24 DE FEBRERO DEL 2023
REDES DE COMPUTADORA

REPORTE DE LECTURA

NOMBRE DEL LIBRO

ICND1 OFFICIAL CERT-GUIDE THIRD EDITION.

NOMBRE DEL PROFESOR:
ISMAEL JIMÉNEZ SÁNCHEZ

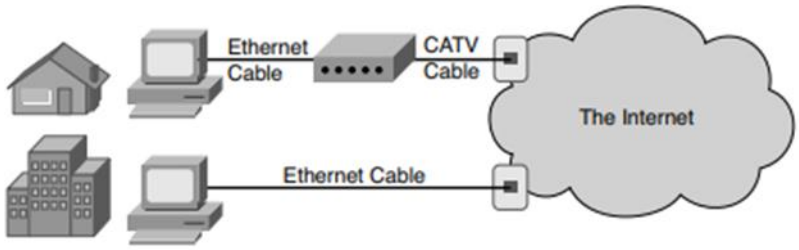
NOMBRE DEL ALUMNO:
BRAYAN ALEXIS MAAS CANCHE

- **Capítulo 1**

Perspectivas sobre la creación de redes

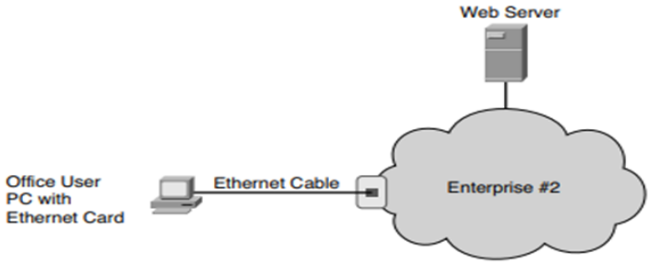
Recientemente ahora se está tomando en serio el aprendizaje sobe redes de computadoras esto es para que se pueda lograr con un poco de conocimiento lograr establecer una red de internet en ciertas áreas como empresas o tiendes entre otros. Como mucha gente, su perspectiva sobre las redes puede ser la de un usuario de la red, como opuesto al ingeniero de redes que construye redes. Para algunos, su visión de las redes podría basarse en cómo usa Internet, desde su casa, usando Internet de alta velocidad conexión.

Figure 1-1 *End-User Perspective on Networks*



Es claro que para entender sobre la estructura de una red como en el ejemplo de la figure 1-1 n donde muestra ambas perspectivas de trabajo en red. Se proyecta a un usuario común con internet que esta conectados por mediante cables de alta velocidad esté conectado mediante un módem estas épocas ya tienen fibra óptica para mayor velocidad y luego se conecta a un televisor por cable de Ethernet hacia una caja.

Figure 1-2 *An Example Representation of an Enterprise Network*



A continuación, ahora mostraremos otro tipo de presentación se muestra en la Figura 1-2, que ahora es de qué forma se comunica un servidor web a través de la red empresarial, de forma de una nube se representa una parte de una red.

Esto está guiado por el reglamento de cisco conceptos, con los protocolos ya establecidos con la normativa de cisco.

permite a un usuario conectarse a Internet utilizando Debido a que la mayoría de las redes empresariales también se conectan a Internet, un trabajador puede estar sentado en su casa o en una oficina pequeña y comunicarse con los servidores de la empresa gracias a los de proveedores de servicios de Internet (ISP). De hecho, el término en sí, Internet, se forma acortando la frase "redes interconectadas".

Para crear Internet, los ISP ofrecen acceso a Internet, por lo general mediante una línea de televisión por cable Ethernet, mediante la ayuda de un módem.

Cada empresa normalmente se conecta al menos a un ISP, utilizando conexiones permanentes generalmente llamados enlaces de red de área amplia (WAN). Finalmente, los ISP del mundo también conectarse entre sí. Estas redes interconectadas, desde el hogar más pequeño con una sola PC red, a teléfonos móviles y reproductores de MP3, a redes empresariales con miles de dispositivos: todos se conectan a Internet global.

- **Capítulo 2**

Las redes TCP/IP y OSI

Modelos

Puede pensar en un modelo de red como un conjunto de planos donde se muestra la estructura de cómo debería estar el cableado para una función correcta en el área de trabajo sin obstáculos de esta manera se podra construir su propia red, ya configurada con sus propias ip para mandar archivos entre ellos.

Temas de la Fundación

Modelo de red TCP/IP

Se 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.

Hoy en día, el mundo de las redes informáticas utiliza un modelo de red: TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet). Sin embargo, el mundo no siempre ha sido tan simple. Los proveedores crearon los primeros protocolos de red; estos protocolos admitían solo los de ese proveedor ordenadores.

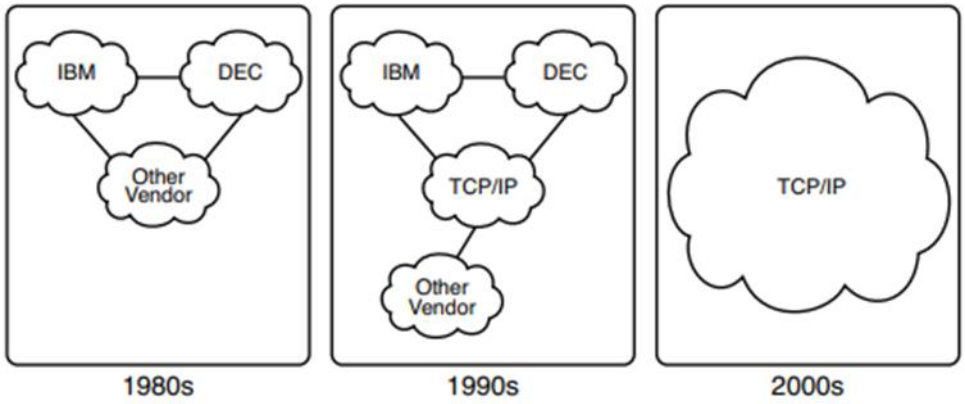
Comenzando a fines de la década de 1970, comenzando a trabajar en lo que se conocería como el modelo de red de interconexión de sistemas abiertos (OSI).

