

JUAN CARLOS MATA GUTIERREZ

SISTEMAS COMPUTACIONALES

CCENT/CCNA ICND1 640-822 Official Cert Guide Third Edition

Capítulo 1-6

Capítulo 1 introducción de redes informáticas

Este capítulo le brinda una perspectiva alegre sobre las redes, cómo fueron originalmente creadas y por qué las redes funcionan como lo hacen.

De manera similar, un empleado de una empresa o un estudiante de una universidad ve el mundo como una conexión a través de un enchufe de pared. Normalmente, esta conexión utiliza un tipo de red de área local (LAN) denominada Ethernet. En lugar de necesitar un cable módem, la PC se conecta directamente a un

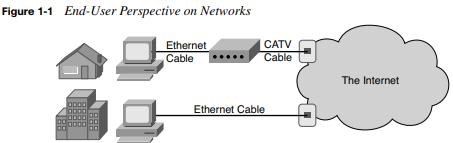
Enchufe estilo Ethernet en una placa de pared (el enchufe es muy parecido al enchufe típico que se usa hoy en día para el cableado telefónico, pero el conector es un poco más grande). Al igual que con Internet por cable de alta velocidad

Conexiones, la conexión Ethernet no requiere que el usuario de la PC haga nada primero para conectarse a la red—siempre está ahí esperando ser utilizada, similar a la toma de corriente.

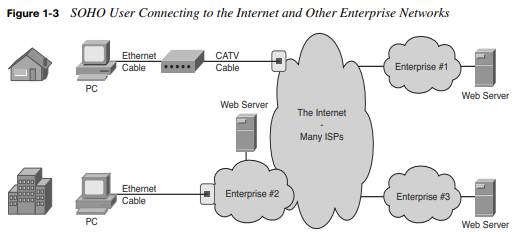
Desde la perspectiva del usuario final, ya sea en casa, en el trabajo o en la escuela, lo que sucede detrás del enchufe de pared es mágico. Así como la mayoría de la gente no entiende realmente cómo funcionan los automóviles, cómo funcionan los televisores, etc., la mayoría de las personas que usan las redes no entienden cómo funcionan.

¡Tampoco quieren! Pero si ha leído tanto en el Capítulo 1, obviamente tiene un poco más de interés en las redes que un usuario final típico. Al final de este libro, tendrá una comprensión bastante completa de lo que hay detrás de ese enchufe de pared en ambos casos. se muestra en la Figura 1-1.

Los exámenes CCNA, y en particular el examen ICND1 (640-822), se centran en dos ramas principales de conceptos, protocolos y dispositivos de redes. Una de estas dos ramas principales se llama redes empresariales. Una red empresarial es una red creada por una corporación, o empresa, con el fin de permitir que sus empleados se comuniquen.



La segunda rama principal de redes cubierta en el examen ICND1 se llama oficina pequeña/ oficina en casa, o SOHO. Esta rama de las redes utiliza los mismos conceptos, protocolos y dispositivos utilizados para crear redes empresariales, además de algunas características adicionales que no son necesario para las empresas. La red SOHO permite a un usuario conectarse a Internet usando una PC y cualquier conexión a Internet, como la conexión a Internet por cable de alta velocidad que se muestra en la Figura 1-1. Debido a que la mayoría de las redes empresariales también se conectan a Internet, SOHO el usuario puede sentarse en casa o en una oficina pequeña y comunicarse con los servidores de la empresa red, así como con otros hosts en Internet. La figura 1-3 muestra el concepto.



Capítulo 2 El TCP/IP y Modelos OSI

Los exámenes CCNA incluyen una cobertura detallada de un modelo de red: Protocolo de control de transmisión/Protocolo de Internet (TCP/IP). TCP/IP es el modelo de red más utilizado en la historia de las redes. Puede encontrar soporte para TCP/IP en prácticamente todos los sistemas operativos (SO) de computadora que existen hoy en día, desde teléfonos móviles hasta computadoras centrales. Todas las redes creadas con productos de Cisco en la actualidad admiten TCP/IP.

Y como era de esperar, los exámenes CCNA se centran en gran medida en TCP/IP.

