro extremo. Si las personas en ambos extremos intentan hablar al mismo tiempo, no se establece ninguna de las transmisiones.

Full-Duplex

Cuando los datos circulan en ambas direcciones a la vez, la transmisión se denomina full-duplex. A pesar de que los datos circulan en ambas direcciones, el ancho de banda se mide en una sola dirección. Un cable de red con 100 Mbps en modo full-duplex tiene un ancho de banda de 100 Mbps.

Un ejemplo de comunicación full-duplex es una conversación telefónica. Ambas personas pueden hablar y escuchar al mismo tiempo.

La tecnología de red full-duplex mejora el rendimiento de la red ya que se pueden enviar y recibir datos de manera simultánea. La tecnología de banda ancha permite que varias señales viajen en el mismo cable simultáneamente. Las tecnologías de banda ancha, como la línea de suscriptor digital (DSL) y el cable, funcionan en modo full-duplex. Con una conexión DSL, los usuarios, por ejemplo, pueden descargar datos en la computadora y hablar por teléfono al mismo tiempo.

Analogía de la autopista



8.3 Descripción de las tecnologías y los conceptos básicos de networking

8.3.2 Descripción del direccionamiento IP

Una dirección IP es un número que se utiliza para identificar un dispositivo en la red. Cada dispositivo conectado en una red debe tener una dirección IP exclusiva para poder comunicarse con otros dispositivos de la red. Como se observó anteriormente, un host es un dispositivo que envía o recibe información en la red. Los dispositivos de red son dispositivos que trasladan datos en la red, incluso hubs, switches y routers. En una LAN, cada uno de los hosts y de los dispositivos de red debe tener una dirección IP dentro de la misma red para poder comunicarse entre sí.

Por lo general, el nombre y las huellas digitales de una persona no se modifican. Ofrecen un rótulo o una dirección para el aspecto físico de la persona, es decir, el cuerpo. Por otra parte, la dirección postal de una persona se refiere al lugar donde la persona vive o recibe el correo. Esta dirección puede modificarse. En un host, la dirección de control de acceso al medio (MAC), que se explica más adelante, se asigna a la NIC del host y se denomina dirección física. La dirección física es siempre la misma, independientemente del lugar donde se ubique el host en la red, del mismo modo que las huellas digitales son siempre iguales para la persona, aunque ésta se mude.

La dirección IP es similar a la dirección postal de una persona. Se conoce como una dirección lógica, ya que se asigna lógicamente en función de la ubicación del host. La dirección IP o dirección de red se basa en la red local, y un administrador de red la asigna a cada host. Este proceso es similar a la asignación que hace un Gobierno local respecto de la dirección de una calle en función de la descripción lógica de la ciudad o del pueblo y del barrio.

Una dirección IP consiste en una serie de 32 bits binarios (unos y ceros). Resulta muy difícil para las personas leer una dirección IP binaria. Por ello, los 32 bits se agrupan en cuatro bytes de 8 bits, denominados octetos. Una dirección IP, incluso en este formato agrupado, es difícil de leer, escribir y recordar; por lo tanto, cada octeto se presenta como su valor decimal, separado por un punto. Este formato se denomina notación decimal punteada. Cuando se configura un host con una dirección IP, se escribe como un número decimal punteado, por ejemplo: 192.168.1.5. Suponga que tuviera que escribir el equivalente binario de 32 bits de: 1100000010101000000000100000101. Si se escribiera mal sólo un bit, la dirección sería diferente y el host no podría comunicarse en la red.

La dirección IP lógica de 32 bits es jerárquica y está compuesta por dos partes. La primera parte identifica la red, y la segunda identifica un host en dicha red. Ambas partes son necesarias en una dirección IP. Por ejemplo, si un host tiene la dirección IP 192.168.18.57, los primeros tres octetos, 192.168.18, identifican la porción de red de la dirección; y el último octeto, 57, identifica el host. Esto se denomina direccionamiento jerárquico, porque la porción de red indica la red en la cual se ubica cada dirección exclusiva de host. Los routers sólo deben saber cómo llegar a cada red y no la ubicación de cada host individual.

Las direcciones IP se clasifican en cinco grupos:

- * Clase A: Grandes redes, implementadas por grandes empresas y algunos países.
- * Clase B: Redes medianas, implementadas por universidades.
- * Clase C: Pequeñas redes, implementadas por ISP para las suscripciones de clientes.
- * Clase D: Uso especial para multicasting.
- * Clase E: Utilizada para pruebas experimentales.

Máscara de subred

La máscara de subred se utiliza para indicar la porción de la red de una dirección IP. Al igual que la dirección IP, la máscara de subred es un número decimal punteado. Por lo general, todos los hosts de una LAN utilizan la misma máscara de subred. La Figura 1 muestra las máscaras de subred por defecto para las direcciones IP utilizables que se asignan a las primeras tres clases de direcciones IP:

- * 255.0.0.0: Clase A, que indica que el primer octeto de la dirección IP es la porción de la red.
- * 255.255.0.0: Clase B, que indica que los primeros dos octetos de la dirección IP es la porción de la red.
- * 255.255.255.0: Clase C, que indica que los primeros tres octetos de la dirección IP es la porción de la red.

Si una organización cuenta con una red Clase B pero debe proporcionar direcciones IP para cuatro redes LAN, la organización deberá subdividir la dirección Clase B en cuatro partes más pequeñas. La división en subredes es una división lógica de una red. Proporciona los medios para dividir una red, y la máscara de subred especifica la forma en que está subdividida. Un administrador de red experimentado normalmente realiza una división en subredes. Una vez creado el esquema de división en subredes, las direcciones IP y máscaras de subred correspondientes pueden configurarse en los hosts en las cuatro redes LAN. Estas habilidades se enseñan en Cisco Networking Academy, en los cursos relacionados con los conocimientos de red del nivel de CCNA.

Configuración manual

En una red con pocos hosts, la configuración manual de cada dispositivo con la dirección IP correspondiente es fácil de realizar. Un administrador de red que comprende el direccionamiento IP debe asignar las direcciones y debe saber cómo elegir una dirección válida para una red específica. La dirección IP que se especifica es exclusiva para cada host dentro de la misma red o subred.

Para especificar manualmente una dirección IP en un host, vaya a la opciones de TCP/IP en la ventana Propiedades correspondiente a la tarjeta de interfaz de red (NIC). La tarjeta NIC es el hardware que permite que una computadora se conecte a una red. Tiene una dirección denominada dirección de control de acceso al medio (MAC). Mientras que la dirección IP es una dirección lógica que define el administrador de la red, una dirección MAC está "grabada" o programada de manera permanente en la NIC en el momento de su fabricación. La dirección IP de una NIC se puede modificar, pero la dirección MAC nunca se modifica.

La diferencia principal entre una dirección IP y una dirección MAC reside en que la dirección MAC se utiliza para entregar tramas en la LAN, mientras que una dirección IP se utiliza para transportar tramas fuera de la LAN. Una trama es un paquete de datos con la información de dirección agregada al comienzo y al final del paquete antes de la transmisión por la red. Una vez que una trama se entrega a la LAN de destino, la dirección MAC se utiliza para entregar la trama al host final en dicha LAN.

Si muchas computadoras componen la LAN, la configuración manual de las direcciones IP para todos los hosts de la red puede ser una tarea que demande mucho tiempo y que resulte proclive a errores. En este caso, el uso de un servidor de protocolo de configuración dinámica de host (DHCP) asignaría automáticamente las direcciones IP y simplificaría considerablemente el proceso de direccionamiento.

Clases de direcciones IP

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

Las direcciones Clase D se utilizan para grupos multicast. No es necesario asignar un octeto o bits a distintas direcciones de red o de host. Las direcciones Clase E se reservan para investigación solamente.

8.3 Descripción de las tecnologías y los conceptos básicos de networking

8.3.3 Definición de DHCP

El protocolo de configuración dinámica de host (DHCP) es una utilidad de software que se utiliza para asignar las direcciones IP a los dispositivos de red de modo dinámico. El proceso dinámico elimina la necesidad de asignar las direcciones IP manualmente. Se puede instalar un servidor de DHCP y se pueden configurar los hosts de manera que obtengan una dirección IP automáticamente. Cuando una computadora está configurada para obtener una dirección IP automáticamente, todas las demás casillas de configuración de dirección IP aparecen atenuadas, como se muestra en la Figura 1. El servidor conserva una lista de las direcciones IP para asignar y administra el proceso de manera que todos los dispositivos de la red reciban una dirección IP exclusiva. Cada dirección se guarda durante un plazo predeterminado. Cuando transcurre dicho plazo, el servidor de DHCP puede utilizar esta dirección para cualquier computadora que se incorpore a la red.

A continuación, se presenta la información de dirección IP que un servidor de DHCP puede asignar a los hosts:

- * Dirección IP
- * Máscara de subred
- * Gateway por defecto
- * Valores opcionales, como una dirección de servidor del sistema de nombres de dominios (DNS)

El servidor de DHCP recibe una solicitud de un host. A continuación, el servidor selecciona la información de dirección IP de un conjunto de direcciones por defecto que se almacenan en una base de datos. Una vez seleccionada la información de dirección IP, el

servidor de DHCP ofrece estos valores al host que realiza la solicitud en la red. Si el host acepta el ofrecimiento, el servidor de DHCP arrienda la dirección IP por un período de tiempo determinado.

El uso de un servidor de DHCP simplifica la administración de una red, ya que el software hace un seguimiento de las direcciones IP. La configuración automática de TCP/IP también reduce la posibilidad de asignar direcciones IP duplicadas o no válidas. Antes de que una computadora en la red pueda aprovechar los servicios del servidor de DHCP, la computadora debe poder identificar el servidor en la red local. Se puede configurar una computadora para que acepte una dirección IP de un servidor de DHCP al hacer clic en la opción Obtener dirección IP automáticamente de la ventana de configuración de NIC, como se muestra en la Figura 2.

Si la computadora no se puede comunicar con el servidor de DHCP para obtener una dirección IP, el sistema operativo Windows asignará automáticamente una dirección IP privada. Si se asigna una dirección IP a su computadora en el intervalo de 169.254.0.0 a 169.254.255.255, su computadora sólo podrá comunicarse con otras computadoras que se encuentren en el mismo intervalo. Estas direcciones privadas pueden ser útiles, por ejemplo, en una práctica de laboratorio en la que se desee evitar el acceso fuera de la red. Esta función del sistema operativo se denomina direccionamiento IP privado automático (APIPA). APIPA solicitará continuamente una dirección IP de un servidor de DHCP para su computadora.

Propiedades de TCP/IP



Obtener una dirección IP automáticamente



Un protocolo es un conjunto de reglas. Los protocolos de Internet son conjuntos de reglas que rigen la comunicación dentro de las computadoras de una red y entre ellas. Las especificaciones del protocolo definen el formato de los mensajes que se intercambian. Una carta enviada mediante el sistema postal también usa protocolos. Parte del protocolo especifica la posición en el sobre donde se debe escribir la dirección de entrega. Si la dirección de entrega está escrita en el lugar equivocado, no se podrá entregar la carta.

La temporización es de vital importancia para el funcionamiento de la red. Los protocolos requieren que los mensajes lleguen dentro de intervalos de tiempo determinados para que las computadoras no esperen indefinidamente los mensajes que puedan haberse perdido. Por lo tanto, los sistemas cuentan con uno o más temporizadores durante la transmisión de los datos. Los protocolos también inician acciones alternativas si la red no cumple con las reglas de temporización. Muchos protocolos están formados por un suite de otros protocolos agrupados en capas. Estas capas dependen del funcionamiento de las demás capas del grupo para su funcionamiento correcto.

A continuación, se mencionan las funciones principales de los protocolos:

- * Identificar errores.
- * Comprimir los datos.
- * Decidir cómo deben enviarse los datos.
- * Direccionar los datos.
- * Decidir cómo anunciar los datos enviados y recibidos.

Aunque existen muchos otros protocolos, en la Figura 1, se resumen algunos de los protocolos más comunes que se utilizan en redes y en Internet.

Para comprender cómo funcionan las redes e Internet, debe estar familiarizado con los protocolos comúnmente utilizados. Estos protocolos se utilizan para explorar la Web, enviar y recibir correo electrónico y transferir archivos de datos. Conocerá otros protocolos a medida que adquiera más experiencia en TI, pero éstos no se utilizan con tanta frecuencia como los protocolos comunes que se describen aquí.

En la Figura 2, haga clic en los nombres de los protocolos para obtener más información sobre cada uno de ellos.

Cuanto más comprenda sobre cada uno de estos protocolos, más entenderá sobre el funcionamiento de las redes e Internet.

Protocolos

Protocolo	Descripción
TCP/IP	Un protocolo utilizado para transportar datos en Internet.
NETBEUI/NETBIOS	Un protocolo pequeño y rápido, diseñado para una red de grupo de trabajo que no requiere conexión a Internet.
IPX/SPX	Un protocolo utilizado para transportar datos en una red Netware de Novell.
HTTP/HTTPS	Un protocolo que define de qué manera se intercambian archivos en la Web.
FTP	Un protocolo que brinda servicios para la transferencia y la manipulación de archivos.
SSH	Un protocolo que se utiliza para conectar computadoras de manera segura.
Telnet	Un protocolo que utiliza una conexión basada en texto para una computadora remota TCP/IP.
POP	Un protocolo utilizado para descargar mensajes de correo electrónico de un servidor de correo electrónico.
IMAP	Un protocolo utilizado para descargar mensajes de correo electrónico de un servidor de correo electrónico.
SMTP	Un protocolo utilizado para enviar correo en una red TCP/IP.