Modelo OSI: para estandarizar los protocolos de red de datos para permitir la comunicación entre todas computadoras en todo el planeta. ISO trabajó hacia esta ambiciosa y noble meta, con participantes de la mayoría de las naciones tecnológicamente desarrolladas en la Tierra participando en el proceso.

Durante la década de 1990, las empresas comenzaron a agregar OSI, TCP/IP o ambos a su empresa.

Redes, Sin embargo, a fines de la década de 1990, TCP/IP se había convertido en la opción común y OSI se cayó. General detrás de la empresa redes en esa década, todavía con redes basadas en múltiples modelos de redes, pero incluyendo TCP/IP. Aquí, en el siglo XXI, domina TCP/IP. Todavía existen modelos de red patentados, pero en su mayoría han sido descartados a favor de TCP/IP. El modelo OSI, cuyo desarrollo sufrido en parte debido a un proceso de estandarización formal más lento en comparación con TCP/IP.

Figure 2-1 *Historical Progression: Proprietary Models to the Open TCP/IP Model*



Descripción general del modelo de red TCP/IP

El modelo TCP/IP define y hace referencia a una gran colección de protocolos que permiten ordenadores para comunicarse. Para definir un protocolo, TCP/IP utiliza documentos llamados Solicitudes para comentarios (RFC).

El modelo TCP/IP también evita repetir el trabajo ya realizado por algún otro organismo de normalización o consorcio de proveedores simplemente refiriéndose a los estándares o protocolos creados por esos grupos.

Capa de aplicación TCP/IP

Los protocolos de capa de aplicación TCP/IP brindan servicios al software de aplicación que se ejecuta en un ordenador. La capa de aplicación no define la aplicación en sí, pero define servicios que necesitan las aplicaciones. Por ejemplo, el protocolo de aplicación HTTP define cómo la web los navegadores puede

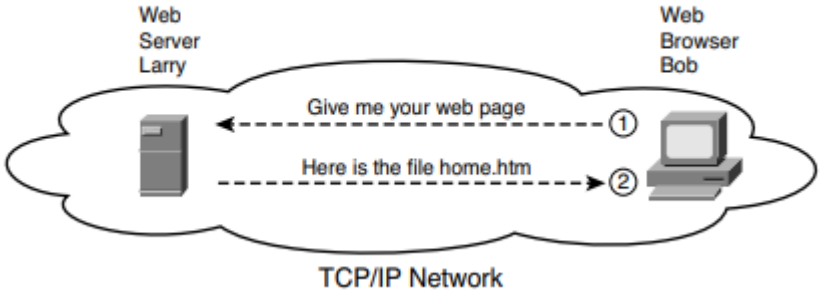
extraer el contenido de una página web desde un servidor web. En resumen, la aplicación La capa proporciona una interfaz entre el software que se ejecuta en una computadora y la red misma.

Descripción general de HTTP

¿Qué sucede realmente para permitir que esa página web aparezca en su navegador web?

Imagina que Bob abre su navegador. Su navegador ha sido configurado para preguntar automáticamente para el servidor web La página web predeterminada de Larry o la página de inicio. La lógica general se parece a la Figura 2-3.

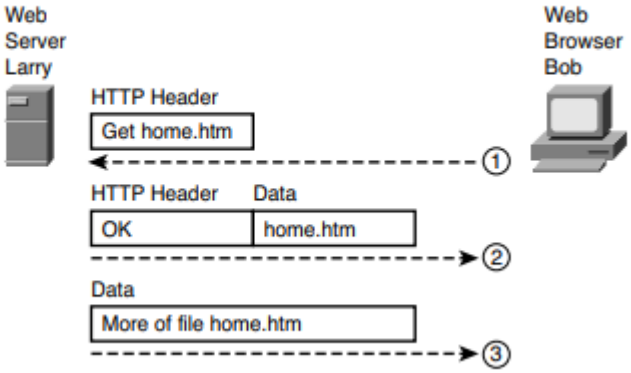
Figure 2-3 *Basic Application Logic to Get a Web Page*



Mecanismos del protocolo HTTP

Mirando más de cerca, este ejemplo muestra cómo las aplicaciones en cada computadora de punto final: específicamente, la aplicación de navegador web y la aplicación de servidor web—use un protocolo TCP/IP protocolo de la capa de aplicación.