El examen ICND1, y el examen ICND2 en pequeña medida, también cubren un segundo modelo de red, denominado modelo de referencia de interconexión de sistemas abiertos (OSI). Históricamente, OSI fue el primer gran esfuerzo para crear un modelo de red independiente del proveedor. Debido a ese momento, muchos de los términos que se usan hoy en redes provienen del modelo OSI, por lo que la sección de este capítulo sobre OSI analiza OSI y la terminología relacionada.

Modelo de red CP/IP

Un modelo de red, a veces también llamado arquitectura de red o modelo de red, se refiere a un conjunto completo de documentos. Individualmente, cada documento describe una pequeña función requerida para una red; colectivamente, estos documentos definen todo lo que debe suceder para que una red informática funcione. Algunos documentos definen un protocolo, que es un conjunto de reglas lógicas que los dispositivos deben seguir para comunicarse. Otros documentos definen algunos requisitos físicos para la creación de redes.

Puede pensar en un modelo de red como piensa en un plano arquitectónico para construir una casa.

Además, las diferentes personas que construyen la casa utilizando el plano, como enmarcadores, electricistas, albañiles, pintores, etc., saben que si siguen el plano, su parte del trabajo no debería causar problemas a los demás trabajadores.

De manera similar, podría construir su propia red (escribir su propio software, construir sus propias tarjetas de red, etc.) para crear una red. Sin embargo, es mucho más fácil simplemente comprar y usar productos que ya se ajustan a algún modelo o modelo de red bien conocido.

Debido a que los proveedores de productos de red construyen sus productos con algún modelo de red en mente, sus productos deberían funcionar bien juntos.

Descripción general del modelo de red TCP/IP

El modelo TCP/IP define y hace referencia a una gran colección de protocolos que permiten que las computadoras se comuniquen. Para definir un protocolo, TCP/IP utiliza documentos llamados Solicitudes

para comentarios (RFC). (Puede encontrar estos RFC utilizando cualquier motor de búsqueda en línea). El modelo TCP/IP también evita repetir el trabajo ya realizado por algún otro organismo de estándares o consorcio de proveedores al simplemente referirse a los estándares o protocolos creados por esos grupos.

Por ejemplo, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define las LAN Ethernet; el modelo TCP/IP no define Ethernet en los RFC, pero se refiere a IEEE Ethernet como una opción.

Se puede hacer una comparación fácil entre teléfonos y computadoras que usan TCP/IP. .

De manera similar, cuando compra una computadora nueva hoy, implementa el modelo TCP/IP hasta el punto de que generalmente puede sacar la computadora de la caja, conectar todos los cables correctos, encenderla y conectarla a la red. Puede usar un navegador web para conectarse a su favorito

sitio web. ¿Cómo? Bueno, el sistema operativo de la computadora implementa partes del modelo TCP/IP. La tarjeta Ethernet, o tarjeta LAN inalámbrica, integrada en la computadora implementa algunos estándares LAN a los que hace referencia el modelo TCP/IP. En resumen, los proveedores que crearon el hardware y software implementado TCP/IP.

Modelo de red OSI

En un momento de la historia del modelo OSI, muchas personas pensaron que OSI ganaría la batalla de los modelos de redes discutidos anteriormente. Si eso hubiera ocurrido, en lugar de ejecutar TCP/IP en todas las computadoras del mundo, esas computadoras estarían ejecutando OSI.

Sin embargo, OSI no ganó esa batalla. De hecho, OSI ya no existe como un modelo de red que podría usarse en lugar de TCP/IP, aunque todavía existen algunos de los protocolos originales a los que hace referencia el modelo OSI.

Entonces, ¿por qué OSI está incluso en este libro? Terminología. Durante esos años en los que muchas personas pensaron que el modelo OSI se convertiría en un lugar común en el mundo de las redes (principalmente a fines de la década de 1980 y principios de la de 1990), muchos proveedores y documentos de protocolo comenzaron a usar terminología del modelo OSI. Esa terminología permanece hoy. Por lo tanto, si bien nunca necesitará trabajar con una computadora que use OSI, para comprender la terminología moderna de redes, debe comprender algo acerca de OSI.

Comparando OSI y TCP/IP

El modelo OSI tiene muchas similitudes con el modelo TCP/IP desde un punto de vista conceptual básico.