Detalles de protocolos comunes	
TCP/IP	La suite de protocolos TCP/IP se ha convertido en el estándar dominante para internetworking. TCP/IP representa un conjunto de estándares públicos que especifican cómo los paquetes de información se intercambian entre computadoras a través de una o más redes.
IPX/SPX	Intercambio de paquetes de internetwork/Intercambio de paquete secuenciado es la suite de protocolos utilizada originalmente por el sistema operativo de red de Novell Corporations, NetWare. Brinda funciones similares a las que se incluyen en TCP/IP. Novell, en sus versiones actuales, es compatible con el conjunto de aplicaciones TCP/IP. Aún existe una gran base instalada de redes NetWare que sigue utilizando IPX/SPX.
NetBEUI	La interfaz de usuario NetBIOS extendida es un protocolo utilizado principalmente en redes pequeñas de Windows NT. NetBEUI no se puede enrutar ni utilizar con routers para la comunicación en una red grande. NetBEUI es ideal para redes peer-to-peer pequeñas que incluyen pocas computadoras directamente conectadas entre sí. Puede utilizarse junto con otro protocolo enrutable, como TCP/IP. Esto proporciona al administrador de red las ventajas del alto rendimiento de NetBEUI dentro de la red local y la capacidad de comunicarse más allá de la LAN a través de TCP/IP.
AppleTalk	AppleTalk es una suite de protocolos para colocar en red computadoras Macintosh. Está compuesta por un completo conjunto de protocolos que abarcan las siete capas del modelo de referencia OSI. El protocolo AppleTalk fue diseñado para ser ejecutado en LocalTalk, la topología física de la LAN de Apple, y en los principales tipos de LAN, sobre todo Ethernet y Token Ring.
HTTP	El protocolo de transferencia de hipertexto rige la manera en que se intercambian los archivos, como texto, gráficos, sonidos y video, en la World Wide Web (WWW). El grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force) desarrolló los estándares para HTTP.
FTP	El protocolo de transferencia de archivos es un protocolo que ofrece servicios para la transferencia y la manipulación de archivos. El FTP permite conexiones múltiples y simultáneas con sistemas de archivos remotos.
SSH	El host Secure Socket se utiliza para conectarse de manera segura a una computadora remota.
TELNET	Telnet es una aplicación que se utiliza para conectarse a una computadora remota, pero carece de funciones de seguridad.
POP	El protocolo de oficina de correos se utiliza para descargar correo electrónico de un servidor de correo remoto.
IMAP	El protocolo de acceso a mensajes de Internet también se utiliza para descargar correo electrónico de un servidor de correo remoto.
SMTP	El protocolo simple de transferencia de correo (SMTP) se utiliza para enviar un correo electrónico a un servidor de correo remoto.

Protocolos de red

Actividad de tipos de red

Para seleccionar una respuesta, arrastre las opciones a la posición y haga clic en Verificar.

IPX/SPX	Un protocolo utilizado para transportar datos en una red Netware de Novell.
Netbeui/Netbios	Un protocolo pequeño y rápido, diseñado para una red de grupo de trabajo que no requiere conexión a Internet.
TCP/IP	Un protocolo utilizado para transportar datos en Internet.
Telnet	Un protocolo que utiliza una conexión basada en texto para una computadora remota TCP/IP.
SMTP	Un protocolo utilizado para enviar correo en una red TCP/IP.

8.3 Descripción de las tecnologías y los conceptos básicos de networking

8.3.5 Definición de ICMP

Los dispositivos conectados en una red utilizan el protocolo de mensajes de control de Internet (ICMP) para enviar mensajes de control y de error a las computadoras y a los servidores. Existen varios usos para ICMP, como anuncios de errores de la red, anuncios de congestión de la red y resolución de problemas.

El buscador de paquetes de Internet (ping) se suele utilizar para probar las conexiones entre computadoras. El ping es una utilidad de línea de comandos simple, pero muy útil, que se utiliza para determinar si se puede acceder a una dirección IP específica. Puede hacer ping a la dirección IP para comprobar la conectividad IP. El ping funciona mediante el envío de solicitud de eco de ICMP a una computadora de destino o a otro dispositivo de red. Luego, el dispositivo receptor envía un mensaje de respuesta de eco de ICMP para confirmar la conectividad.

El ping constituye una herramienta para la resolución de problemas que se utiliza para determinar la conectividad básica. En la Figura 1, se muestran los switches de línea de comandos que se pueden utilizar con el comando ping. Se envían cuatro solicitudes de eco de ICMP (pings) a la computadora de destino. Si se puede alcanzar, la computadora de destino responde con cuatro respuestas de eco de ICMP. El porcentaje de respuestas exitosas puede ayudarlo a determinar la confiabilidad y la accesibilidad de la computadora de destino.

Asimismo, se puede utilizar el comando ping para buscar la dirección IP de un host cuando el nombre es conocido. Si hace ping al nombre de un sitio Web, por ejemplo, www.cisco.com, como se muestra en la Figura 2, aparecerá la dirección IP del servidor.

Se utilizan otros mensajes de ICMP para informar paquetes no entregados, datos en una red IP que incluyen direcciones IP de origen y de destino, y si un dispositivo está muy ocupado para manejar el paquete. Los datos, en forma de paquete, llegan a un router, que es un dispositivo de red que envía los paquetes de datos en las redes hacia sus destinos. Si el router no sabe adónde enviar el paquete, lo elimina. Luego, el router envía un mensaje de ICMP a la computadora emisora que le indica que se eliminaron los datos. Cuando un router está muy ocupado, puede enviar a la computadora emisora un mensaje de ICMP diferente que indica que debe reducir la velocidad porque la red está congestionada.

Switches de comando ping

```
Símbolo del sistema
C:\>ping /?

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-w IOS]
      [-r cuenta] [-s cuenta] [-j lista-host] [-k lista-host]
      [-w tiempo de espera] nombre-destino

Opciones:
-t           Ping al host especificado hasta que se pare.
             Para ver estadísticas y continuar - presionar Control-Inter;
             Parar - presionar Control-C.
-a          Resolver direcciones en nombres de host.
-n cuenta   Número de peticiones eco para enviar.
-l tamaño   Enviar tamaño del búfer.
-f          Establecer No Fragmentar el indicador en paquetes.
-i TTL      Tiempo de vida.
-p IOS      Tipo de servicio.
-r cuenta   Ruta del registro para la cuenta de saltos.
-s count    Sello de hora para la cuenta de saltos.
-j lista-host Afloja la ruta de origen a lo largo de la lista- host.
-k lista-host Restringir la ruta de origen a lo largo de la lista- host.
-w tiempo de espera Tiempo de espera en milisegundos para esperar cada
             respuesta.
```

Utilice el comando ping para encontrar una dirección

```
Símbolo del sistema
C:\>ping cisco.com

Haciendo ping a cisco.com [198.133.219.25] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 198.133.219.25:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
             (100% perdidos).
```

8.4 Descripción de los componentes físicos de una red

Se pueden usar diversos dispositivos en una red para proporcionar conectividad. El dispositivo que se utilice dependerá de la cantidad de dispositivos que se conecten, el tipo de conexiones que éstos utilicen y la velocidad a la que funcionen los dispositivos. A continuación, se mencionan los dispositivos más comunes en una red:

- * Computadoras
- * Hubs
- * Switches
- * Routers
- * Puntos de acceso inalámbrico

Se necesitan los componentes físicos de una red para trasladar los datos entre estos dispositivos. Las características de los medios determinan dónde y cómo se utilizan los componentes. A continuación, se mencionan los medios más comunes utilizados en las redes:

- * Par trenzado
- * Cableado de fibra óptica
- * Ondas de radio

Al completar esta sección, alcanzará los siguientes objetivos:

- * Identificación de nombres, propósitos y características de los dispositivos de red.
- * Identificación de nombres, propósitos y características de los cables de red comunes.

Componentes físicos de red



8.4 Descripción de los componentes físicos de una red

8.4.1 Identificación de nombres, propósitos y características de los dispositivos de red

Para que la transmisión de datos sea más extensible y eficaz que una simple red peer-to-peer, los diseñadores de red utilizan dispositivos de red especializados, como hubs, switches, routers y puntos de acceso inalámbrico, para enviar datos entre los dispositivos.

Hubs

Los hubs, que se muestran en la Figura 1, son dispositivos que extienden el alcance de una red al recibir datos en un puerto y, luego, al regenerar los datos y enviarlos a todos los demás puertos. Este proceso implica que todo el tráfico de un dispositivo conectado al hub se envía a todos los demás dispositivos conectados al hub cada vez que el hub transmite datos. Esto genera una gran cantidad de tráfico en la red. Los hubs también se denominan concentradores porque actúan como punto de conexión central para una LAN.

Puentes y switches

Los archivos se descomponen en pequeñas piezas de datos, denominadas paquetes, antes de ser transmitidos a través de la red. Este proceso permite la comprobación de errores y una retransmisión más fácil en caso de que se pierda o se dañe el paquete. La información de dirección se agrega al comienzo y al final de los paquetes antes de su transmisión. El paquete, junto con la información de dirección, se denomina trama.

Las redes LAN generalmente se dividen en secciones denominadas segmentos, de la misma manera que una empresa se divide en departamentos. Los límites de los segmentos se pueden definir con un puente. Un puente es un dispositivo que se utiliza para filtrar el tráfico de la red entre los segmentos de la LAN. Los puentes llevan un registro de todos los dispositivos en cada segmento al cual está conectado el puente. Cuando el puente recibe una trama, examina la dirección de destino a fin de determinar si la trama debe enviarse a un segmento distinto o si debe descartarse. Asimismo, el puente ayuda a mejorar el flujo de datos, ya que mantiene las tramas confinadas sólo al segmento al que pertenece la trama.

Los switches, que se muestran en la Figura 2, también se denominan puentes multipuerto. Es posible que un puente típico tenga sólo dos puertos para unir dos segmentos de la misma red. Un switch tiene varios puertos, según la cantidad de segmentos de red que se desee conectar. Un switch es un dispositivo más sofisticado que un puente. Un switch genera una tabla de las direcciones MAC de las

computadoras que están conectadas a cada puerto. Cuando una trama llega a un puerto, el switch compara la información de dirección de la trama con su tabla de direcciones MAC. Luego, determina el puerto que se utilizará para enviar la trama.

Routers

Mientras que un switch conecta segmentos de una red, los routers, que se muestran en la Figura 3, son dispositivos que conectan redes completas entre sí. Los switches utilizan direcciones MAC para enviar una trama dentro de una misma red. Los routers utilizan direcciones IP para enviar tramas a otras redes. Un router puede ser una computadora con un software de red especial instalado o un dispositivo creado por fabricantes de equipos de red. Los routers contienen tablas de direcciones IP junto con las rutas de destino óptimas a otras redes.

Puntos de acceso inalámbrico

Los puntos de acceso inalámbrico, que se muestran en la Figura 4, proporcionan acceso de red a los dispositivos inalámbricos, como las computadoras portátiles y los asistentes digitales personales (PDA). El punto de acceso inalámbrico utiliza ondas de radio para comunicarse con radios en computadoras, PDA y otros puntos de acceso inalámbrico. Un punto de acceso tiene un alcance de cobertura limitado. Las grandes redes precisan varios puntos de acceso para proporcionar una cobertura inalámbrica adecuada.

Dispositivos multipropósito

Existen dispositivos de red que realizan más de una función. Resulta más cómodo adquirir y configurar un dispositivo que satisfaga todas sus necesidades que comprar un dispositivo para cada función. Esto resulta más evidente para el usuario doméstico. Para el hogar, el usuario preferiría un dispositivo multipropósito antes que un switch, un router y un punto de acceso inalámbrico. Un ejemplo de dispositivo multipropósito es Linksys 300N, que se muestra en la Figura 5.

Hubs



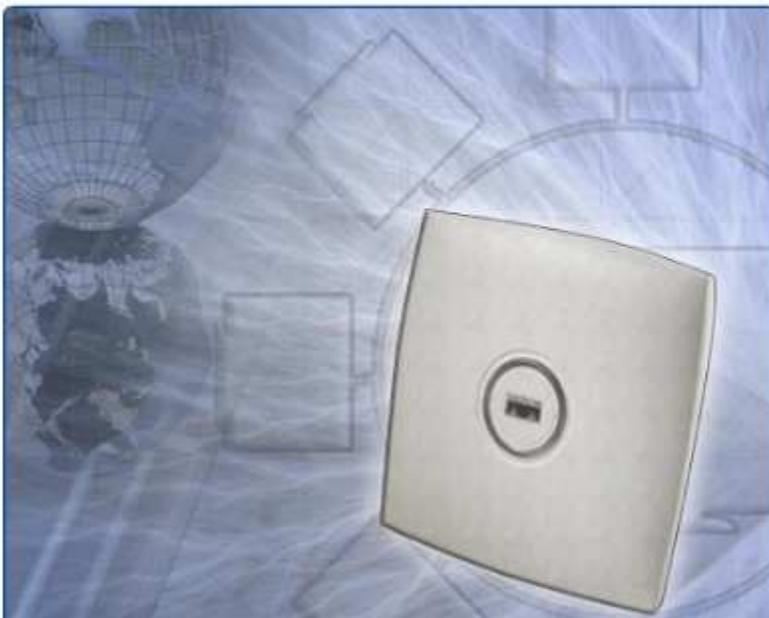
Switches



Routers



Puntos de acceso inalámbrico



Dispositivo multipropósito



8.4.2 Identificación de nombres, propósitos y características de los cables de red comunes

Hasta hace poco, los cables constituían el único medio para conectar dispositivos en las redes. Existe una gran variedad de cables de conexión de red. Los cables coaxiales y de par trenzado utilizan cobre para la transmisión de datos. Los cables de fibra óptica utilizan plástico o cristal para la transmisión de datos. Estos cables difieren en ancho de banda, tamaño y costo. Debe conocer el tipo de cable que se debe utilizar en los distintos casos para poder instalar los cables correctos para el trabajo. También debe saber resolver los problemas que se presenten.

Par trenzado

El par trenzado es un tipo de cableado de cobre que se utiliza para las comunicaciones telefónicas y la mayoría de las redes Ethernet. Un par de hilos forma un circuito que transmite datos. El par está trenzado para proporcionar protección contra crosstalk, que es el ruido generado por pares de hilos adyacentes en el cable. Los pares de hilos de cobre están envueltos en un aislamiento de plástico con codificación de color y trenzados entre sí. Un revestimiento exterior protege los paquetes de pares trenzados.

Cuando circula electricidad por un hilo de cobre, se crea un campo magnético alrededor del hilo. Un circuito tiene dos hilos y, en un circuito, los dos hilos tienen campos magnéticos opuestos. Cuando los dos hilos del circuito se encuentran uno al lado del otro, los campos magnéticos se cancelan mutuamente. Esto se denomina efecto de cancelación. Sin el efecto de cancelación, las comunicaciones de la red se ralentizan debido a la interferencia que originan los campos magnéticos.