Figure 2-4 *HTTP Get Request, HTTP Reply, and One Data-Only Message*



Capa de transporte TCP/IP

Aunque existen muchos protocolos de capa de aplicación TCP/IP, la capa de transporte TCP/IP incluye un número menor de protocolos. Las dos capas de

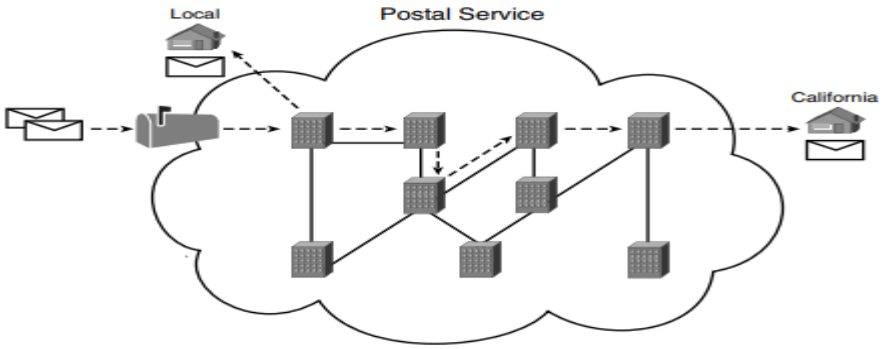
transporte más utilizadas los protocolos son el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario.

Los protocolos de la capa de transporte brindan servicios a los protocolos de la capa de aplicación que residen en uno. Capa superior en el modelo TCP/IP.

Capa de Internet TCP/IP

La capa de aplicación incluye muchos protocolos. La capa de transporte incluye menos, la mayoría en particular, TCP y UDP. La capa de Internet TCP/IP incluye una pequeña cantidad de protocolos, pero sólo un protocolo principal: el Protocolo de Internet (IP). De hecho, el nombre TCP/IP es simplemente los nombres de los dos protocolos más comunes (TCP e IP) separados por /a.

Figure 2-6 *Postal Service Forwarding (Routing) Letters*

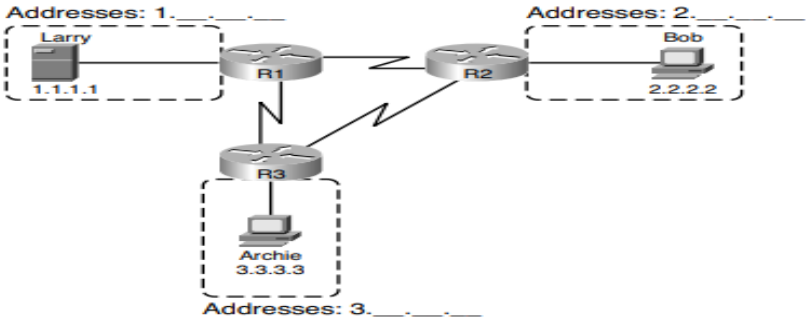


Las capas de aplicación y transporte de TCP/IP actúan como la persona que envía cartas a través del servicio Postal. Estas capas superiores funcionan de la misma manera independientemente de si el punto final las computadoras anfitrionas están en la misma LAN o están separadas por todo Internet. para enviar un mensaje, estas capas superiores le piden a la capa debajo de ellas, la capa de Internet, que entregue el mensaje.

Conceptos básicos de direccionamiento de protocolo de Internet

IP define direcciones por varias razones importantes. Primero, cada dispositivo que usa TCP/IP— cada host TCP/IP necesita una dirección única para que pueda identificarse en la red. IP también define cómo agrupar direcciones, al igual que el sistema postal agrupa direcciones basadas en códigos postales (como los códigos postales en los EE. UU.).

Figure 2-7 *Simple TCP/IP Network: Three Routers with IP Addresses Grouped*



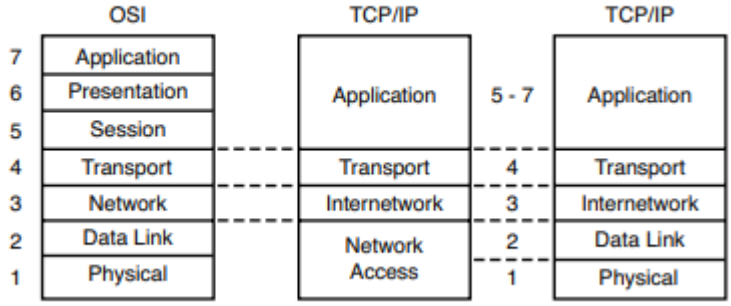
En un momento de la historia del modelo OSI, pensaron que OSI ganaría la batalla de los modelos de redes. Sin embargo, OSI no ganó esa batalla. De hecho, OSI ya no existe como un modelo de red que podría usarse en lugar de TCP/IP.

Comparando OSI y TCP/IP

El modelo OSI tiene muchas similitudes con el modelo TCP/IP desde una perspectiva conceptual básica. Tiene capas, y cada capa define un conjunto de funciones típicas de redes. Se refieren a múltiples protocolos y estándares que implementan las funciones especificadas por cada capa.

La Figura 2-13 compara el modelo OSI de siete capas con los modelos TCP/IP de cuatro y cinco capas.

Figure 2-13 *OSI Model Compared to the Two TCP/IP Models*



Describir protocolos haciendo referencia a las capas OSI

Los documentos de red suelen describir los protocolos y estándares TCP/IP haciendo referencia a las capas OSI, tanto por número de capa como por nombre de capa.

Aunque la capa de red OSI y la capa de Internet TCP/IP son similares, la figura no indica por qué son similares. Para apreciar por qué las capas TCP/IP corresponden a una capa OSI en particular, debe comprender mejor las capas

OSI. Aunque los detalles difieren significativamente, coincide con los objetivos generales y la intención de la capa de red de ambos.

Otro ejemplo, es que la capa de transporte TCP/IP define muchas funciones, incluida la recuperación de errores. La capa de transporte OSI también define estas mismas funciones, aunque con diferentes detalles y diferentes protocolos específicos. Como resultado, la industria de las redes dice que TCP esta basado en el modelo OSI.