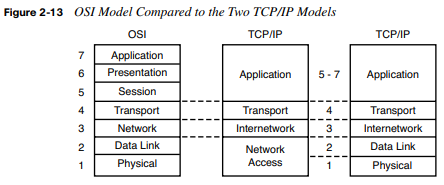
Perspectiva. Tiene (siete) capas, y cada capa define un conjunto de funciones de red típicas. Al igual que con TCP/IP, cada una de las capas OSI hace referencia a múltiples protocolos y estándares.

Que implementan las funciones especificadas por cada capa. En otros casos, al igual que para TCP/IP, los comités OSI no crearon nuevos protocolos o estándares, sino que hicieron referencia a otros protocolos que ya estaban definidos. Por ejemplo, el IEEE define los estándares de Ethernet, por lo que los comités de OSI no perdieron tiempo especificando un nuevo tipo de Ethernet; simplemente se refería a los estándares IEEE Ethernet.

Hoy en día, el modelo OSI se puede utilizar como estándar de comparación con otros modelos de redes.

La Figura 2-13 compara el modelo OSI de siete capas con el de cuatro y cinco capas.

Modelos TCP/IP.



Capítulo 3 Fundamentos de LANs

Una red empresarial típica consta de varios sitios. Los dispositivos del usuario final se conectan a una LAN, lo que permite que las computadoras locales se comuniquen entre sí. Además, cada sitio tiene un enrutador que se conecta tanto a la LAN como a una red de área amplia (WAN), con la

WAN que proporciona conectividad entre los distintos sitios. Con enrutadores y una WAN, las computadoras en diferentes sitios también pueden comunicarse.

Este capítulo describe los conceptos básicos de cómo crear LAN en la actualidad, con el Capítulo 4, "Fundamentos de WAN", que describe los conceptos básicos de creación de WAN. Ethernet es el rey indiscutible de los estándares LAN en la actualidad. Históricamente hablando, existían varios estándares de LAN en competencia, incluidos Token Ring, Interfaz de datos distribuidos por fibra (FDDI) y

Modo de transferencia asíncrono (ATM). Eventualmente, Ethernet ganó sobre todos los estándares de LAN de la competencia, de modo que hoy en día, cuando piensa en LAN, nadie se pregunta de qué tipo: es Ethernet.

Una descripción general de las LAN Ethernet moderno

El término Ethernet hace referencia a una familia de estándares que, en conjunto, definen las capas de enlace físico y de datos del tipo de LAN más popular del mundo. Los diferentes estándares varían en cuanto a la velocidad admitida, siendo comunes en la actualidad velocidades de 10 megabits por segundo (Mbps), 100 Mbps y 1000 Mbps (1 gigabit por segundo o Gbps). Los estándares también difieren en cuanto a los tipos de cableado y la longitud permitida del cableado. Por ejemplo, los estándares de Ethernet más utilizados permiten el uso de cableado de par trenzado sin blindaje (UTP) económico, mientras que otros estándares exigen un cableado de fibra óptica más costoso. El cableado de fibra óptica puede valer la pena en algunos casos, porque el cableado es más seguro y permite distancias mucho más largas entre dispositivos. Para admitir las necesidades muy variadas para construir una LAN (necesidades de diferentes velocidades, diferentes tipos de cableado (compensando los requisitos de distancia frente al costo) y otros factores), se han desarrollado muchas variaciones de los estándares de Ethernet. sido creado.

Los estándares originales de Ethernet: 10BASE2 y 10BASE5

Ethernet se entiende mejor considerando primero las dos primeras especificaciones de Ethernet, 10BASE5 y 10BASE2. Estas dos especificaciones de Ethernet definieron los detalles de las capas de enlace físico y de datos de las primeras redes Ethernet. (10BASE2 y 10BASE5 difieren en sus detalles de cableado, pero para la discusión en este capítulo, puede considerar que se comportan de manera idéntica). Con estas dos especificaciones, el ingeniero de red instala una serie de cables coaxiales que conectan cada dispositivo en la red Ethernet. No hay concentrador, interruptor o panel de cableado. Ethernet consta únicamente de las NIC de Ethernet colectivas en las computadoras y el cableado coaxial. La serie de cables crea un circuito eléctrico, llamado bus, que se comparte entre todos los dispositivos de Ethernet. Cuando una computadora quiere enviar algunos bits a otra computadora en el bus, envía una señal eléctrica y la electricidad se propaga a todos los dispositivos en la red Ethernet.