Existen dos tipos básicos de cables de par trenzado:

- * Par trenzado no blindado (UTP): Cable que tiene dos o cuatro pares de hilos. Este tipo de cable cuenta sólo con el efecto de cancelación producido por los pares trenzados de hilos que limita la degradación de la señal que causa la interfaz electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cableado UTP es más comúnmente utilizado en redes. Los cables UTP tienen un alcance de 100 m (328 ft).

- * Par trenzado blindado (STP): Cada par de hilos está envuelto en un papel metálico para aislar mejor los hilos del ruido. Los cuatro pares de hilos están envueltos juntos en una trenza o papel metálico. El cableado STP reduce el ruido eléctrico desde el interior del cable. Asimismo, reduce la EMI y la RFI desde el exterior del cable.

Aunque el STP evita la interferencia de manera más eficaz que el UTP, STP es más costoso debido al blindaje adicional y es más difícil de instalar debido a su grosor. Además, el revestimiento metálico debe estar conectado a tierra en ambos extremos. Si no está conectado a tierra correctamente, el blindaje actúa como una antena que recoge las señales no deseadas. El STP se utiliza principalmente fuera de América del Norte.

Clasificación en categorías

Los cables UTP vienen en varias categorías que se basan en dos factores:

- * La cantidad de hilos que contiene el cable.
- * La cantidad de trenzas de dichos hilos.

La Categoría 3 es el cableado que se utiliza para los sistemas de telefonía y para LAN Ethernet a 10 Mbps. La Categoría 3 tiene cuatro pares de hilos.

La Categoría 5 y la Categoría 5e tienen cuatro pares de hilos con una velocidad de transmisión de 100 Mbps. La Categoría 5 y la Categoría 5e son los cables de red más comúnmente utilizados. El cableado Categoría 5e tiene más trenzas por pie que el de Categoría 5. Estas trenzas adicionales contribuyen a evitar la interferencia de fuentes externas y de otros hilos que se encuentran dentro del cable.

Algunos cables Categoría 6 tienen un divisor plástico para separar los pares de hilos, lo que evita la interferencia. Los pares también tienen más trenzas que los del cable Categoría 5e. La Figura 1 muestra un cable de par trenzado.

Cable coaxial

El cable coaxial es un cable con núcleo de cobre envuelto en un blindaje grueso. Se utiliza para conectar computadoras en una red. Existen diversos tipos de cable coaxial:

- * Thicknet o 10BASE5: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 500 m.
- * Thinnet 10BASE2: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 185 m.
- * RG-59: El más comúnmente utilizado para la televisión por cable en los Estados Unidos.
- * RG-6: Cable de mayor calidad que RG-59, con más ancho de banda y menos propensión a interferencia.

La Figura 2 muestra un cable coaxial.

Cable de fibra óptica

Una fibra óptica es un conductor de cristal o plástico que transmite información mediante el uso de luz. El cable de fibra óptica, que se muestra en la Figura 3, tiene una o más fibras ópticas envueltas en un revestimiento. Debido a que está hecho de cristal, el cable de fibra óptica no se ve afectado por la interferencia electromagnética ni por la interferencia de radiofrecuencia. Todas las señales se transforman en pulsos de luz para ingresar al cable y se vuelven a transformar en señales eléctricas cuando salen de él. Esto implica que el cable de fibra óptica puede emitir señales que son más claras, pueden llegar más lejos y puede tener más ancho de banda que el cable fabricado con cobre u otros metales.

El cable de fibra óptica puede alcanzar distancias de varias millas o kilómetros antes de que la señal deba regenerarse. El cable de fibra óptica es generalmente más costoso que el cable de cobre, y los conectores son más costosos y difíciles de ensamblar. Los conectores comunes para las redes de fibra óptica son SC, ST y LC. Estos tres tipos de conectores de fibra óptica son half-duplex, lo que permite que los datos circulen en una sola dirección. Por lo tanto, se precisan dos cables.

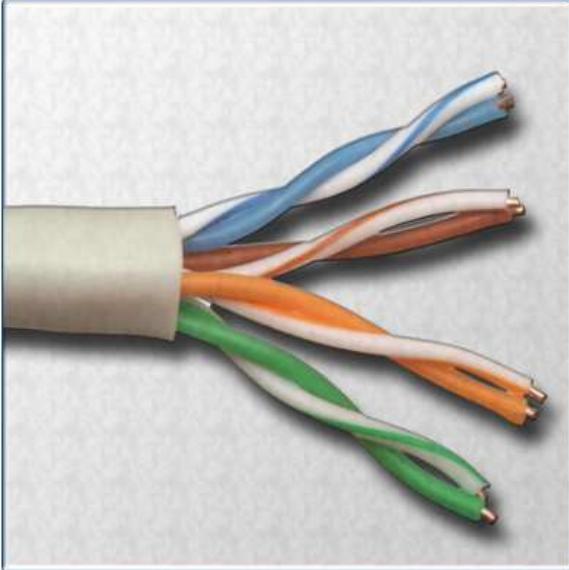
A continuación, se mencionan los dos tipos de cable de fibra óptica de cristal:

* Multimodo: Cable que tiene un núcleo más grueso que el cable monomodo. Es más fácil de realizar, puede usar fuentes de luz (LED) más simples y funciona bien en distancias de hasta unos pocos kilómetros.

* Monomodo: Cable que tiene un núcleo muy delgado. Es más difícil de realizar, usa láser como fuente de luz y puede transmitir señales a docenas de kilómetros con facilidad.

El cable de fibra óptica, que se muestra en la Figura 3, consiste en una o más fibras ópticas envueltas en un revestimiento.

Cables de par trenzado



Cables coaxiales



Cableado de fibra óptica



8.5 Descripción de las arquitecturas y topologías de red LAN

La mayoría de las computadoras con las que trabaja formarán parte de una red. Las topologías y arquitecturas son elementos fundamentales para el diseño de una red de computadoras. Aunque no necesite crear una red de computadoras, debe comprender cómo se diseña a fin de trabajar en computadoras que forman parte de una red.

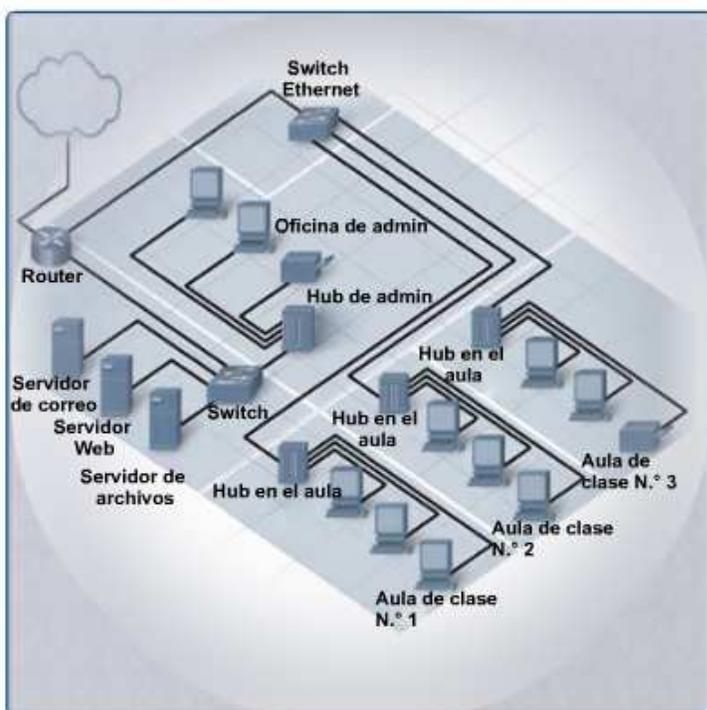
Hay dos tipos de topologías de LAN: la física y la lógica. Una topología física, que se muestra en la Figura 1, es la distribución física de los componentes de la red. Una topología lógica, que se muestra en la Figura 2, determina la forma en que los hosts se comunican a través de un medio, como un cable o las ondas de aire. Por lo general, las topologías se representan como diagramas de red.

Una arquitectura LAN se crea en torno a una topología. La arquitectura LAN comprende todos los componentes que forman la estructura de un sistema de comunicación. Estos componentes incluyen el hardware, el software, los protocolos y la secuencia de operaciones.

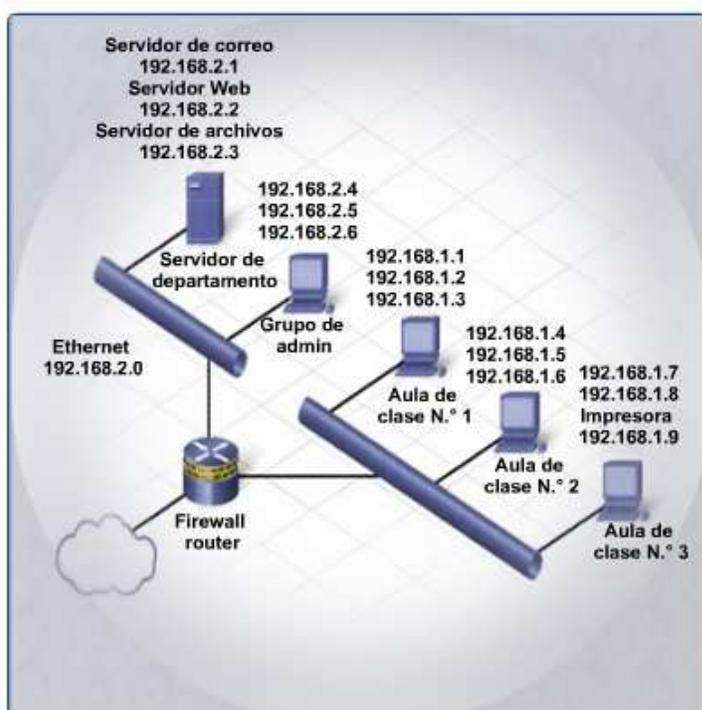
Al completar esta sección, alcanzará los siguientes objetivos:

- * Describir las topologías LAN.
- * Describir las arquitecturas LAN.

Topología física



Topología lógica



8.5 Descripción de las arquitecturas y topologías de red LAN

8.5.1 Descripción de las topologías LAN

Una topología física define el modo en que se conectan computadoras, impresoras y otros dispositivos a una red. Una topología lógica describe la forma en que el host accede al medio y se comunica en la red. El tipo de topología determina las capacidades de la red, por ejemplo: facilidad de configuración, velocidad y longitudes de cables.

Topologías físicas

La Figura 1 muestra las topologías físicas de LAN comunes:

- * Bus
- * Anillo
- * Estrella
- * Estrella extendida o jerárquica
- * Malla

Topología de bus

En la topología de bus, cada computadora se conecta a un cable común. El cable conecta una computadora a la siguiente, como una línea de autobús que recorre una ciudad. El cable tiene un casquillo en el extremo, denominado terminador. El terminador evita que las señales reboten y provoquen errores en la red.

Topología de ring

En una topología de ring, los hosts se conectan en un círculo o anillo físico. Dado que la topología de ring no tiene principio ni final, el cable no precisa terminadores. Una trama con formato especial, denominada token, viaja alrededor del anillo y se detiene en cada host. Si un host desea transmitir datos, debe conocer los datos y la dirección de destino a la trama. La trama se desplaza alrededor del anillo hasta que se detiene en el host con la dirección de destino. El host de destino extrae los datos de la trama.

Topología de estrella

La topología de estrella tiene un punto de conexión central, que generalmente es un dispositivo como un hub, un switch o un router. Cada host de la red tiene un segmento de cable que conecta el host directamente con el punto de conexión central. La ventaja de una topología de estrella reside en la facilidad de resolución de problemas. Cada host está conectado al dispositivo central con su propio cable. Si se presenta un problema en dicho cable, sólo ese host se ve afectado. El resto de la red continúa en funcionamiento.

Topología de estrella extendida o jerárquica

Una topología de estrella extendida o jerárquica es una red en estrella con un dispositivo de red adicional conectado al dispositivo de red principal. Por lo general, un cable de red se conecta a un hub y, luego, los otros hubs se conectan al primer hub. Las redes más grandes, como las de grandes empresas o universidades, utilizan la topología de estrella jerárquica.

Topología de malla

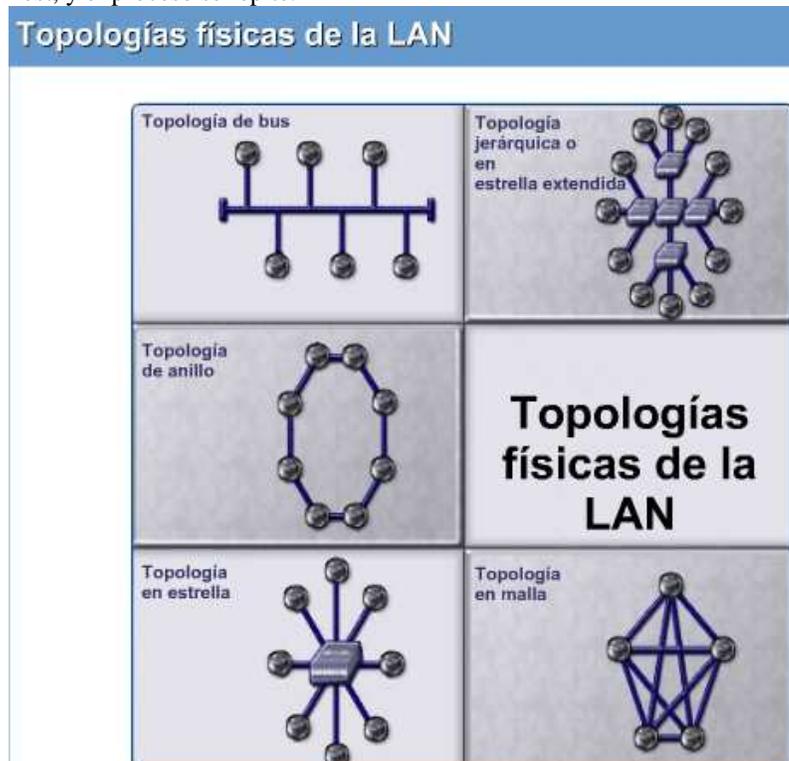
La topología de malla conecta todos los dispositivos entre sí. Cuando todos los dispositivos están interconectados, la falla de un cable no afecta a la red. La topología de malla se utiliza en redes WAN que interconectan redes LAN.