Capas OSI y sus funciones

Una de las mejores formas de aprender sobre la función de las diferentes capas OSI es pensar en las funciones del modelo TCP/IP y correlacionarlas. Si utiliza el modelo TCP/IP de cinco capas, las cuatro capas inferiores de OSI y TCP/IP se correlacionan muy juntas.

La Tabla 2-4 define las funciones de las siete capas.

Table 2-4 *OSI Reference Model Layer Definitions*

Layer	Functional Description
7	Layer 7 provides an interface between the communications software and any applications that need to communicate outside the computer on which the application resides. It also defines processes for user authentication.
6	This layer's main purpose is to define and negotiate data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption is also defined by OSI as a presentation layer service.
5	The session layer defines how to start, control, and end conversations (called sessions). This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data.

Layer	Functional Description
4	Layer 4 protocols provide a large number of services, as described in Chapter 6, "Fundamentals of TCP/IP Transport, Applications, and Security." Although OSI Layers 5 through 7 focus on issues related to the application, Layer 4 focuses on issues related to data delivery to another computer (for instance, error recovery and flow control).
3	The network layer defines three main features: logical addressing, routing (forwarding), and path determination. Routing defines how devices (typically routers) forward packets to their final destination. Logical addressing defines how each device can have an address that can be used by the routing process. Path determination refers to the work done by routing protocols to learn all possible routes, and choose the best route.
2	The data link layer defines the rules that determine when a device can send data over a particular medium. Data link protocols also define the format of a header and trailer that allows devices attached to the medium to successfully send and receive data.
1	This layer typically refers to standards from other organizations. These standards deal with the physical characteristics of the transmission medium, including connectors, pins, use of pins, electrical currents, encoding, light modulation, and the rules for how to activate and deactivate the use of the physical medium.

Conceptos y beneficios de las capas OSI

Los modelos de red que dividen las funciones en diferentes capas permiten que un paquete de software o dispositivo de hardware implemente funciones desde una capa y suponga que otro software/hardware realizará las funciones definidas por las otras capas.

La siguiente lista resume los beneficios de las especificaciones de protocolo en capas:

- Menos complejo: los modelos de red dividen los conceptos en partes más pequeñas.
- Interfaces estándar: varios proveedores creen productos que cumplen una función particular.
- Más fácil de aprender: los humanos pueden debatir y aprender sobre los detalles de una especificación de protocolo.
- Más fácil de desarrollar: permite cambios de programa más fáciles y un desarrollo de productos más rápido.
- Interoperabilidad de múltiples proveedores: los equipos de red de múltiples proveedores pueden funcionar en la misma red.
- Ingeniería modular: un proveedor puede escribir software que implemente capas superiores.

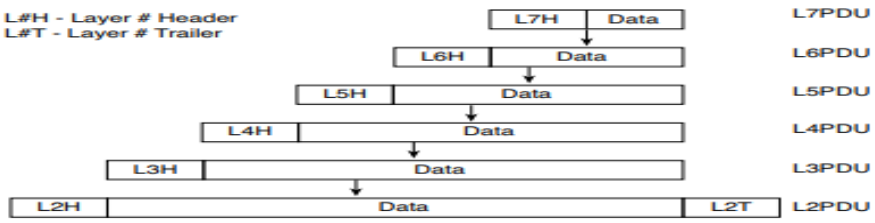
Terminología de encapsulación OSI

La capa inferior encapsula los datos de la capa superior detrás de un encabezado.

Una PDU representa los bits que incluyen los encabezados y los tráileres de esa capa, así como los datos encapsulados.

La Figura 2-14 representa el proceso de encapsulación típico.

Figure 2-14 *OSI Encapsulation and Protocol Data Units*



- Capítulo 3

Capítulo 3 Fundamentos de LANs

El término Ethernet se refiere a una familia de estándares que en conjunto definen las capas físicas y de enlace de datos del tipo de LAN más popular del mundo. Los diferentes estándares varían en lo que se refiere a la velocidad soportada, con velocidades de 10 megabits por segundo (Mbps), 100 Mbps, y 1000 Mbps (1 gigabit por segundo, o Gbps) que es la más común actualmente. Los estándares también difieren en cuanto a los tipos de cableado y la longitud permitida para el cableado. Por ejemplo, los estándares Ethernet más comúnmente utilizados permiten el uso de cableado UTP (par trenzado sin *apantallar, unshielded turisted-pair) barato, mientras que otros estándares exigen un* cableado de fibra óptica, más caro.

El coste del cableado de fibra óptica podría merecer la pena en algunos casos porque resulta más seguro y permite unas distancias mucho mayores entre dispositivos. A fin de soportar necesidades tan diversas en cuanto a la construcción de una LAN.

El Instituto de ingenieros eléctricos y electrónicos (IEEE, Inslilute o f Electrical and Electronics Engineers) ha definido muchos estándares Ethernet desde que inició el proceso de estandarización de las LANs a principios de la década de 1980. La mayoría de los están- dares define una variación diferente de Ethernet en la capa física, con diferencias en cuanto a velocidad y tipos de cableado. Además, para la capa de enlace de datos, el IEEE separa las funciones en dos subcapas:

• 1.a subcapa 802.3 MAC (Control de acceso al medio, Media Access Control).

• La subcapa 802.2 LLC (Control de enlace lógico, Logical Link Control).

De hecho, las direcciones MAC toman su nombre del nombre IEEE para esta porción inferior de los estándares Ethernet de la capa de enlace de datos.