Protocolos de enlace de datos Ethernet

Una de las fortalezas más significativas de la familia de protocolos Ethernet es que estos protocolos utilizan el mismo conjunto pequeño de estándares de enlace de datos. Por ejemplo, el direccionamiento de Ethernet funciona igual en todas las variaciones de Ethernet, incluso desde 10BASE5, hasta Ethernet de 10 Gbps, incluidos los estándares de Ethernet que utilizan otros tipos de cableado además de UTP. Además, el algoritmo CSMA/CD es técnicamente una parte de la capa de enlace de datos, y nuevamente se aplica a la mayoría de los tipos de Ethernet, a menos que se haya desactivado.

Esta sección cubre la mayoría de los detalles de los protocolos de enlace de datos de Ethernet, en particular, el direccionamiento de Ethernet, la trama, la detección de errores y la identificación del tipo de datos dentro de la trama de Ethernet.

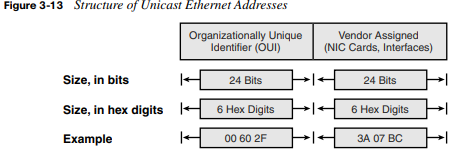
Direccionamiento Ethernet

El direccionamiento de LAN Ethernet identifica dispositivos individuales o grupos de dispositivos en una LAN. Cada dirección tiene una longitud de 6 bytes, generalmente se escribe en hexadecimal y, en los dispositivos Cisco, generalmente se escribe con puntos que separan cada conjunto de cuatro dígitos hexadecimales.

El IEEE define el formato y la asignación de direcciones LAN. El IEEE requiere direcciones MAC de unidifusión únicas a nivel mundial en todas las tarjetas de interfaz LAN. (IEEE las llama direcciones MAC porque los protocolos MAC como IEEE 802.3 definen los detalles de direccionamiento).

Para garantizar una dirección MAC única, los fabricantes de tarjetas Ethernet codifican la dirección MAC en la tarjeta, generalmente en un chip ROM. La primera mitad de la dirección identifica al fabricante de la tarjeta. Este código, que el IEEE asigna a cada fabricante, se denomina identificador único organizativo (OUI). Cada fabricante asigna una dirección MAC con su propio OUI como la primera mitad de la dirección, y a la segunda mitad de la dirección se le asigna un número que este fabricante nunca ha usado en otra tarjeta.

La figura 3-13 muestra la estructura.



Las direcciones de grupo identifican más de una tarjeta de interfaz LAN. El IEEE define dos generales

Categorías de direcciones de grupo para Ethernet:

■ Direcciones de difusión: las direcciones MAC del grupo IEEE más utilizadas, las

Dirección de difusión, tiene un valor de FFFF.FFFF.FFFF (notación hexadecimal). La dirección de difusión implica que todos los dispositivos de la LAN deben procesar la trama.

■ Direcciones de multidifusión: las direcciones de multidifusión se utilizan para permitir que un subconjunto de dispositivos en una LAN se comunique. Cuando IP multidifunde a través de Ethernet, las direcciones MAC de multidifusión utilizadas por IP siguen este formato: 0100.5exx.xxxx, donde se puede usar cualquier valor en la última mitad de la dirección.

Capítulo 4 Fundamentos de WANs

La capa física OSI, o Capa 1, define los detalles de cómo mover datos de un dispositivo a otro. De hecho, mucha gente piensa en la capa 1 de OSI como "bits de envío". Las capas superiores encapsulan los datos, como se describe en el Capítulo 2, “La red TCP/IP y OSI.

Modelos. No importa lo que hagan las otras capas OSI, eventualmente el remitente de los datos necesita transmitir los bits a otro dispositivo. La capa física OSI define los estándares y protocolos utilizados para crear la red física y enviar los bits a través de esa red.

Conexiones WAN desde el punto de vista del cliente

Los conceptos detrás de una conexión punto a punto son simples. Sin embargo, para comprender completamente lo que hace el proveedor de servicios para construir su red para respaldar su línea punto a punto, necesitará pasar mucho tiempo estudiando y aprendiendo tecnologías fuera del alcance.