Topologías lógicas

Los dos tipos más comunes de topologías lógicas son broadcast y paso de tokens.

En una topología de broadcast, cada host direcciona cualquiera de los datos a un host específico o a todos los host conectados a la red. No hay un orden preestablecido que los hosts deban seguir para utilizar la red: los datos se transmiten en la red por orden de llegada.

El paso 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, 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 repite.



8.5 Descripción de las arquitecturas y topologías de red LAN

8.5.2 Descripción de las arquitecturas LAN

La arquitectura LAN describe las topologías físicas y lógicas que se utilizan en una red. En la Figura 1, se muestran las tres arquitecturas LAN más comunes.

Ethernet

La arquitectura Ethernet se basa en el estándar IEEE 802.3. El estándar IEEE 802.3 especifica que una red emplea el método de control de acceso denominado Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). En CSMA/CD, los hosts acceden a la red mediante el método de topología de broadcast de orden de llegada para la transmisión de datos.

Ethernet emplea una topología lógica de broadcast o bus y una topología física de bus o de estrella. A medida que las redes se amplían, la mayoría de las redes Ethernet se implementan mediante una topología de estrella jerárquica o extendida, como se muestra en la Figura 1. Las velocidades estándar de transferencia son 10 Mbps y 100 Mbps, pero los estándares nuevos proponen Gigabit Ethernet, que puede alcanzar velocidades de hasta 1000 Mbps (1 Gbps).

Token Ring

IBM originalmente desarrolló Token Ring como una arquitectura de red confiable y basada en el método de control de acceso de paso de tokens. Token Ring se integra generalmente con los sistemas de computadora central de IBM. Token Ring se utiliza con computadoras y computadoras centrales.

Token Ring constituye un ejemplo de una arquitectura en la que la topología física es distinta de su topología lógica. La topología Token Ring se conoce como un anillo cableado en forma de estrella ya que el aspecto externo del diseño de la red es una estrella. Las computadoras se conectan a un hub central, denominado unidad de acceso de estación múltiple (MSAU). Sin embargo, en el interior del dispositivo, el cableado forma una ruta circular de datos que crea un anillo lógico. El anillo lógico se crea debido a que el token viaja fuera de un puerto MSAU a una computadora. Si la computadora no tiene datos para enviar, el token se envía nuevamente al puerto MSAU y luego hacia el puerto siguiente, hasta la próxima computadora. Este proceso continúa para todas las computadoras y, por lo tanto, se asemeja a un anillo físico.

FDDI

FDDI es un tipo de red Token Ring. La implementación y la topología de FDDI difieren de la arquitectura LAN Token Ring de IBM. FDDI se utiliza frecuentemente para conectar varios edificios en un complejo de oficinas o en una ciudad universitaria.

FDDI se ejecuta en cable de fibra óptica. Combina el rendimiento de alta velocidad con las ventajas de la topología de ring de paso de tokens. FDDI se ejecuta a 100 Mbps en una topología de anillo doble. El anillo externo se denomina anillo principal y el anillo interno se denomina anillo secundario.

Normalmente, el tráfico circula sólo en el anillo principal. Si se produce un error en el anillo principal, los datos circulan automáticamente en el anillo secundario en la dirección opuesta.

Un anillo dual de FDDI admite un máximo de 500 computadoras por anillo. La distancia total de cada longitud del anillo de cable es de 100 km (62 millas). Cada 2 km (1,2 millas), se precisa un repetidor, que es un dispositivo que regenera las señales. En los últimos años, muchas redes token ring fueron reemplazadas por redes Ethernet más veloces.

Arquitecturas LAN

Arquitectura	Topología física	Topología lógica
Ethernet	Bus Estrella Estrella extendida	Bus
Token Ring	Estrella	Anillo
Interfaz de datos distribuida por fibra (FDDI)	Anillo doble	Anillo

8.6 Identificación de las organizaciones de estándares

Muchas organizaciones de estándares de todo el mundo tienen la responsabilidad de establecer estándares de networking. Los fabricantes utilizan los estándares como base para el desarrollo de tecnología, en especial, tecnologías de red y comunicaciones. La

tecnología de estandarización garantiza que los dispositivos utilizados serán compatibles con otros dispositivos que usen la misma tecnología. Los grupos de estándares crean, examinan y actualizan los estándares. Estos estándares se aplican al desarrollo de tecnología a fin de satisfacer las exigencias de mayor ancho de banda, comunicación eficaz y servicio confiable.

Haga clic en los estándares que aparecen en la Figura 1 para obtener más información.

Organización de estándares	
CCITT	<p><i>Comit Consultivo Internacional Telegráfico y Telefónico</i> Comité que define los estándares internacionales de comunicación. El CCITT definió el estándar para el envío de documentos por fax y los estándares que definen la transmisión de datos a través de líneas telefónicas, como V.90, que permiten transmisiones de hasta 56 000 bps. A partir de 1992, esta organización se transformó en el Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T)</p>
IEEE	<p>El IEEE es una asociación sin fines de lucro de profesionales técnicos que consta de más de 377000 miembros en 150 países. Esta organización se fundó en 1884 y está compuesta por ingenieros, científicos y estudiantes. Gracias al aporte de sus miembros, el IEEE es una autoridad líder en áreas técnicas que abarcan desde la ingeniería informática, la tecnología biomédica y las telecomunicaciones hasta la energía eléctrica, el aeroespacio y la electrónica para el consumo.</p> <p>El IEEE tiene más de 860 estándares activos y 700 en proceso de desarrollo. El IEEE es conocido por el desarrollo de estándares para la industria de la informática y la electrónica. En especial, los 802 estándares de la IEEE sobre las redes de área local se usan en gran medida.</p>
ISO	<p>La Organización Internacional para la Estandarización (ISO) es una organización internacional compuesta por organismos de normalización nacionales de más de 140 países. Por ejemplo, el Instituto Nacional Estadounidense de Estándares (ANSI) es miembro de la ISO. La ISO es una organización no gubernamental dedicada a promover el desarrollo de la normalización y actividades relacionadas. La labor de la ISO consiste en producir acuerdos internacionales, que se publican como estándares internacionales.</p> <p>La ISO definió varios estándares informáticos importantes. Entre ellos, el más significativo es tal vez, el modelo Interconexión de sistemas abiertos (OSI), una arquitectura estandarizada para el diseño de redes.</p> <p>La ISO, la Comisión de Electrotécnica Internacional (IEC, International Electrotechnical Commission) y la Unión Internacional de Telecomunicaciones (ITU, International Electrotechnical Commission) han creado una sociedad estratégica con la Organización Mundial del Comercio (WTO, World Trade Organization).</p>
IAB	<p>El Consejo de Arquitectura de Internet (IAB, Internet Architecture Board) es un comité que supervisa el desarrollo técnico y de ingeniería de Internet mediante la Sociedad de Internet (ISOC, Internet Society). Este comité supervisa al Grupo de Trabajo de Ingeniería de Internet (IETF, Internet Engineering Task Force) y al Grupo de Trabajo de Investigación de Internet (IRTF, Internet Research Task Force). En 1992, cuando Internet se convirtió en una entidad pública, el nombre que hoy conocemos provino del Consejo de Arquitectura de Internet, originalmente formado por el Departamento de Defensa de los Estados Unidos.</p>

IEC	<p>La Comisión de Electrotécnica Internacional (IEC) se fundó en 1906 y es la organización internacional que prepara y publica los estándares internacionales para las tecnologías eléctricas y electrónicas, y todas las tecnologías relacionadas. La IEC se fundó a partir de una resolución aprobada en el Congreso Eléctrico Internacional (International Electrical Congress) celebrado en St. Louis, EE. UU., en 1904. Está compuesta por más de 60 países e incluye a las principales naciones del mundo dedicadas al comercio y un número cada vez mayor de países industrializados.</p> <p>La misión de la IEC es promover, a través de sus miembros, la cooperación internacional en todas las cuestiones relacionadas con las electrotecnologías (como las tecnologías electrónica, magnética y electromagnética, electroacústica, multimedia, de telecomunicaciones y producción, y de distribución de energía) y también en las disciplinas generales asociadas, como terminología y símbolos, compatibilidad electromagnética, medición y rendimiento, fiabilidad, diseño y desarrollo, seguridad y medio ambiente.</p> <p>La IEC es uno de los organismos reconocidos por la WTO que, como parte de su acuerdo sobre barreras técnicas al comercio, le encomendó la tarea de control de las organizaciones nacionales y regionales que adoptaron el uso de estándares internacionales de la IEC como la base de estándares nacionales o regionales.</p>
ANSI	<p>El Instituto Nacional Estadounidense de Estándares (ANSI, American National Standards Institute) es una organización privada, sin fines de lucro, que administra y coordina el sistema de estándares y evaluación de conformidad de las normas en los EE. UU. El ANSI identifica los requisitos industriales y públicos para el consenso nacional, y coordina y administra su desarrollo, resuelve problemas relacionados con estándares nacionales y garantiza la participación efectiva en la estandarización internacional. A partir de 1918, la misión del instituto es mejorar la competitividad comercial de los EE. UU. en el ámbito internacional y la calidad de vida dentro del país, ya que promueve y facilita los estándares de consenso voluntario y los sistemas de evaluación de conformidad de las normas y, además, salvaguarda la integridad de estos factores.</p> <p>El ANSI no se encarga del desarrollo de estándares. Por el contrario, facilita su desarrollo por medio del proceso de establecimiento de consenso entre los grupos calificados. Éste es el motivo por el cual su acrónimo aparece en tantos estándares.</p>
TIA/EIA	<p>La Asociación de la Industria de las Telecomunicaciones (TIA, Telecommunications Industry Association) y la Asociación de Industrias de Electrónica (EIA, Electronic Industries Alliance) son asociaciones de comercio que desarrollan y publican de forma conjunta una serie de estándares que abarcan el cableado estructurado para voz y los datos para las LAN. Estos estándares de la industria evolucionaron a partir de la desregulación de la industria telefónica de los EE. UU. en 1984, que transfirió la responsabilidad del cableado de edificaciones al propietario del edificio. Antes de esto, AT&T utilizaba cables y sistemas de su propiedad.</p>

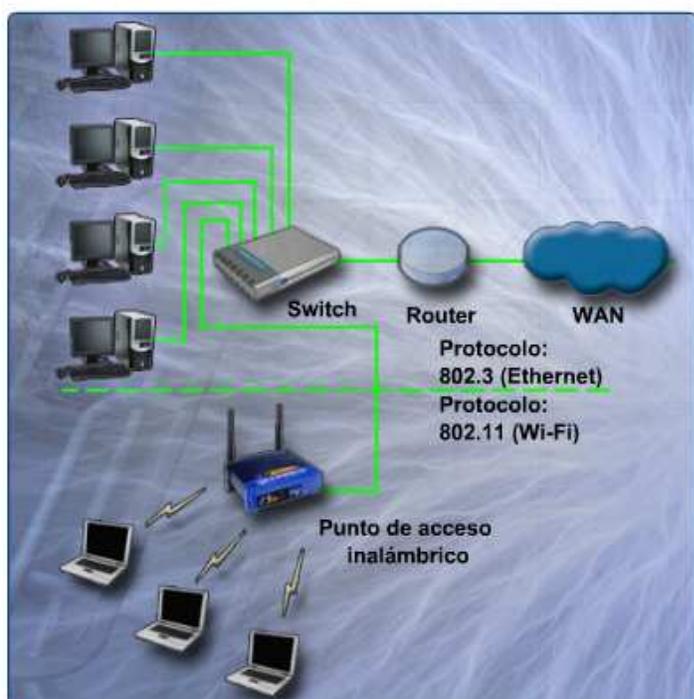
8.7 Identificación de los estándares de Ethernet

Los protocolos de Ethernet describen las reglas que controlan el modo en que se establece la comunicación en una red Ethernet. Con el fin de garantizar que todos los dispositivos Ethernet sean compatibles entre sí, IEEE creó estándares que los fabricantes y programadores deben cumplir al desarrollar dispositivos Ethernet.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Explicar los estándares de Ethernet por cable.
- * Explicar los estándares de Ethernet inalámbrica.

Interoperabilidad entre estándares



8.7 Identificación de los estándares de Ethernet 8.7.1 Explicación de los estándares de Ethernet por cable

IEEE 802.3

La arquitectura Ethernet se basa en el estándar IEEE 802.3. El estándar IEEE 802.3 especifica que una red implementa el método de control de acceso CSMA/CD.

En CSMA/CD, todas las estaciones finales "escuchan" al cable a fin de detectar espacio libre para enviar los datos. Este proceso es similar a la espera de tono de marcado del teléfono antes de marcar un número. Cuando la estación terminal detecta que no hay otro host que esté transmitiendo, intenta enviar los datos. Si ninguna otra estación envía datos al mismo tiempo, esta transmisión llega a la computadora de destino sin ningún problema. Si otra estación terminal observó la misma señal clara y transmitió al mismo tiempo, se produce una colisión en los medios de red.

La primera estación que detecta la colisión o la duplicación de voltaje envía una señal de congestión que ordena a todas las estaciones que detengan la transmisión y ejecuten un algoritmo de postergación. Un algoritmo de postergación calcula momentos aleatorios en los que la estación terminal comienza a intentar la transmisión por la red nuevamente. Este momento aleatorio está expresado, por lo general, en dos milisegundos o milésimos de segundo. Esta secuencia se origina cada vez que se produce una colisión en la red y puede reducir la transmisión de Ethernet hasta un 40%.

Tecnologías Ethernet

El estándar IEEE 802.3 define varias implementaciones físicas que admiten Ethernet. A continuación, se describen algunas de las implementaciones más comunes.

Ethernet

10BASE-T es una tecnología Ethernet que emplea una topología de estrella. 10BASE-T es una arquitectura Ethernet conocida cuyas funciones se indican en su nombre:

- * El diez (10) representa una velocidad de 10 Mbps.
- * BASE representa la transmisión de banda base. En la transmisión de banda base, todo el ancho de banda de un cable se utiliza para un tipo de señal.
- * La T representa el cableado de cobre de par trenzado.