Cada nuevo estándar del IEEE para la capa física requiere muchas diferencias en la capa física. Sin embargo, cada uno de estos estándares de la capa física utiliza exactamente la misma cabecera 802.3, y cada uno también usa la subcapa LLC superior. La Tabla 3.2 enumera los estándares de la capa física Ethernet del IEEE que más se utilizan.

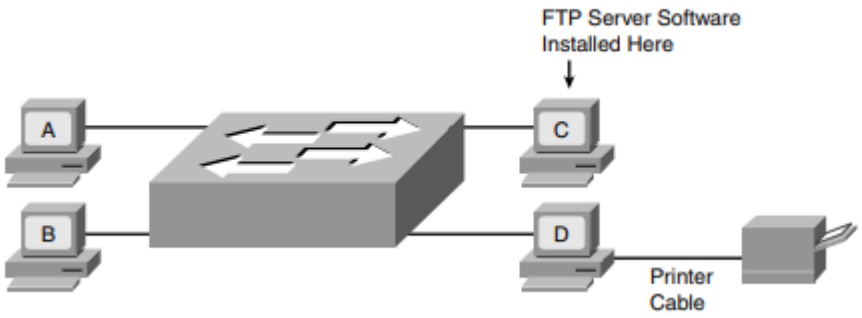
Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Fiber, 550 m (SX) 5 km (LX)
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	100 m

La tabla resulta apropiada para el estudio, pero los términos que contiene exigen una pequeña explicación. En primer lugar, observe que el término Ethernet se utiliza a menudo con el significado "todos los tipos de Ethernet", pero en algunos casos se utiliza con el significado "Ethernet 10BASE-T". (Como el término Ethernet puede resultar ambiguo a veces, este libro se refiere a Ethernet 10-Mbps como 10BASE-T cuando en la explicación es importante el tipo específico de Ethernet.) En segundo lugar, observe que el nombre alternativo de cada tipo de Ethernet especifica la velocidad en Mbps; 10 Mbps, 100 Mbps y 1000 Mbps. Las letras T y TX de los nombres alternativos se refieren al hecho de que cada uno de estos estándares define el uso de cableado UTP, donde T se refiere a la "T" de "par trenzado".

Para construir y crear una LAN moderna utilizando cualquiera de los tipos basados en UTP de las LANs Ethernet enumeradas en la Tabla 3.2, necesita los siguientes compo¬ nentes:

• Computadoras con una tarjeta de interfaz de red (NIC) Ethernet instalada. • Un hub Ethernet o un szoitch Ethernet.

Figure 3-1 *Typical Small Modern LAN*



La mayoría de las personas pueden crear una LAN como la de la Figura 3.1 casi sin conocimientos reales de cómo funcionan las LANs. Casi todos los PCs contienen una NIC Ethernet instalada de fábrica. No es necesario que los switches estén configurados para poder enviar tráfico entre computadoras. Todo lo que tiene que hacer es conectar el switch a un cable de alimentación y conectar los cables UTP de cada PC al switch. Con ello, los PCs deberían poder enviarse tramas Ethernet entre sí. Puede utilizar una LAN así de pequeña para muchos propósitos, incluso sin una conexión WAN. Considere las siguientes funciones para las que una LAN es la solución de pequeña escala perfecta:

Compartir archivos: Cada computadora puede configurarse para compartir todo su sistema de archivos, o determinadas partes del mismo, para que las demás computadoras puedan leer, o posiblemente leer y escribir, los archivos de dicha

computadora. Normal- mente, esta función forma parte del sistema operativo de un PC.

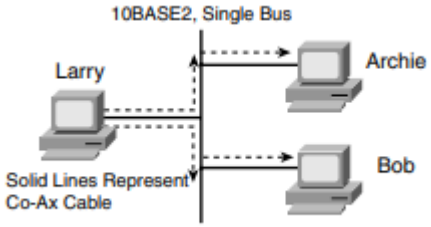
Compartir una impresora: Las computadoras también pueden compartir sus impresoras. Por ejemplo, los PCs A, B y C de la Figura 3.1 podrían imprimir documentos en la impresora del PC D. Esta función también forma parte normalmente del sistema operativo de un PC.

Transferir archivos: Una computadora podría instalar un servidor de transferencia de archivos, para de este modo permitir a otras computadoras enviar y recibir archivos a y desde otra computadora. Por ejemplo, el PC C podría tener instalado un software de ser.

Jugar Los PCs pueden tener juegos instalados para que varios jugadores puedan jugar simultáneamente en la misma partida. Los juegos se comunicarían entonces utilizando Ethernet.

Los estándares Ethernet originales: 10BASE2 y 10BASE5

Ethernet se entiende mejor considerando las dos primeras especificaciones Ethernet, 10BASE5 y 10BASE2. Estas dos especificaciones Ethernet definían los detalles de las capas física y de enlace de datos de las primeras redes Ethernet. (10BASE2 y 10BASE5 difieren en sus detalles de cableado, pero para las explicaciones de este capítulo consideraremos que son idénticas.) Con estas dos especificaciones, el ingeniero de redes instala una serie de cables coaxiales que conectan cada dispositivo de la red Ethernet. No hay ningún hub, switch o panel de cableado. Ethernet consiste únicamente en el conjunto de NICs Ethernet de las computadoras y el cableado coaxial. Las series de cables crean un circuito eléctrico.



Las líneas sólidas de la figura representan el cableado de la red física. Las líneas dis- continuas con flechas representan la ruta que toma la trama transmitida por Larry. Larry envía una señal eléctrica a través de su NIC Ethernet por el cable, y tanto Bob como Archie reciben la señal. El cableado crea un bus eléctrico físico, por lo que la señal transmitida es recibida por todas las estaciones de la LAN. Al igual que un autobús escolar se detiene a lo largo de una ruta en casa de todos

los estudiantes, la señal eléctrica en una red 10BASE2 o 10BASE5 se propaga a todas las estaciones de la LAN.