Del examen ICND1. Sin embargo, la mayor parte de lo que necesita saber sobre las WAN para el examen ICND1 se relaciona con cómo se implementan las conexiones WAN entre la compañía telefónica y el sitio del cliente. En el camino, deberá aprender un poco sobre la terminología utilizada por el proveedor.

Estándares de cableado WAN

Cisco ofrece una gran variedad de diferentes tarjetas de interfaz WAN para sus enrutadores, incluidas interfaces seriales síncronas y asíncronas. Para cualquiera de los enlaces serie punto a punto o enlaces Frame Relay de este capítulo, el enrutador utiliza una interfaz que admite la comunicación síncrona.

**Capa 2 de OSI para WAN punto a punto**

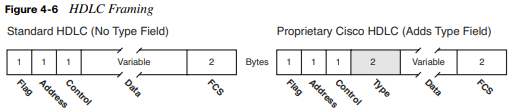
Los protocolos WAN utilizados en los enlaces serie punto a punto proporcionan la función básica de entrega de datos a través de ese enlace. Los dos protocolos de capa de enlace de datos más populares utilizados en enlaces punto a punto son el control de enlace de datos de alto nivel (HDLC) y el protocolo punto a punto (PPP).

HDLC

Debido a que los enlaces punto a punto son relativamente simples, HDLC solo tiene una pequeña cantidad de trabajo por hacer. En particular, HDLC necesita determinar si los datos pasaron el enlace sin ningún error; HDLC descarta el marco si ocurrieron errores. Además, HDLC necesita identificar el tipo de paquete dentro de la trama HDLC para que el dispositivo receptor conozca el tipo de paquete. Para lograr el objetivo principal de entregar datos a través del enlace y verificar errores e identificar el tipo de paquete, HDLC define la trama. El encabezado HDLC incluye una dirección

y un campo Tipo de protocolo, con el tráiler que contiene un campo de secuencia de verificación de tramas (FCS). La figura 4-6 describe el marco HDLC estándar y el marco HDLC que es propiedad de Cisco.

HDLC define un campo de dirección de 1 byte, aunque en los enlaces punto a punto no es realmente necesario.



CAPITULO 5 FUNDAMENTOS DEL DIRECCIONAMIENTO Y ENRUTAMIENTO IPV4

La capa física OSI (Capa 1) define cómo transmitir bits a través de un tipo particular de red física. La capa de enlace de datos OSI (capa 2) define la trama, el direccionamiento, la detección de errores y las reglas sobre cuándo usar el medio físico. Aunque son importantes, estas dos capas no definen cómo entregar datos entre dispositivos que existen lejos uno del otro, con muchas redes físicas diferentes ubicadas entre las dos computadoras. Este capítulo explica la función y el propósito de la capa de red OSI (Capa 3): la entrega de datos de extremo a extremo entre dos computadoras. Independientemente del tipo de red física a la que esté conectado cada equipo terminal y de los tipos de redes físicas utilizadas entre los dos equipos, la capa de red define cómo reenviar o enrutar los datos entre los dos equipos.

Los protocolos equivalentes a la Capa 3 de OSI definen cómo se pueden entregar los paquetes desde la computadora que crea el paquete hasta la computadora que necesita recibir el paquete. Para alcanzar ese objetivo, un protocolo de capa de red OSI define las siguientes características:

Enrutamiento: el proceso de reenvío de paquetes (PDU de capa 3).

Direccionamiento lógico: Direcciones que se pueden utilizar independientemente del tipo de redes físicas utilizadas, proporcionando a cada dispositivo (al menos) una dirección. El direccionamiento lógico permite que el proceso de enrutamiento identifique el origen y el destino de un paquete.

Protocolo de enrutamiento: un protocolo que ayuda a los enrutadores al aprender dinámicamente sobre los grupos de direcciones en la red, lo que a su vez permite que el proceso de enrutamiento (reenvío) funcione bien.

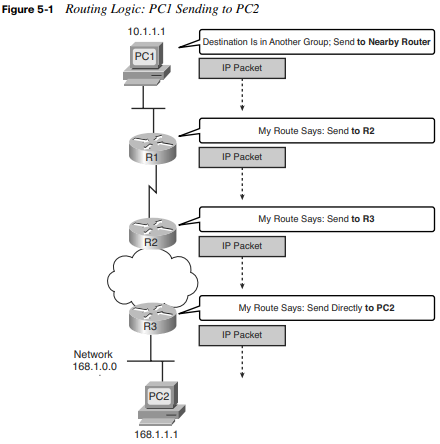
Otras utilidades: la capa de red también se basa en otras utilidades. Para TCP/IP, estas utilidades incluyen Sistema de nombres de dominio (DNS), Protocolo de configuración dinámica de host (DHCP), Protocolo de resolución de direcciones (ARP) y ping.