Ventajas de 10BASE-T:

- * La instalación del cable no es costosa en comparación con la instalación de fibra óptica.
- * Los cables son delgados, flexibles y más fáciles de instalar que el cableado coaxial.
- * El equipo y los cables se actualizan con facilidad.

Desventajas de 10BASE-T:

- * La longitud máxima de un segmento de 10BASE-T es de sólo 100 m (328 ft).
- * Los cables son propensos a sufrir interferencia electromagnética (EMI).

Fast Ethernet

Las exigencias de gran ancho de banda de muchas aplicaciones modernas, como videoconferencia en directo y streaming audio, han generado la necesidad de disponer de velocidades más altas para la transferencia de datos. Muchas redes precisan más ancho de banda que Ethernet de 10 Mbps.

100BASE-TX es mucho más rápida que 10BASE-T y tiene un ancho de banda teórico de 100 Mbps.

Ventajas de 100BASE-TX:

- * A 100 Mbps, las velocidades de transferencia de 100BASE-TX son diez veces mayores que las de 10BASE-T.
- * 100BASE-X utiliza cableado de par trenzado, que es económico y fácil de instalar.

Desventajas de 100BASE-TX:

- * La longitud máxima de un segmento de 100BASE-TX es de sólo 100 m (328 ft).
- * Los cables son propensos a sufrir interferencia electromagnética (EMI).

1000BASE-T se denomina comúnmente Gigabit Ethernet. Gigabit Ethernet es una arquitectura LAN.

Ventajas de 1000BASE-T:

- * La arquitectura 1000BASE-T admite velocidades de transferencia de datos de 1 Gbps. A 1 Gbps, es diez veces más rápida que Fast Ethernet y 100 veces más rápida que Ethernet. Esta velocidad mayor permite implementar aplicaciones que exigen gran cantidad de ancho de banda, como vídeo en directo.
- * La arquitectura 1000BASE-T tiene interoperabilidad con 10BASE-T y 100BASE-TX.

Desventajas de 1000BASE-T:

- * La longitud máxima de un segmento de 1000BASE-T es de sólo 100 m (328 ft).
- * Es propenso a sufrir interferencias.
- * Las tarjetas NIC y los switches de Gigabit son costosos.
- * Se precisa equipo adicional.

10BASE-FL, 100BASE-FX, 1000BASE-SX y LX son tecnologías Ethernet de fibra óptica.

Estándares de Ethernet por cable

	10BASE-T	100BASE-TX	1000BASE-T
Medios	EIA/TIA Categoría 3; 4; 5 UTP, dos pares	EIA/TIA Categoría 5, 5e UTP, dos pares	EIA/TIA Categoría 5, 5e UTP, cuatro pares
Longitud máxima de segmento	100 m (328 ft)	100 m (328 ft)	100 m (328 ft)
Topología	Estrella	Estrella	Estrella
Conector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)

8.7 Identificación de los estándares de Ethernet

8.7.2 Explicación de los estándares de Ethernet inalámbrica

IEEE 802.11 es el estándar que especifica la conectividad para las redes inalámbricas. IEEE 802.11 o Wi-Fi se refiere al grupo colectivo de estándares 802.11a, 802.11b, 802.11g y 802.11n. Estos protocolos especifican las frecuencias, velocidades y otras capacidades de los diversos estándares Wi-Fi.

802.11a

Los dispositivos que conforman el estándar 802.11a permiten que las redes WLAN alcancen velocidades de transferencia de datos de 54 Mbps. Los dispositivos IEEE 802.11a funcionan en un intervalo de radiofrecuencia de 5 GHz y dentro de una distancia máxima de 45,7 m (150 ft).

802.11b

802.11b funciona en un intervalo de frecuencia de 2,4 GHz con una velocidad máxima teórica de transferencia de datos de 11 Mbps. Estos dispositivos funcionan dentro de una distancia máxima de 91 m (300 ft).

802.11g

IEEE 802.11g ofrece la misma velocidad máxima teórica que 802.11a, que es 54 Mbps, pero funciona en el mismo espectro de 2,4 GHz que 802.11b. A diferencia de 802.11a, 802.11g es compatible con 802.11b. 802.11g también tiene un alcance máximo de 91 m (300 ft).

802.11n

802.11n es un estándar inalámbrico más nuevo que tiene un ancho de banda teórico de 540 Mbps y funciona en un intervalo de frecuencia de 2,4 GHz o 5 GHz con un alcance máximo de 250 m (984 ft).

Estándares de Ethernet inalámbrica

Estándar	Ancho de banda	Frecuencia	Intervalo	Interoperabilidad
IEEE 802.11a	Hasta 54 Mbps	5 GHz en la banda	150 ft (45.7 m)	No interoperabilidad con 802.11b, 802.11g, 802.11n
IEEE 802.11b	Hasta 11 Mbps	2.4 GHz en la banda	300 ft (91 m)	Interoperabilidad con 802.11g
IEEE 802.11g	Hasta 54 Mbps	2.4 GHz en la banda	300 ft (91 m)	Interoperabilidad con 802.11b
IEEE 802.11n (Pre - estándar)	Hasta 540 Mbps	2.4 GHz en la banda	984 ft (250 m)	Interoperabilidad con 802.11b, 802.11g

8.8 Explicación de los modelos de datos OSI y TCP/IP

Un modelo arquitectónico es un marco de referencia común para explicar las comunicaciones en Internet y desarrollar protocolos de comunicación. Divide las funciones de los protocolos en capas administrables. Cada capa desempeña una función específica en el proceso de comunicación a través de una red.

El modelo TCP/IP fue creado por investigadores del Departamento de Defensa (DoD) de los Estados Unidos. El modelo TCP/IP es una herramienta que se utiliza para ayudar a explicar la suite de protocolos TCP/IP, que constituye el estándar predominante para la transferencia de datos en las redes. Este modelo tiene cuatro capas, como se muestra en la Figura 1.

A principios de la década de 1980, la Organización Internacional para la Estandarización (ISO) desarrolló el modelo Interconexión de sistema abierto (OSI), que se definió en el estándar ISO 7498-1, a fin de estandarizar la forma en que los dispositivos se comunican en la red. Este modelo tiene siete capas (como se muestra en la Figura 1) y fue un gran avance para garantizar la interoperabilidad entre los dispositivos de red.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Definir el modelo TCP/IP.
- * Definir el modelo OSI.
- * Comparar el modelo OSI con el modelo TCP/IP.

Modelo TCP/IP en comparación con el modelo OSI

Modelo TCP/IP	Modelo OSI
	Aplicación
Aplicación	Presentación
	Sesión
Transporte	Transporte
Internet	Red
Acceso a red	Enlace de datos
	Física

8.8 Explicación de los modelos de datos OSI y TCP/IP

8.8.1 Definición del modelo TCP/IP

El modelo de referencia TCP/IP ofrece un marco de referencia común para el desarrollo de los protocolos que se utilizan en Internet. Está compuesto por capas que realizan las funciones necesarias para preparar los datos para su transmisión a través de una red. El cuadro de la Figura 1 muestra las cuatro capas del modelo TCP/IP.

Un mensaje comienza en la capa superior, la capa de aplicación, y se desplaza por las capas de TCP/IP hasta la capa inferior, la capa de acceso a la red. Se agrega la información del encabezado al mensaje a medida que se desplaza hacia abajo por cada capa y después se transmite. Después de llegar a destino, el mensaje vuelve por cada capa del modelo TCP/IP. La información del encabezado que se agregó al mensaje se elimina a medida que el mensaje se desplaza hacia arriba por las capas hacia su destino.

Protocolos de aplicación

Los protocolos de la capa de aplicación ofrecen servicios de red a las aplicaciones de usuarios, como los exploradores Web y los programas de correo electrónico. Examine algunos de los protocolos de Internet más comunes de la Figura 2, la capa de aplicación, para obtener más información sobre los protocolos que funcionan en esta capa.

Protocolos de transporte

Los protocolos de la capa de transporte ofrecen una administración integral de los datos. Una de las funciones de estos protocolos es dividir los datos en segmentos administrables para facilitar su transporte a través de la red. Examine cada uno de los protocolos de la Figura 3, la capa de transporte, para obtener más información sobre los protocolos que funcionan en esta capa.

Protocolos de Internet

Los protocolos de la capa de Internet funcionan en la tercera capa de la parte superior en el modelo TCP/IP. Estos protocolos se utilizan para proporcionar conectividad entre los hosts de la red. Examine cada uno de los protocolos de la Figura 4, la capa de Internet, para obtener más información sobre los protocolos que funcionan en esta capa.

Protocolos de acceso de red

Los protocolos de la capa de acceso de red describen los estándares que utilizan los hosts para acceder a los medios físicos. En esta capa, se definen las tecnologías y los estándares de Ethernet IEEE 802.3, como CSMA/CD y 10BASE-T.

Modelo TCP/IP

Modelo TCP/IP	Capa	Descripción
Aplicación	4	Donde operan los protocolos de alto nivel, como SMTP y FTP
Transporte	3	Donde existen los protocolos de control de flujo y conexión
Internet	2	Donde se ejecutan el direccionamiento IP y el enrutamiento
Acceso a red	1	Donde existen el direccionamiento MAC y los componentes físicos de red

8.8 Explicación de los modelos de datos OSI y TCP/IP

8.8.2 Definición del modelo OSI

El modelo OSI es un marco estándar de la industria y se utiliza para dividir las comunicaciones de red en siete capas distintas. A pesar de que existen otros modelos, la mayoría de los fabricantes de redes de la actualidad crean sus productos con este marco.

Se denomina stack de protocolo al sistema que implementa un comportamiento de protocolo que consta de una serie de estas capas. Los stacks de protocolos se pueden implementar en hardware o software, o bien en una combinación de ambos. Por lo general, sólo las capas inferiores se implementan en hardware, y las capas superiores se implementan en software.

Cada capa es responsable de una parte del procesamiento para preparar los datos para su transmisión a través de la red. El cuadro de la Figura 1 muestra las funciones de cada capa del modelo OSI.

En el modelo OSI, cuando se transfieren los datos, se dice que viajan virtualmente hacia abajo a través de las capas del modelo OSI de la computadora emisora y hacia arriba a través de las capas del modelo OSI de la computadora receptora.

Cuando un usuario desea enviar datos, como correo electrónico, se inicia un proceso de encapsulación en la capa de aplicación. La capa de aplicación es responsable de proporcionar a las aplicaciones acceso a la red. La información circula por las tres capas superiores y es considerada como datos cuando llega a la capa de transporte.

En la capa de transporte, los datos se descomponen en segmentos más administrables o unidades de datos de protocolo (PDU) de la capa de transporte, para su transporte ordenado por la red. Una PDU describe los datos a medida que se desplazan desde una capa del modelo

OSI hasta la otra. La PDU de la capa de transporte también contiene información como números de puerto, de secuencia y de acuse de recibo, que se utiliza para el transporte confiable de los datos.

En la capa de red, cada segmento de la capa de transporte se transforma en un paquete. El paquete contiene el direccionamiento lógico y demás información de control de la capa 3.

En la capa de enlace de datos, cada paquete de la capa de red se transforma en una trama. La trama contiene la información de dirección física y corrección de errores.

En la capa física, la trama se transforma en bits. Estos bits se transmiten uno por uno a través del medio de red.

En la computadora receptora, el proceso de desencapsulación revierte el proceso de encapsulación. Los bits llegan a la capa física del modelo OSI de la computadora receptora. El proceso de desplazamiento hacia arriba del modelo OSI de la computadora receptora llevará los datos a la capa de aplicación, donde un programa de correo electrónico mostrará el mensaje.

NOTA: Una regla mnemotécnica puede ayudarlo a recordar las siete capas del modelo OSI. Algunos ejemplos son: "Algunas Personas Sólo Toman Ron En Fiestas" y "Festejemos Este Récord Tan Simpático Para Algunos".

Modelo OSI

Modelo OSI	Capa	Descripción
Aplicación	7	Responsable de los servicios de red para las aplicaciones
Presentación	6	Transforma el formato de los datos y proporciona una interfaz estándar para la capa de aplicación
Sesión	5	Establece, administra y finaliza las conexiones entre las aplicaciones locales y las remotas
Transporte	4	Proporciona transporte confiable y control del flujo a través de la red
Red	3	Responsable del direccionamiento lógico y el dominio del enrutamiento
Enlace de datos	2	Proporciona direccionamiento físico y procedimientos de acceso a medios
Física	1	Define todas las especificaciones eléctricas y físicas de los dispositivos

8.8 Explicación de los modelos de datos OSI y TCP/IP

8.8.3 Comparación entre el modelo OSI y el modelo TCP/IP

Tanto el modelo OSI como el modelo TCP/IP son modelos de referencia que se utilizan para describir el proceso de comunicación de datos. El modelo TCP/IP se utiliza específicamente para la suite de protocolos TCP/IP, y el modelo OSI se utiliza para el desarrollo de comunicación estándar para equipos y aplicaciones de diversos proveedores.

El modelo TCP/IP realiza el mismo proceso que el modelo OSI, pero utiliza cuatro capas en lugar de siete. El cuadro de la Figura 1 muestra una comparación de las capas de los dos modelos.

8.9 Descripción de la configuración de una tarjeta NIC y un módem

Para conectarse a Internet, es necesaria una tarjeta de interfaz de red (NIC). La tarjeta NIC puede venir instalada desde la fábrica, o el usuario puede adquirirla por su cuenta. En muy pocos casos, es posible que deba actualizarse el controlador. Se puede utilizar el disco del controlador que viene con la motherboard o el adaptador, o se puede suministrar un controlador que se descargó del fabricante.

Después de instalar la NIC y el controlador, se puede conectar la computadora a la red.

Además de instalar una NIC, es posible que también se deba instalar un módem para poder conectarse a Internet.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Instalar o actualizar un controlador de NIC.
- * Conectar la computadora a una red existente.
- * Describir la instalación de un módem.

Tarjetas de red y módems



8.9 Descripción de la configuración de una tarjeta NIC y un módem

8.9.1 Instalación o actualización de un controlador de NIC

A veces, los fabricantes presentan un software de controlador nuevo para una NIC. Un controlador nuevo puede mejorar la funcionalidad de la NIC o puede ser necesario para la compatibilidad con el sistema operativo.