En términos sencillos, CSMA/CD se parece a lo que ocurre en una sala de reuniones con muchos asistentes. Es difícil entender lo que dos personas están diciendo cuando hablan al mismo tiempo, por lo que normalmente una persona habla y el resto escucha. Imagine que Bob y Larry quieren responder a los comentarios del orador actual. Tan pronto como este último se toma un respiro, Bob y Larry intentan hablar al mismo tiempo.

Si Larry oye la voz de Bob antes de emitir un sonido, Larry debería detenerse y dejar hablar a Bob. O puede que los dos empiecen a hablar casi al mismo tiempo, así que se "pisan" el uno al otro y nadie puede escuchar lo que se dice. Después está el legendario "Perdóneme, prosiga con lo que estaba diciendo", y habla Larry o Bob. O quizás se mete otra persona por medio y habla mientras Larry y Bob se ceden el tumo mutuamente. Estas "reglas" están basadas en nuestra cultura; CSMA/CD está basado en las especificaciones del protocolo Ethernet y logra el mismo tipo de objetivo.

• Un dispositivo que quiere enviar una trama espera hasta que la LAN está en silencio (es decir, no se están enviando tramas actualmente) antes de intentar enviar una señal eléctrica.

• Si aun así se produce una colisión, los dispositivos que la provocaron esperan una cantidad de tiempo aleatoria y después lo vuelven a intentar.

Repetidores

Al igual que cualquier tipo de LAN, 10BASE5 y 10BASE2 tienen limitaciones en cuanto a la longitud total de un cable. Con 10BASE5, el límite era de 500 metros; con 10BASE2, era de 185 metros. Curiosamente, el 5 y el 2 de los nombres 10BASE5 y 10BASE2 representan la longitud máxima del cable: el 2 se refiere a 200 metros, que es un número muy cercano al máximo real establecido en 185 metros. (Los dos tipos de Ethernet trabajaban a 10 Mbps.)

Los repetidores se conectan a múltiples segmentos de cable, reciben la señal eléctrica en un cable, interpretar los bits como 1 y 0, y generar una señal nueva, limpia y fuerte en el otro cable. Un repetidor no amplifica simplemente la señal, porque amplificar la señal podría también amplifica cualquier ruido captado en el camino.

No debe esperar que necesite implementar LAN Ethernet 10BASE5 o 10BASE2 hoy.

Sin embargo, con fines de aprendizaje, tenga en cuenta varios puntos clave de esta sección como pasa a los conceptos que se relacionan con las LAN de hoy:

■ Las LAN Ethernet originales creaban un bus eléctrico al que se conectaban todos los dispositivos.

■ Debido a que pueden ocurrir colisiones en este bus, Ethernet definió el algoritmo CSMA/CD, que definió una forma de evitar colisiones y tomar medidas cuando ocurrieron colisiones.

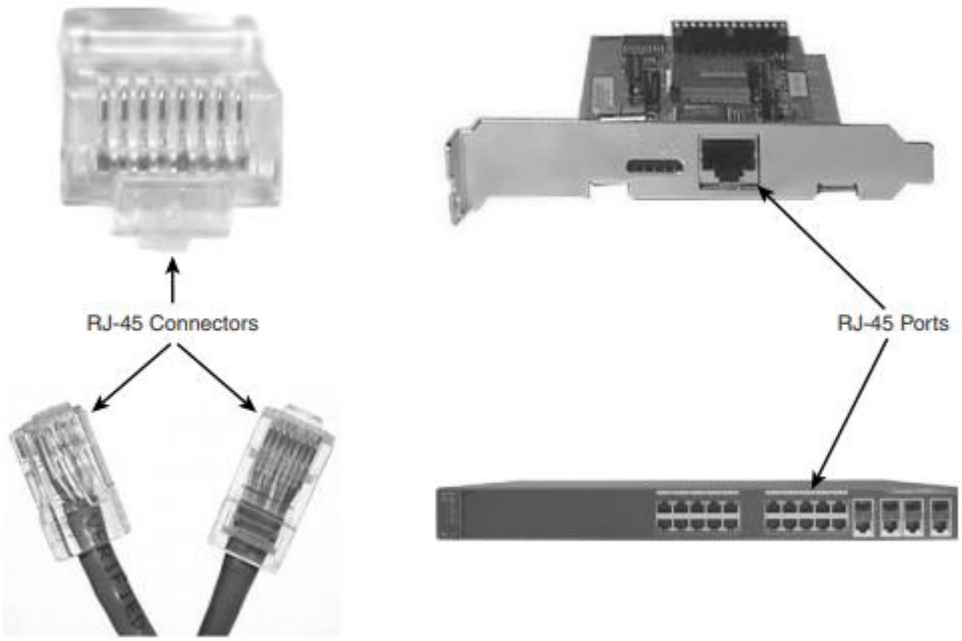
■ Los repetidores extendieron la longitud de las LAN limpiando la señal eléctrica y repitiéndola, una función de Capa 1, pero sin interpretar el significado de la señal eléctrica.