Descripción general de las funciones de la capa de red

Un protocolo que define el enrutamiento y el direccionamiento lógico se considera un protocolo de capa de red o de capa 3. OSI define un protocolo único de Capa 3 llamado Servicios de red sin conexión (CLNS), pero, como es habitual con los protocolos OSI, rara vez se ve en las redes hoy en día. En el pasado reciente, es posible que haya visto muchos otros protocolos de capa de red, como el Protocolo de Internet (IP), el Intercambio de paquetes entre redes (IPX) de Novell o el Protocolo de entrega de datagramas (DDP) de AppleTalk. Hoy en día, el único protocolo de Capa 3 que se usa ampliamente es el protocolo de capa de red TCP/IP, específicamente, IP.

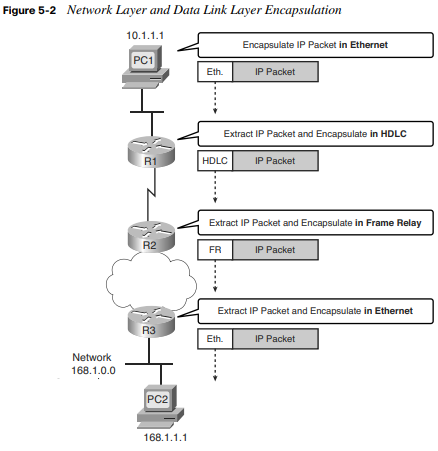
**Enrutamiento (reenvío)**

El enrutamiento se centra en la lógica de extremo a extremo del reenvío de datos. La Figura 5-1 muestra un ejemplo simple de cómo funciona el enrutamiento. La lógica ilustrada por la figura es relativamente simple. Para que la PC1 envíe datos a la PC2, debe enviar algo al enrutador R1, que lo envía al enrutador R2, luego al enrutador R3 y finalmente a la PC2. Sin embargo, la lógica utilizada por cada dispositivo a lo largo de la ruta varía ligeramente.



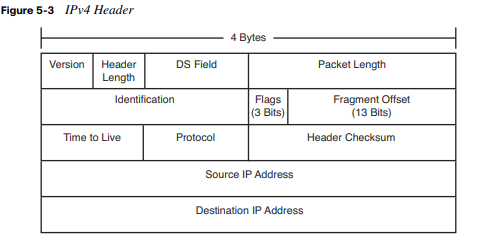
Interacción de la capa de red con la capa de enlace de datos

Cuando el protocolo de capa de red está procesando el paquete, decide enviar el paquete a la interfaz de red adecuada. Antes de que los bits reales puedan colocarse en esa interfaz física, la capa de red debe entregar el paquete a los protocolos de la capa de enlace de datos, que, a su vez, solicitan a la capa física que envíe los datos. Y como se describió en el Capítulo 3, "Fundamentos de las LAN", la capa de enlace de datos agrega el encabezado y el final apropiados al paquete, creando una trama, antes de enviar las tramas a través de cada red física. El proceso de enrutamiento reenvía el paquete, y solo el paquete, de un extremo a otro a través de la red, descartando los encabezados y los tráileres del enlace de datos en el camino. Los procesos de la capa de red entregan el paquete de extremo a extremo, utilizando encabezados de enlace de datos sucesivos y remolques solo para llevar el paquete al siguiente enrutador o host en la ruta. Cada capa de enlace de datos sucesiva simplemente lleva el paquete de un dispositivo al siguiente. La Figura 5-2 señala la lógica de encapsulación de claves en cada dispositivo, utilizando los mismos ejemplos que en la Figura 5-1.



Paquetes IP y el encabezado IP

Los paquetes IP encapsulados en las tramas de enlace de datos que se muestran en la Figura 5-2 tienen un encabezado IP, seguido de encabezados y datos adicionales. Como referencia, la Figura 5-3 muestra los campos dentro del encabezado IPv4 estándar de 20 bytes, sin campos de encabezado IP opcionales, como suele verse en la mayoría de las redes actuales.