Al instalar un controlador nuevo, asegúrese de deshabilitar el software de protección contra virus para que ninguno de los archivos se instale de manera incorrecta. Algunos antivirus detectan las actualizaciones de controlador como un posible ataque de virus. Además, sólo se debe instalar un controlador por vez; de lo contrario, algunos procesos de actualización pueden presentar conflictos.

Una mejor práctica consiste en cerrar todas las aplicaciones que están en ejecución para que no utilicen ninguno de los archivos asociados con la actualización del controlador. Antes de actualizar un controlador, deberá visitar el sitio Web del fabricante. En muchos casos, podrá descargar un archivo de controlador ejecutable de autoextracción que instalará o actualizará el controlador de manera automática. Otra posibilidad es hacer clic en el botón Actualizar controlador en la barra de herramientas del Administrador de dispositivos.

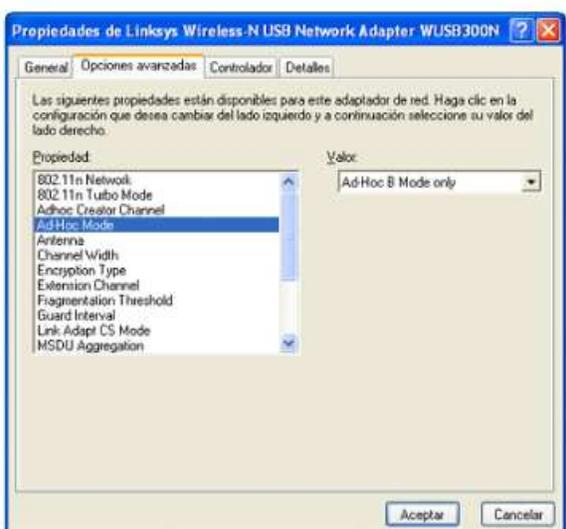
El signo "+" ubicado junto a la categoría de adaptadores de red permite expandir la categoría y mostrar los adaptadores de red instalados en el sistema. Para ver y cambiar las propiedades del adaptador o actualizar el controlador, haga doble clic en el adaptador. En la ventana de propiedades del adaptador, seleccione la ficha Controlador.

Una vez finalizada la actualización, se recomienda reiniciar la computadora, aunque no aparezca el mensaje que le solicita que reinicie el sistema. El reinicio de la computadora garantizará que la instalación se haya realizado del modo planeado y que el controlador nuevo funcione correctamente. Cuando instale varios controladores, reinicie la computadora entre cada actualización a fin de asegurarse de que no existan conflictos. Este paso demanda tiempo adicional, pero garantiza la instalación correcta del controlador.

Desinstalación de un controlador de NIC

Si un controlador de NIC nuevo no funciona del modo previsto después de la instalación, podrá desinstalarlo o volver al anterior. Haga doble clic en el adaptador del Administrador de dispositivos. En la ventana Propiedades del adaptador, seleccione la ficha Controlador y haga clic en Volver al controlador anterior. Esta opción no estará disponible si no había un controlador instalado antes de la actualización. En dicho caso, deberá buscar un controlador para el dispositivo e instalarlo manualmente si el sistema operativo no encontró un controlador adecuado para la tarjeta NIC.

Propiedades adaptador en el Admin. de dispositivos



8.9 Descripción de la configuración de una tarjeta NIC y un módem

8.9.2 Conexión de la computadora a una red existente

Una vez instalados los controladores de NIC, podrá conectarse a la red. Conecte un cable de red, también denominado cable Ethernet o de conexión directa, al puerto de red de la computadora. Conecte el otro extremo al dispositivo de red o al jack de pared.

Una vez conectado el cable, observe las luces de enlace junto al puerto Ethernet en la NIC para ver si hay actividad. La Figura 1 muestra la actividad de red en una NIC. Si no hay actividad, es posible que se deba a un cable defectuoso, a un puerto hub defectuoso o, incluso, a una NIC defectuosa. Es posible que deba reemplazar un dispositivo o más de uno para corregir el problema.

Después de comprobar que la computadora está conectada a la red y que las luces de enlace de la NIC indican que la conexión funciona, la computadora necesitará una dirección IP. La mayoría de las redes están configuradas para que la computadora reciba una dirección IP automáticamente de un servidor de DHCP local. Si la computadora no tiene una dirección IP, deberá introducir una dirección IP exclusiva en las propiedades de TCP/IP de la NIC.

Todas las NIC deben configurarse con la siguiente información:

- * Protocolos Se debe implementar el mismo protocolo entre dos computadoras que se comunican en la misma red.
- * Dirección IP Esta dirección puede configurarse y debe ser exclusiva para cada dispositivo. La dirección IP se puede configurar manualmente, o DHCP puede asignarla de manera automática.
- * Dirección MAC Cada dispositivo tiene una dirección MAC exclusiva. La dirección MAC viene asignada desde la fábrica y no se puede modificar.

Una vez que la computadora está conectada a la red, se debe comprobar la conectividad con el comando ping. Utilice el comando ipconfig, como se muestra en la Figura 2, para detectar su dirección IP. Haga ping a su propia dirección IP para asegurarse de que su NIC funciona correctamente. Después de determinar el funcionamiento de su NIC, haga ping a su gateway por defecto u otra computadora de su red, como se indica en la Figura 3. Un gateway por defecto permite que un host se comunique fuera de su red. Si tiene conexión a Internet, haga ping a un sitio Web conocido, como www.cisco.com. Si puede hacer ping correctamente a un sitio de Internet o a otra computadora de su red, su conexión funciona correctamente. Si no puede hacer ping a uno de ellos, deberá verificar la conexión con el proceso de resolución de problemas.

Luces de enlace



Comando ipconfig

```
Command Prompt
C:\>ipconfig /all

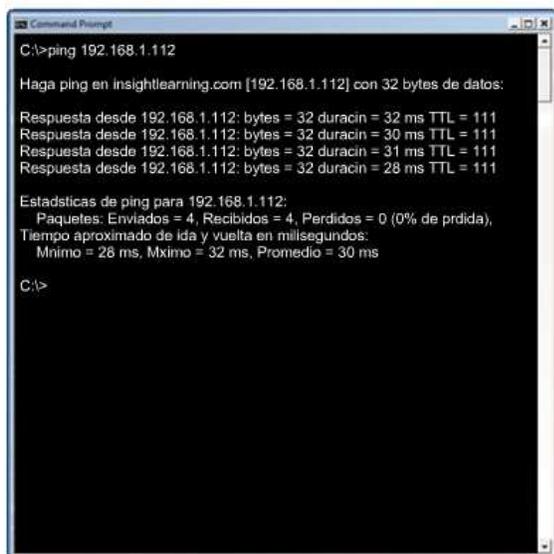
Configuración IP de Windows

Nombre de host . . . . . : rick
Sufrío de DNS principal . . . . . :
Tipo de nodo . . . . . : Hbrido
Enrutamiento IP habilitado . . . . . : No
WINS Proxy habilitado . . . . . : No
Lista de bsqueda de sufrío DNS . . . . . : ph.cox.net
ph.cox.net

Conexión de rea local del adaptador Ethernet:

Sufrío DNS específico de la conexión . : ph.cox.net
Descripción . . . . . : Controlador integrado Broadcom 440x 10/100
Dirección física . . . . . : 00-12-3F-E0-59-3D
Dhcp habilitado . . . . . : S
Autoconfiguración habilitada . . . . . : S
Dirección IP . . . . . : 192.168.1.112
Máscara de subred . . . . . : 255.255.255.0
Gateway por defecto . . . . . : 192.168.1.1
Servidor de DHCP . . . . . : 192.168.1.1
Servidor DNS . . . . . : 69.2.15.25
69.2.15.30
69.6.15.30
Comienzo del arrendamiento: . . . . . : martes, 3 de abril de 2007,
3:10:02 a. m.
Finalización del arrendamiento: . . . . . : miércoles, 4 de abril de 2007,
3:10:02 a. m.
```

Comando ping



```
C:\>ping 192.168.1.112

Haga ping en insightlearning.com [192.168.1.112] con 32 bytes de datos:

Respuesta desde 192.168.1.112: bytes = 32 duracin = 32 ms TTL = 111
Respuesta desde 192.168.1.112: bytes = 32 duracin = 30 ms TTL = 111
Respuesta desde 192.168.1.112: bytes = 32 duracin = 31 ms TTL = 111
Respuesta desde 192.168.1.112: bytes = 32 duracin = 28 ms TTL = 111

Estadísticas de ping para 192.168.1.112:
    Paquetes: Enviados = 4, Recibidos = 4, Perdidos = 0 (0% de prdida),
Tiempo aproximado de ida y vuelta en milisegundos:
    Míimo = 28 ms, Mxíimo = 32 ms, Promedio = 30 ms

C:\>
```

8.9 Descripción de la configuración de una tarjeta NIC y un módem

8.9.3 Descripción de la instalación de un módem

Un módem es un dispositivo electrónico que transfiere datos entre una computadora y otra mediante señales analógicas a través de una línea telefónica. En la Figura 1, se muestran ejemplos de módems. El módem convierte los datos digitales en señales analógicas para su transmisión. El módem en el extremo receptor convierte las señales analógicas nuevamente en datos digitales para que la computadora los pueda interpretar. El proceso de conversión de señales analógicas a señales digitales, y viceversa, se denomina modulación/desmodulación. La transmisión basada en módem es muy precisa, a pesar de que las líneas telefónicas pueden resultar ruidosas debido a los chasquidos, la estática u otros problemas.

Un módem interno se conecta a una ranura de expansión en la motherboard. Para configurar un módem, es posible que se deban establecer jumpers para seleccionar las direcciones E/S e IRQ. No se necesita ninguna configuración para un módem plug-and-play, que sólo se puede instalar en una motherboard que admita plug-and-play. Se debe configurar un módem que utilice un puerto serial que aún no esté en uso. Además, se deben instalar los controladores de software que vienen con el módem para que éste funcione correctamente. Los controladores de módems se instalan del mismo modo que los controladores de NIC.

Los módems externos se conectan a una computadora mediante los puertos seriales y USB .

El acceso telefónico a redes (DUN) se produce cuando las computadoras utilizan el sistema de telefonía pública para establecer comunicación. Los módems se comunican entre sí mediante señales de tono de audio. Esto significa que los módems pueden copiar las características de marcado de un teléfono. El acceso telefónico a redes crea una conexión de protocolo de punto a punto (PPP) entre dos computadoras mediante una línea telefónica.

Una vez establecida la conexión de línea, se produce una "secuencia de intercambio de señales" entre los dos módems y las computadoras. La secuencia de intercambio de señales es una serie de comunicaciones cortas que se establecen entre los dos sistemas. Esto se realiza para establecer la capacidad de los dos módems y las computadoras para participar en el intercambio de datos. Los módems de dial-up envían datos a través de una línea telefónica serial en forma de señal analógica. Dado que las señales analógicas cambian de manera gradual y continua, se pueden trazar como ondas. En este sistema, las señales digitales se representan con unos y ceros. Las señales digitales deben convertirse en una onda para que puedan viajar a través de las líneas telefónicas. El módem receptor vuelve a convertirlas a la forma digital (unos y ceros) para que la computadora receptora pueda procesar los datos.

Comandos AT

Todos los módems precisan un software para controlar la sesión de comunicación. La mayoría del software de módems utiliza un conjunto de comandos compatibles con Hayes. El conjunto de comandos Hayes se basa en un grupo de instrucciones que siempre comienza con un conjunto de caracteres de atención (AT), seguido de los caracteres de comando. Estos comandos se denominan comandos AT. En la Figura 2, se muestra el conjunto de comandos AT.

Los comandos AT son comandos de control de módem. El conjunto de comandos AT se utiliza para proporcionar al módem instrucciones tales como marcar, colgar, reiniciar, entre otras. La mayoría de los manuales del usuario que se incluyen con un módem tienen una lista completa del conjunto de comandos AT.

El código estándar compatible con Hayes para el marcado es ATDxxxxxxx. Por lo general, no hay espacios en una cadena AT. Si se introduce un espacio, la mayoría de los módems lo omitirá. La "x" representa el número marcado. Habrá siete dígitos para una llamada local y 11 dígitos para una llamada de larga distancia. Una W indica que el módem esperará una línea externa, si es necesario, para establecer un tono antes de continuar. A veces, se agrega una T, que representa el marcado por tonos, o una P, que representa el marcado por pulsos.

Módems



Comandos AT

Comando AT	Función
AT	Código de atención que precede a todos los comandos de acción del módem.
AP	Marque el número telefónico, xxxxxxx, con marcación por pulsos.
ATDT xxxxxxx	Marque el número telefónico, xxxxxxx, con marcación por tonos.
ATA	Conteste el teléfono de inmediato.
ATHO	Corte la llamada de inmediato.
ATZ	Restablezca la configuración de conexión del módem.
ATF	Restablezca los parámetros y la configuración del modem según los valores por defecto de fábrica.
AT+++	Interrumpa la señal, cambie del modo datos al modo comando.
P	Significa marcación por pulsos.
T	Significa marcación por tonos.
W	Indica que el módem esperará.

8.10 Identificación de los nombres, los propósitos y las características de otras tecnologías utilizadas para establecer la conectividad

Existen varias maneras de conectarse a Internet. Las empresas de telefonía, cable, satélite y telecomunicaciones privadas ofrecen conexiones a Internet para uso empresarial o doméstico.

En la década de 1990, Internet se utilizaba generalmente para la transferencia de datos. Las velocidades de transmisión eran lentas en comparación con las conexiones de alta velocidad que existen en la actualidad. La mayoría de las conexiones a Internet eran módems analógicos que utilizaban el "sistema de servicio telefónico tradicional" (POTS) para enviar y recibir datos. En los últimos años, muchas empresas y usuarios domésticos han cambiado por conexiones a Internet de alta velocidad. El ancho de banda adicional permite la transmisión de voz y vídeo, y, también de datos.

Es necesario comprender cómo los usuarios se conectan a Internet y las ventajas y desventajas de los diversos tipos de conexión.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Describir las tecnologías de telefonía.
- * Definir la comunicación por línea de energía.
- * Definir banda ancha.
- * Definir VOIP.