Los tres estándares de Ethernet más comunes utilizados hoy en día: 10BASE-T (Ethernet), 100BASE-TX (Fast Ethernet o FE) y 1000BASE-T (Gigabit Ethernet o GE): use cableado UTP. Existen algunas diferencias clave, particularmente con la cantidad de pares de cables necesarios en cada caso, y en el tipo (categoría) de cableado. Esta sección examina algunos de los detalles de cableado UTP, señalando las diferencias entre estos tres estándares en el camino. En particular, esta sección describe los cables y los conectores en los extremos de los cables, cómo usan los hilos en los cables para enviar datos y los pines requeridos para una correcta operación.

Cables UTP y Conectores RJ-45

El cableado UTP utilizado por los estándares Ethernet populares incluye dos o cuatro pares de alambres Debido a que los alambres dentro del cable son delgados y quebradizos, el cable en sí tiene una exterior chaqueta de plástico flexible para soportar los cables. Cada cable de cobre individual también tiene un delgado revestimiento de plástico para ayudar a evitar que el cable se rompa. El revestimiento de plástico de cada cable tiene un color diferente, lo que facilita mirar ambos extremos del cable e identificar los extremos de un alambre individual.

Los extremos del cable suelen tener algún tipo de conector adjunto (normalmente conectores RJ-45), con los extremos de los cables insertados en los conectores. El conector RJ-45 tiene ocho

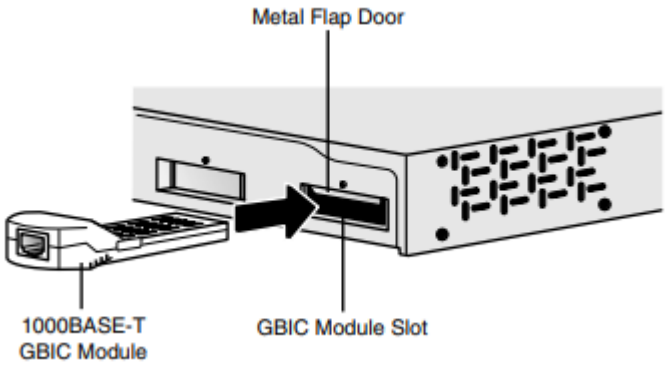


}

La figura muestra tres vistas separadas de un conector RJ-45 a la izquierda. La vista de frente en la parte superior izquierda de la figura se muestran los extremos de los ocho cables en sus posiciones de pin dentro del cable UTP. La parte superior derecha de la figura muestra una NIC de Ethernet que no es aún instalado en una computadora. El puerto RJ-45 en la NIC estaría expuesto en el costado de la computadora, haciéndola fácilmente accesible tan pronto como la NIC se haya instalado en una computadora.

La parte inferior derecha de la figura muestra el costado de un switch Cisco 2960, con múltiples Puertos RJ-45, lo que permite que múltiples dispositivos se conecten fácilmente a la red Ethernet.

Aunque los conectores y puertos RJ-45 son populares, es posible que los ingenieros deseen comprar Cisco Conmutadores LAN que tienen algunos puertos físicos que se pueden cambiar sin tener que compre un interruptor completamente nuevo. Muchos switches de Cisco tienen algunas interfaces que utilizan Convertidores de interfaz Gigabit (GBIC) o conectables de formato pequeño (SFP)



Si un ingeniero de red necesita usar un conmutador existente en una nueva función en una red de campus, el ingeniero podría simplemente comprar un nuevo 1000BASE-LX GBIC para reemplazar el antiguo 1000BASE-T GBIC y reduzca el costo adicional de comprar un conmutador completamente nuevo.

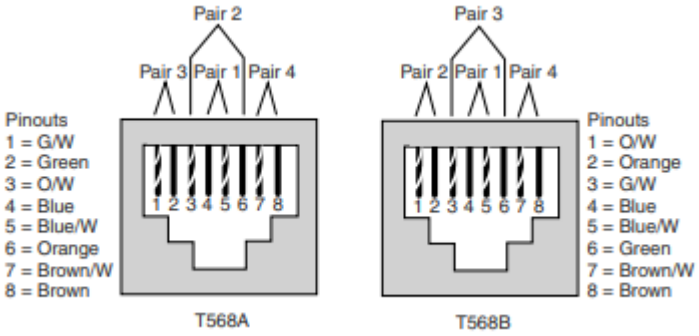
Transmisión de datos mediante pares trenzados

El cableado UTP consta de pares de cables emparejados que, de hecho, están trenzados entre sí, de ahí el nombre par trenzado. Los dispositivos en cada extremo del cable pueden crear un circuito eléctrico utilizando un par de cables enviando corriente en los dos cables, en direcciones opuestas. cuando actual pasa por cualquier alambre, esa corriente induce un campo magnético fuera del alambre; el magnético campo puede a su vez causar ruido eléctrico en otros hilos del cable.

Para enviar datos a través del circuito eléctrico creado a través de un par de cables, los dispositivos utilizan una codificación esquema que define cómo debe variar la señal eléctrica, con el tiempo, para significar una señal binaria 0 o 1. Por ejemplo, 10BASE-T utiliza un esquema de codificación que codifica un 0 binario como una transición de un voltaje más alto a un voltaje más bajo durante la mitad de un intervalo de 1/10,000,000 de segundo.

Asignaciones de pines de cableado UTP para 10BASE-T y 100BASE-TX

Los alambres en el cable UTP deben estar conectados a las posiciones correctas de los pines en el RJ-45 conectores para que la comunicación funcione correctamente. Como se mencionó anteriormente, el RJ-45 El conector tiene ocho posiciones de clavijas, o simplemente clavijas, en las que se colocan los cables de cobre dentro del sobresalga el cable. Los pines de cableado: la elección de qué color de cable va en qué pin posición: debe cumplir con los estándares de Ethernet descritos en esta sección.