Al igual que las direcciones de las calles postales, las direcciones de la capa de red se agrupan según la ubicación física en una red. Las reglas difieren para algunos protocolos de capa de red, pero con el direccionamiento IP, la primera parte de la dirección IP es la misma para todas las direcciones en un grupo.

Por ejemplo, en las Figuras 5-1 y 5-2, las siguientes convenciones de direccionamiento IP definen los grupos de direcciones IP (redes IP) para todos los hosts en esa interconexión de redes:

■ Hosts en la parte superior Ethernet: las direcciones comienzan con 10

■ Hosts en el enlace serial R1-R2: las direcciones comienzan con 168.10

■ Hosts en la red Frame Relay R2-R3: las direcciones comienzan con 168.11

■ Hosts en la parte inferior Ethernet: las direcciones comienzan con 168.1

Direccionamiento IP

El direccionamiento IP es absolutamente el tema más importante para los exámenes CCNA. Para cuando haya completado su estudio, debería sentirse cómodo y confiado en su comprensión de las direcciones IP, sus formatos, los conceptos de agrupación, cómo subdividir grupos en subredes, cómo interpretar la documentación para el direccionamiento IP de las redes existentes, etc. en. En pocas palabras, ¡es mejor que sepa direccionar y dividir en subredes! Esta sección presenta el direccionamiento IP y la división en subredes y también cubre los conceptos detrás de la estructura de una dirección IP, incluida la forma en que se relaciona con el enrutamiento IP.

Definiciones de direcciones IP

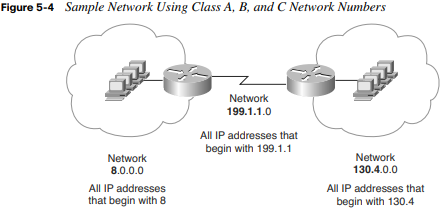
Si un dispositivo quiere comunicarse usando TCP/IP, necesita una dirección IP. Cuando el dispositivo tiene una dirección IP y el software y hardware adecuados, puede enviar y recibir paquetes IP. Cualquier dispositivo que pueda enviar y recibir paquetes IP se denomina host IP.

Las direcciones IP constan de un número de 32 bits, generalmente escrito en notación decimal con puntos. La parte "decimal" del término proviene del hecho de que cada byte (8 bits) de la dirección IP de 32 bits se muestra como su equivalente decimal. Los cuatro números decimales resultantes se escriben en secuencia, con "puntos" o puntos decimales, separando los números, de ahí el nombre decimal con puntos. Por ejemplo, 168.1.1.1 es una dirección IP escrita en formato decimal con puntos; la versión binaria real es

10101000 00000001 00000001 00000001.

Cómo se agrupan las direcciones IP

Las especificaciones originales para TCP/IP agrupaban las direcciones IP en conjuntos de direcciones consecutivas denominadas redes IP. Las direcciones en una sola red tienen el mismo valor numérico en la primera parte de todas las direcciones en la red. La Figura 5-4 muestra una interred simple que tiene tres redes IP separadas

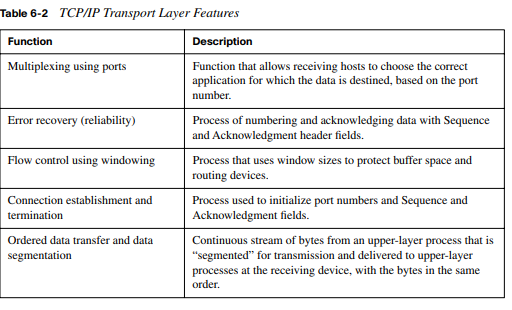


Capítulo 6 Fundamentos del tcp/ip, transporte, aplicaciones y seguridad.

La capa de transporte OSI (Capa 4) define varias funciones, las más importantes son la recuperación de errores y el control de flujo. Asimismo, los protocolos de la capa de transporte TCP/IP también implementan este mismo tipo de características. Tenga en cuenta que tanto el modelo OSI como el modelo TCP/IP llaman a esta capa la capa de transporte. Pero, como de costumbre, cuando se hace referencia al modelo TCP/IP, el nombre y el número de capa se basan en OSI, por lo que cualquier protocolo de capa de transporte TCP/IP se considera protocolo de capa 4.