Conectividad



8.10 Identificación de nombres, propósitos y características de otras tecnologías que se utilizan para establecer la conectividad

8.10.1 Descripción de las tecnologías de telefonía

Existen diversas soluciones WAN para la conexión entre sitios o a Internet. Los servicios de conexión WAN ofrecen diferentes velocidades y niveles de servicio. Antes de comprometerse con cualquier tipo de conexión a Internet, investigue todos los servicios disponibles para determinar la mejor solución que satisfaga las necesidades de su cliente.

Teléfono analógico

Esta tecnología utiliza las líneas de telefonía de voz estándar. Este tipo de servicio emplea un módem que coloca una llamada telefónica en otro módem en un sitio remoto, como un proveedor de servicios de Internet. Existen dos grandes desventajas en el uso de la línea telefónica con un módem analógico. La primera consiste en que la línea telefónica no puede utilizarse para llamadas de voz cuando el módem está en uso. La segunda es el ancho de banda limitado que proporciona el servicio de telefonía analógica. El ancho de banda máximo que utiliza un módem analógico es de 56 Kbps, pero, en realidad, suele ser mucho menor. Un módem analógico no resulta una buena solución para las exigencias de las redes con mucha actividad.

Red digital de servicios integrados (ISDN)

ISDN es el próximo avance en servicio WAN. ISDN constituye un estándar para el envío de voz, vídeo y datos a través del cableado telefónico normal. La tecnología ISDN utiliza el cableado telefónico como un servicio de telefonía analógico. No obstante, emplea la tecnología digital para transportar los datos. Dado que utiliza tecnología digital, ofrece mayor calidad de voz y mayor velocidad en la transferencia de datos que el servicio de telefonía analógica tradicional.

Las conexiones digitales ISDN ofrecen tres servicios: Interfaz de acceso básico (BRI), Interfaz de acceso principal (PRI) e ISDN de banda ancha (BISDN). ISDN utiliza dos tipos distintos de canales de comunicación. El canal "B" se utiliza para transportar la información (datos, voz o vídeo) y el canal "D" se suele utilizar para control y señalización, pero puede emplearse para datos.

Haga clic en los nombres de los tipos de ISDN que se muestran en la Figura 1 para obtener más información.

Línea de suscriptor digital (DSL)

DSL es una tecnología "permanente". "Permanente" significa que no necesita marcar cada vez que desea conectarse a Internet. DSL utiliza las líneas telefónicas de cobre existentes para ofrecer una comunicación digital de datos a alta velocidad entre los usuarios finales y las empresas de telefonía. A diferencia de la tecnología ISDN, en la que las comunicaciones de datos digitales reemplazan las comunicaciones analógicas de voz, DSL comparte el cable telefónico con las señales analógicas.

La empresa de telefonía limita el ancho de banda de la voz analógica en las líneas. Este límite permite que DSL coloque los datos digitales en el cable telefónico en la parte no utilizada del ancho de banda. Esta capacidad de compartir el cable telefónico permite que se realicen llamadas de voz mientras DSL se conecta a Internet.

Existen dos consideraciones importantes cuando se selecciona DSL. DSL tiene limitaciones de distancia. Las líneas telefónicas utilizadas con DSL fueron diseñadas para transportar información analógica. Por lo tanto, la distancia a la que se puede enviar la señal digital se encuentra limitada y no puede pasar por cualquier tipo de multiplexor utilizado con líneas telefónicas analógicas. La otra consideración es que la información de voz y los datos transmitidos por DSL deben separarse en el sitio del cliente. Un dispositivo denominado divisor separa la conexión a los teléfonos y la conexión a los dispositivos de red local.

Línea de suscriptor digital asimétrica (ADSL)

ADSL es la tecnología DSL más frecuentemente utilizada en la actualidad. ADSL tiene diversas capacidades de ancho de banda en cada dirección. ADSL tiene una alta velocidad de descarga, por lo general, 1,5 Mbps. La descarga es el proceso de transferencia de datos desde el servidor hasta el usuario final. Este factor es de gran utilidad para los usuarios que descargan grandes cantidades de datos. El índice de carga de alta velocidad de ADSL es menor. ADSL no funciona bien cuando aloja un servidor Web o servidor FTP, los cuales implican actividades de Internet con una carga intensa.

Haga clic en los tipos de DSL que se muestran en la Figura 2 para obtener más información.

Tipos de ISDN	
BRI	La interfaz de acceso básico (BRI, Basic Rate Interface) ISDN ofrece una conexión exclusiva de 128 Kbps que utiliza dos canales B de 64 Kbps. Además, la BRI ISDN utiliza un canal D de 16 Kbps para la configuración, el control y el corte de llamadas.
PRI	La interfaz de acceso principal (PRI, Primary Rate Interface) ISDN ofrece hasta 1,544 Mbps a través de 23 canales B en América del Norte y Japón o 2,048 Mbps a través de 30 canales B en Europa y Australia. Además, la PRI ISDN utiliza un canal D de 64 Kbps para el mantenimiento de llamadas.
BISDN	La ISDN de banda ancha administra diversos tipos de servicio al mismo tiempo. La ISDN de banda ancha (BISDN) mayormente se utiliza en backbones de red.

Tipos de DSL	
ADSL	En la actualidad, la DSL asimétrica es la implementación más común. Las velocidades de descarga oscilan entre 384 Kbps y más de 6 Mbps. La velocidad de carga suele ser menor.
HDSL	La DSL de alta velocidad proporciona el mismo ancho de banda en ambas direcciones: en América del Norte es de 1,544 Mbps y en Europa es de 2,048 Mbps.
SDSL	La DSL simétrica proporciona la misma velocidad de carga y descarga de hasta 3 Mbps.
VDSL	La DSL de alta velocidad proporciona anchos de banda de 13 a 52 Mbps de descarga y de 16 Mbps de carga.
IDSL	En efecto, la DSL ISDN es DSL a través de líneas ISDN. Es un conjunto de normas CCITT/ITU de transmisión digital a través del cable telefónico común de cobre y también de otros medios, con una velocidad máxima de hasta 144 Kbps. La ISDN está disponible en áreas que no cuentan con las características necesarias para la implementación de DSL. Se necesita un adaptador ISDN en ambos extremos, el extremo del usuario como módem y un proveedor de servicio. Generalmente, la ISDN se ofrece en áreas urbanas de los Estados Unidos y Europa mediante compañías telefónicas locales.

8.10.2 Definición de la comunicación por línea de energía

La comunicación por línea de energía (PLC) constituye un método de comunicación que utiliza los cables de distribución de energía (red eléctrica local) para enviar y recibir datos.

PLC también se denomina:

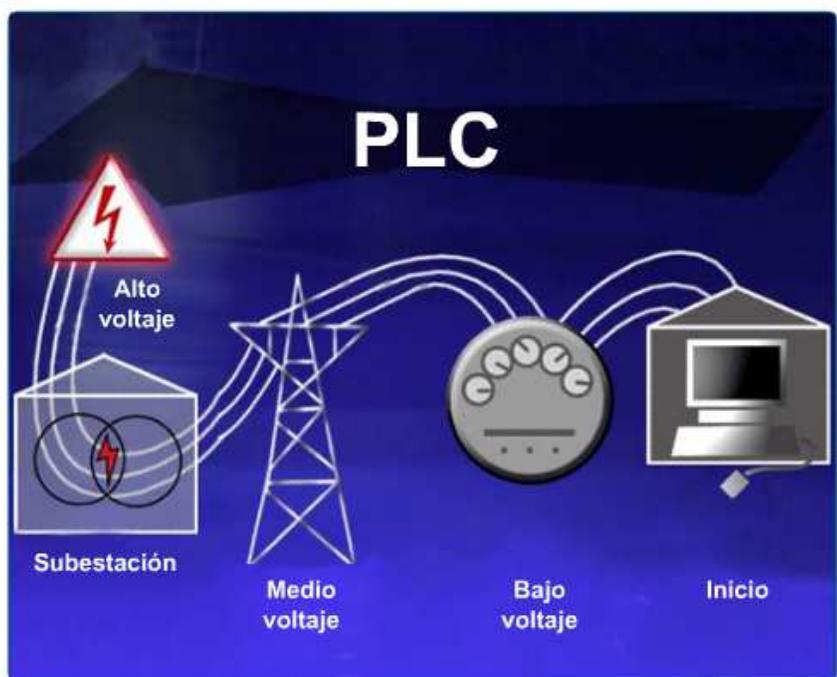
- * Red de línea de energía (PLN).
- * Comunicación por red eléctrica.
- * Telecomunicaciones por línea de energía (PLN).

Con PLC, una empresa de energía eléctrica puede superponer una señal analógica sobre la CA estándar de 50 ó 60 Hz que viaja por las líneas eléctricas. La señal analógica puede transportar señales de voz y datos.

La PLC puede estar disponible en áreas donde otras conexiones de alta velocidad no lo están. PLC es más rápida que un módem analógico y puede ser mucho menos costosa que otros tipos de conexión de alta velocidad. A medida que esta tecnología evolucione, se encontrará con más frecuencia y podrá aumentar la velocidad.

Puede utilizar una PCL para conectar en red computadoras en su hogar, en lugar de instalar cableado de red o tecnología inalámbrica. Las conexiones PLC pueden utilizarse en cualquier lugar donde exista una toma de corriente. Puede controlar la iluminación y los artefactos eléctricos mediante PCL sin necesidad de instalar un cableado de control.

Comunicación por línea de energía (PLC, PL Comm.)



8.10 Identificación de nombres, propósitos y características de otras tecnologías que se utilizan para establecer la conectividad
8.10.3 Definición de banda ancha

La banda ancha es una técnica empleada para transmitir y recibir varias señales con diversas frecuencias a través de un cable. Por ejemplo, el cable utilizado para instalar la televisión de cable en su hogar puede realizar, a la vez, transmisiones de redes de computadoras. Dado que los dos tipos de transmisión usan frecuencias diferentes, no se interfieren entre sí.

La banda ancha es un método de señalización que utiliza un amplio intervalo de frecuencias que pueden dividirse en canales. En lo que respecta a networking, el término "banda ancha" describe los métodos de comunicación que transmiten dos o más señales simultáneamente. El envío simultáneo de dos o más señales aumenta la velocidad de transmisión. Entre las conexiones de red de banda ancha comunes, las conexiones se encuentran por cable, DSL, ISDN y por satélite.

Cable

Un módem por cable conecta su computadora a la empresa de cable mediante el mismo cable coaxial que se conecta a su televisión. En la Figura 1, se muestra un módem por cable. Puede conectar su computadora directamente al módem por cable, o bien, puede conectarlo a un router, un hub o un dispositivo de red multipropósito para que varias computadoras puedan compartir la conexión a Internet.

DSL

Con DSL, las señales de voz y de datos se transportan en frecuencias diferentes por los cables telefónicos de cobre. Se utiliza un filtro para evitar que las señales de DSL interfieran en las señales telefónicas. En la Figura 2, se muestra un filtro para DSL. Conecte el filtro a un jack telefónico y conecte el teléfono al filtro.

El módem DSL no precisa un filtro. Las frecuencias del teléfono no afectan al módem DSL. Al igual que un módem por cable, un módem DSL se puede conectar directamente a la computadora, o bien puede conectarse a un dispositivo de red para compartir la conexión a Internet con varias computadoras.

ISDN

ISDN constituye otro ejemplo de banda ancha. ISDN emplea varios canales y puede transportar diversos tipos de servicios; por lo tanto, se considera un tipo de banda ancha. ISDN puede transmitir voz, vídeo y datos.

Satélite

La banda ancha por satélite es un método alternativo para los clientes que no pueden obtener conexiones por cable o DSL. Una conexión por satélite no precisa una línea telefónica ni un cable, pero emplea una antena parabólica para la comunicación bidireccional. Por lo general, las velocidades de descarga son de hasta 500 Kbps; las cargas se realizan a aproximadamente 56 Kbps. Se requiere tiempo para que la señal de la antena parabólica se transmita a su proveedor de servicios de Internet (ISP) a través del satélite que gira alrededor de la Tierra.

Las personas que viven en zonas rurales usan con frecuencia la banda ancha por satélite porque necesitan una conexión más veloz que la conexión de acceso telefónico y no disponen de otro tipo de conexión de banda ancha.

Tecnologías de banda ancha



8.10 Identificación de nombres, propósitos y características de otras tecnologías que se utilizan para establecer la conectividad
8.10.4 Definición de VoIP

Voz sobre IP (VoIP) es un método para transferir las llamadas telefónicas mediante redes de datos e Internet. VoIP convierte las señales analógicas de nuestras voces en información digital que se transporta en paquetes IP. VoIP también puede utilizar una red IP existente para ofrecer acceso a la red telefónica pública conmutada (PSTN).

Cuando utiliza VoIP, usted depende de una conexión a Internet. Esto puede ser una desventaja si se produce una interrupción en el servicio de conexión a Internet. Cuando se produce una interrupción en el servicio, el usuario no puede realizar llamadas telefónicas.

Teléfonos VoIP



8.11 Identificación y aplicación de las técnicas comunes de mantenimiento preventivo utilizadas para las redes

Existen técnicas comunes de mantenimiento preventivo que se deben usar de manera continua para que una red funcione correctamente. En una organización, si una computadora no funciona bien, por lo general, sólo un usuario se ve afectado. Pero si la red funciona mal, no podrán trabajar muchos usuarios, o ninguno de ellos podrá hacerlo.

Uno de los problemas más grandes que presentan los dispositivos de red, en particular en la sala de servidores, es el calor. Los dispositivos de red, como computadoras, hubs y switches, no funcionan correctamente cuando se recalientan. Por lo general, el calor excesivo se genera por el polvo acumulado y los filtros de aire sucios. El polvo que se junta dentro de los dispositivos de red y sobre ellos impide la circulación adecuada de aire fresco y, a veces, obstruye los ventiladores. Es importante mantener las salas de red limpias y cambiar los filtros de aire con frecuencia. También se recomienda contar con filtros de repuesto para un mantenimiento rápido.

El mantenimiento preventivo implica la comprobación de los diversos componentes de una red para observar si están deteriorados. Compruebe el estado de los cables de la red, ya que suele ocurrir que alguien los cambie de lugar, los desconecte o los patee. Muchos de los problemas de red se pueden deber a un cable dañado. Debe reemplazar todos los cables que tengan hilos expuestos, estén muy retorcidos o estén doblados.