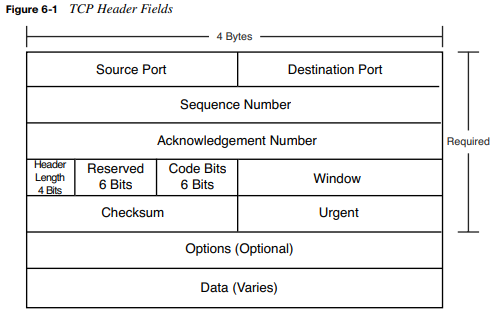
La diferencia clave entre TCP y UDP es que TCP brinda una amplia variedad de servicios a las aplicaciones, mientras que UDP no. Por ejemplo, los enrutadores descartan paquetes por muchas razones, incluidos errores de bits, congestión e instancias en las que no se conocen las rutas correctas. Como ya ha leído, la mayoría de los protocolos de enlace de datos notan errores (un proceso llamado detección de errores) pero luego descartan las tramas que tienen errores. TCP proporciona retransmisión (recuperación de errores) y ayuda para evitar la congestión (control de flujo), mientras que UDP no lo hace. Como un

Como resultado, muchos protocolos de aplicación optan por utilizar TCP.



Protocolo de Control de Transmisión

Cada aplicación TCP/IP generalmente elige usar TCP o UDP según los requisitos de la aplicación. Por ejemplo, TCP proporciona recuperación de errores, pero para hacerlo consume más ancho de banda y usa más ciclos de procesamiento. UDP no realiza la recuperación de errores, pero requiere menos ancho de banda y usa menos ciclos de procesamiento. Independientemente de cuál de los dos protocolos de capa de transporte TCP/IP elija usar la aplicación, debe comprender los conceptos básicos de cómo funciona cada uno de estos protocolos de capa de transporte.



Multiplexación mediante números de puerto TCP

TCP proporciona muchas características a las aplicaciones, a expensas de requerir un poco más de procesamiento y sobrecarga, en comparación con UDP. Sin embargo, TCP y UDP usan un concepto llamado multiplexación. Por lo tanto, esta sección comienza con una explicación de la multiplexación con TCP y UDP. Posteriormente, se exploran las características únicas de TCP.

La multiplexación por TCP y UDP implica el proceso de cómo piensa una computadora cuando recibe datos. La computadora puede estar ejecutando muchas aplicaciones, como un navegador web, un paquete de correo electrónico o una aplicación VoIP de Internet (por ejemplo, Skype). La multiplexación TCP y UDP permite que la computadora receptora sepa a qué aplicación darle los datos

Aplicaciones populares de TCP/IP

A lo largo de su preparación para los exámenes CCNA, se encontrará con una variedad de aplicaciones TCP/IP. Al menos debe conocer algunas de las aplicaciones que se pueden usar para ayudar a administrar y controlar una red.

La aplicación Word Wide Web (WWW) existe a través de navegadores web que acceden al contenido disponible en los servidores web. Aunque a menudo se considera una aplicación de usuario final, en realidad puede usar WWW para administrar un enrutador o conmutador. Habilitas una función de servidor web en el enrutador o conmutador y use un navegador para acceder al enrutador o conmutador

El Sistema de nombres de dominio (DNS) permite a los usuarios usar nombres para referirse a las computadoras, y el DNS se usa para encontrar las direcciones IP correspondientes. DNS también usa un modelo cliente/servidor, con servidores DNS controlados por personal de red, y las funciones de cliente DNS son parte de la mayoría de los dispositivos que usan TCP/IP en la actualidad. El cliente simplemente le pide al servidor DNS que proporcione la dirección IP que corresponde a un nombre dado.

El Protocolo simple de administración de redes (SNMP) es un protocolo de capa de aplicación que se usa específicamente para la administración de dispositivos de red. Por ejemplo, Cisco ofrece una gran variedad de productos de administración de redes, muchos de ellos en la administración de redes CiscoWorks. Familia de productos de software. Se pueden usar para consultar, compilar, almacenar y mostrar información sobre el funcionamiento de una red. Para consultar los dispositivos de red, el software CiscoWorks utiliza principalmente protocolos SNMP