Rotule los cables. Esta práctica le ahorrará tiempo en la resolución de problemas. Consulte los diagramas de cableado y siempre siga con los lineamientos de rotulación de cables de su empresa.

Mantenimiento preventivo de redes



8.12 Resolución de problemas en una red

Los problemas de red pueden ser simples o complejos. Para evaluar la complejidad del problema, debe determinar la cantidad de computadoras conectadas en la red que tienen el problema.

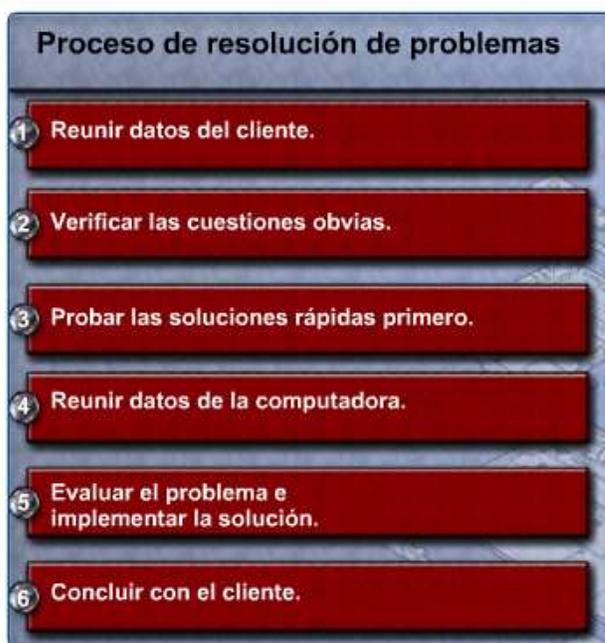
Si existe un problema en una computadora de la red, deberá iniciar el proceso de resolución de problemas en esa computadora. Si existe un problema en todas las computadoras de la red, deberá iniciar el proceso de resolución de problemas en la sala de red, donde estarán conectadas todas las computadoras. En su carácter de técnico, debe desarrollar un método sistemático y lógico para el diagnóstico de problemas en la red mediante la eliminación de un problema por vez.

Siga los pasos descritos en esta sección para definir, reparar y documentar el problema correctamente. En la Figura 1, se muestra el proceso de resolución de problemas.

Al completar esta sección, alcanzará los siguientes objetivos:

- * Revisar el proceso de resolución de problemas.
- * Identificar problemas de red y soluciones comunes.

Proceso de resolución de problemas



8.12 Resolución de problemas de red .

8.12.1 Revisión del proceso de resolución de problemas

Los problemas de red pueden originarse por una combinación de problemas de conectividad, software y hardware. Los técnicos en computación deben tener la capacidad de analizar el problema y determinar la causa del error para poder reparar el problema de red. Este proceso se denomina resolución de problemas.

El primer paso en el proceso de resolución de problemas es reunir los datos del cliente. Las figuras 1 y 2 enumeran las preguntas abiertas y cerradas para formular al cliente.

Una vez que haya hablado con el cliente, deberá verificar las cuestiones obvias. En la Figura 3, se enumeran algunas cuestiones relacionadas con las redes.

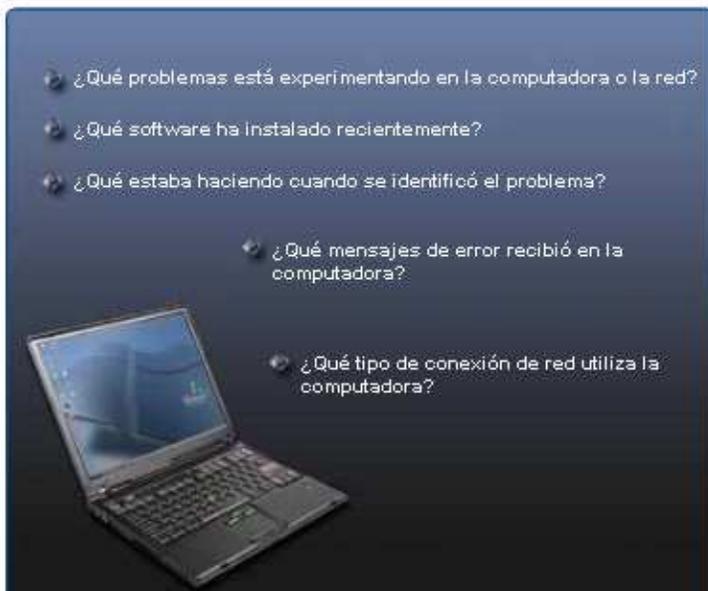
Una vez que las cuestiones obvias se hayan verificado, pruebe con algunas soluciones rápidas. En la Figura 4, se mencionan algunas soluciones rápidas para las redes.

Si las soluciones rápidas no permiten resolver el problema, deberá reunir datos de la computadora. En la Figura 5, se muestran diversos modos de reunir información sobre el problema de red.

En este momento, tendrá la información necesaria para evaluar el problema, buscar e implementar las soluciones posibles. En la Figura 6, se muestran recursos para soluciones posibles.

Una vez solucionado el problema de red, concluirá con el cliente. En la Figura 7, se muestra una lista de tareas necesarias para completar este paso.

Preguntas abiertas



Preguntas cerradas



Verificar las cuestiones obvias.

Proceso de resolución de problemas	
Reunir datos del cliente. Paso 1	<ul style="list-style-type: none">• Conexiones sueltas de cable• NIC instalada incorrectamente• Verifique las luces de enlace de la NIC• Baja intensidad de la señal inalámbrica• Dirección IP no válida
Verificar las cuestiones obvias. Paso 2	
Probar las soluciones rápidas primero. Paso 3	
Reunir datos de la computadora. Paso 4	
Evaluar el problema e implementar la solución. Paso 5	
Concluir con el cliente. Paso 6	

Probar las soluciones rápidas primero.

Proceso de resolución de problemas	
Reunir datos del cliente. Paso 1	<ul style="list-style-type: none">• Verifique que todos los cables estén conectados en la ubicación correcta.• Desconecte y vuelva a conectar los cables y los conectores.• Reinicie la computadora o el dispositivo de red.• Regístrese como un usuario diferente.• Repare o vuelva a habilitar la conexión de red.• Póngase en contacto con el administrador de red.
Verificar las cuestiones obvias. Paso 2	
Probar las soluciones rápidas primero. Paso 3	
Reunir datos de la computadora. Paso 4	
Evaluar el problema e implementar la solución. Paso 5	
Concluir con el cliente. Paso 6	

Reunir datos de la computadora.

Proceso de resolución de problemas	
Reunir datos del cliente. Paso 1	
Verificar las cuestiones obvias. Paso 2	
Probar las soluciones rápidas primero. Paso 3	
Reunir datos de la computadora. Paso 4	<p>Ping se utiliza para verificar la conectividad de red. Envía un paquete a la dirección especificada y espera una respuesta.</p> <p>Nslookup se utiliza para realizar consultas sobre los servidores de nombres de dominio Internet. El resultado es una lista de hosts de un dominio o la información de un host.</p> <p>Tracert se utiliza para determinar la ruta de los paquetes cuando se transfieren a través de la red. Muestra los lugares que presentan dificultades de comunicación entre su computadora y otra.</p> <p>Vista de la red se utiliza para mostrar una lista de computadoras de un grupo de trabajo. Muestra los recursos compartidos disponibles en una red.</p>
Evaluar el problema e implementar la solución. Paso 5	
Concluir con el cliente. Paso 6	

Evaluar el problema e implementar la solución.

Proceso de resolución de problemas	
Reunir datos del cliente. Paso 1	
Verificar las cuestiones obvias. Paso 2	
Probar las soluciones rápidas primero. Paso 3	
Reunir datos de la computadora. Paso 4	
Evaluar el problema e implementar la solución. Paso 5	<ul style="list-style-type: none"> • Experiencia en resolución de problemas • Otros técnicos • Búsqueda en Internet • Grupos de noticias • Preguntas frecuentes del fabricante • Manuales de la computadora • Manuales de los dispositivos • Foros en línea • Sitios Web técnicos
Concluir con el cliente. Paso 6	

Concluir con el cliente.

Proceso de resolución de problemas	
Reunir datos del cliente. Paso 1	• Analice con el cliente la solución implementada.
Verificar las cuestiones obvias. Paso 2	• Haga que el cliente verifique que el problema esté solucionado.
Probar las soluciones rápidas primero. Paso 3	• Proporcione documentación al cliente.
Reunir datos de la computadora. Paso 4	• Documente en la orden de trabajo y en el diario del técnico los pasos realizados para solucionar el problema.
Evaluar el problema e implementar la solución. Paso 5	• Documente todos los componentes utilizados en la reparación.
Concluir con el cliente. Paso 6	• Documente el tiempo que llevó resolver el problema.

8.12 Resolución de problemas de red

8.12.2 Identificación de problemas de red y soluciones comunes

Los problemas en la red pueden atribuirse a problemas de conectividad, software y hardware, o bien, a una combinación de los tres. Usted resolverá algunos tipos de problemas en la red con más frecuencia que otros. La Figura 1 contiene un cuadro con los problemas de red y soluciones comunes.

Problemas y soluciones comunes

Sintoma del problema	Solución posible
La computadora no se puede conectar a un sitio Web conocido.	Verifique la configuración DNS o la configuración del firewall de hardware y software.
La dirección IP de la computadora es 169.254.x.x.	Verifique que el servidor de DHCP esté funcionando correctamente y que se pueda hacer ping.
La computadora no se puede conectar a la red.	Verifique la existencia de cables de red sueltos.
La computadora no puede imprimir con la impresora de red.	Verifique los permisos del usuario y el estado de la impresora de red.

8.13 Resumen

Este capítulo le presentó los conceptos básicos sobre networking, los beneficios de tener una red y las maneras de conectar computadoras a una red. Los distintos aspectos de resolución de problemas en una red se analizaron con ejemplos de cómo analizar e implementar soluciones simples. Es importante recordar los siguientes conceptos de este capítulo:

- * Una red de computadoras se compone de dos o más computadoras que comparten datos y recursos.
- * Una red de área local (LAN) es un grupo de computadoras interconectadas que se encuentran bajo el mismo control administrativo.
- * Una red de área extensa (WAN) es una red que conecta redes LAN que se encuentran en ubicaciones geográficamente separadas.
- * En una red peer-to-peer, los dispositivos están conectados directamente entre sí. Una red peer-to-peer es fácil de instalar y no precisa ningún equipo adicional ni un administrador dedicado. Los usuarios controlan sus propios recursos, y una red funciona mejor con pocas computadoras. Una red cliente/servidor utiliza un sistema dedicado que actúa como el servidor. El servidor responde las solicitudes que realizan los usuarios o clientes conectados a la red.
- * Una LAN utiliza una conexión directa de una computadora a otra. Es adecuada para un área pequeña, como una casa, un edificio o una escuela. Una WAN utiliza líneas de comunicación seriales, punto a punto o punto a multipunto para establecer comunicación en distancias mayores. Una WLAN emplea tecnología inalámbrica para conectar los dispositivos entre sí.

* La topología de la red define el modo en que se conectan computadoras, impresoras y otros dispositivos. La topología física describe el diagrama del cableado y los dispositivos, así como las rutas utilizadas por las transmisiones de datos. La topología lógica es la ruta en la que viajan las señales de un punto a otro. Entre las topologías, se incluyen topologías de bus, estrella, anillo y malla.

* Los dispositivos de red se utilizan para conectar computadoras y dispositivos periféricos de manera que puedan comunicarse. Entre ellos se incluyen hubs, puentes, switches, routers y dispositivos multipropósito. El tipo de dispositivo implementado depende del tipo de red.

* Los medios de red pueden definirse como los medios por los cuales las señales o los datos se envían de una computadora a otra. Las señales pueden transmitirse por cable o por medios inalámbricos. Los tipos de medios explicados fueron: cableado coaxial, de par trenzado, de fibra óptica y radiofrecuencias.

* En la actualidad, la arquitectura Ethernet es el tipo más común de arquitectura LAN. La arquitectura se refiere a la estructura general de un sistema de comunicación o de computación. Determina las capacidades y las limitaciones del sistema. La arquitectura Ethernet se basa en el estándar IEEE 802.3. El estándar IEEE 802.3 especifica que una red implementa el método de control de acceso CSMA/CD.

* El modelo de referencia OSI es un marco estándar de la industria y se utiliza para dividir las funciones de red en siete capas distintas. Estas capas son: aplicación, presentación, sesión, transporte, red, enlace de datos y capa física. Es importante comprender el propósito de cada una de las capas.

* El suite de protocolos TCP/IP se ha transformado en el estándar predominante para Internet. TCP/IP representa un conjunto de estándares públicos que especifican cómo los paquetes de información se intercambian entre computadoras a través de una o más redes.

* Una tarjeta de interfaz de red (NIC) es un dispositivo que se conecta a una motherboard y proporciona puertos para las conexiones de cables de red. Es la interfaz de la computadora con la LAN.

* Un módem es un dispositivo electrónico que se utiliza para comunicaciones entre computadoras mediante líneas telefónicas. Permite la transferencia de datos entre una computadora y otra. El módem convierte los datos orientados a bytes en streams de bits en serie. Todos los módems precisan un software para controlar la sesión de comunicación. El conjunto de comandos que utiliza la mayoría de los elementos de software del módem se conoce como conjunto de comandos compatibles con Hayes.

* Los tres tipos de transmisión para el envío de señales mediante canales de datos son: simplex, half-duplex y full-duplex. La tecnología de red full-duplex mejora el rendimiento ya que se pueden enviar y recibir datos de manera simultánea. DSL, módem por cable bidireccional y otras tecnologías de banda ancha funcionan en modo full-duplex.

* Se debe realizar mantenimiento a los medios y dispositivos de red, como los componentes de computadoras. Es importante limpiar los equipos periódicamente y utilizar un método preventivo para evitar problemas. Repare o cambie el equipo averiado para evitar el tiempo de inactividad.

* Al resolver problemas de red, escuche lo que el cliente le dice para poder formular preguntas abiertas y cerradas que lo ayudarán a determinar por dónde deberá comenzar a corregir el problema. Verifique las cuestiones obvias e intente soluciones rápidas antes de profundizar en el proceso de resolución de problemas.