Cableado 1000BASE-T

Como se señaló anteriormente, 1000BASE-T difiere de 10BASE-T y 100BASE-TX en cuanto a la cableado y pinouts. Primero, 1000BASE-T requiere cuatro pares de cables. Además, Gigabit Ethernet transmite y recibe en cada uno de los cuatro pares de cables simultáneamente.

Mejora del rendimiento mediante el uso de conmutadores

Esta sección examina algunos de los problemas de rendimiento creados cuando se utilizan concentradores, seguido de explicaciones de cómo los conmutadores LAN resuelven los dos problemas de rendimiento más importantes problemas encontrados con los concentradores. Para apreciar mejor el problema, considere la Figura 3-10, que muestra lo que sucede cuando un solo dispositivo envía datos a través de un concentrador

Aumento del ancho de banda disponible mediante conmutadores

El término dominio de colisión define el conjunto de dispositivos cuyas tramas podrían colisionar. Todo dispositivos en 10BASE2, 10BASE5 o cualquier red que utilice un concentrador corren el riesgo de colisiones entre los marcos que envían, por lo que todos los dispositivos en uno de estos tipos de redes Ethernet están en el mismo dominio de colisión

Los conmutadores de LAN reducen significativamente, o incluso eliminan, el número de colisiones en una LAN.

Duplicación del rendimiento mediante el uso de Ethernet dúplex completo

Cualquier red Ethernet que utilice concentradores requiere lógica CSMA/CD para funcionar correctamente. Sin embargo, CSMA/CD impone una lógica semidúplex en cada dispositivo, lo que significa que solo un dispositivo puede enviar a la vez. Debido a que los conmutadores pueden almacenar fotogramas en la memoria, los conmutadores pueden elimine las colisiones en los puertos del conmutador que se conectan a un solo dispositivo. Como resultado, LAN los conmutadores con un solo dispositivo cableado a cada puerto del conmutador permiten el uso de full-

duplex operación. Dúplex completo significa que una tarjeta Ethernet puede enviar y recibir simultáneamente.

Protocolos de enlace de datos Ethernet

Una de las fortalezas más significativas de la familia de protocolos Ethernet es que estos.

Los protocolos utilizan el mismo pequeño conjunto 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, de nuevo aplicable a la mayoría de los tipos de Ethernet, a menos que se haya desactivado.

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, normalmente se escribe con puntos que separan cada conjunto de cuatro dígitos hexadecimales. Por ejemplo, 0000.0C12.3456 es una dirección Ethernet válida.

■ Direcciones de difusión: las direcciones MAC del grupo IEEE más utilizadas, las dirección de difusión, tiene un valor de FFFF.FFFF.FFFF (notación hexadecimal). En 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 para comunicarse. Cuando IP multidifunde a través de Ethernet, el MAC de multidifusión las direcciones utilizadas por IP siguen este formato: 0100.5exx.xxxx, donde se puede utilizar cualquier valor en la última mitad de la dirección.

Encuadre de Ethernet

El encuadre define cómo se interpreta una cadena de números binarios. En otras palabras, enmarcar define el significado detrás de los bits que se transmiten a través de una red. El físico capa le ayuda a obtener una cadena de bits de un dispositivo a otro. Cuando el dispositivo receptor obtiene los bits, ¿cómo deben interpretarse? El término encuadre se refiere a la definición de los campos que se

supone que están en los datos que se reciben. En otras palabras, el encuadre define el significado de los bits transmitidos y recibidos a través de una red.

Identificación de los datos dentro de una trama Ethernet

A lo largo de los años, se han diseñado muchos protocolos de capa de red (Capa 3) diferentes. La mayoría de estos protocolos formaban parte de modelos de protocolos de red más grandes creados por proveedores para dar soporte a sus productos, como IBM Systems Network Architecture (SNA), Novell NetWare, DECnet de Digital Equipment Corporation y AppleTalk de Apple Computer. Además, los modelos OSI y TCP/IP también definieron el protocolo de capa de red

Todos estos protocolos de Capa 3, además de varios otros, podrían usar Ethernet. Para usar Ethernet, el El protocolo de capa de red colocaría su paquete (en términos generales, su PDU L3) en el parte de datos de la trama de Ethernet que se muestra en la Figura 3-14. Sin embargo, cuando un dispositivo recibe tal marco Ethernet, ese dispositivo receptor necesita saber qué tipo de L3 PDU está en el marco de Ethernet. ¿Es un paquete IP? un paquete OSI? ¿SNA? etcétera.

Para crear un campo Tipo para marcos que usan el campo Tipo/Longitud como campo Longitud, ya sea se agregan uno o dos encabezados adicionales después del encabezado Ethernet 802.3 pero antes del Encabezado de capa 3. Por ejemplo, al enviar paquetes IP, la trama Ethernet tiene dos encabezados adicionales:

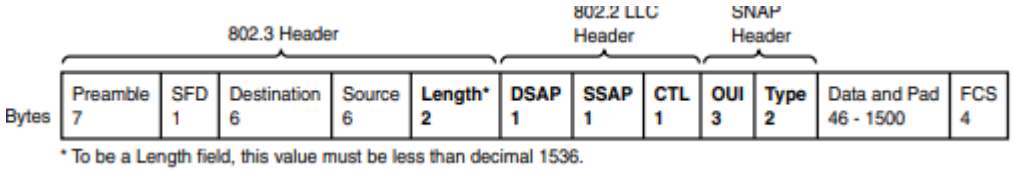
■ Un encabezado de control de enlace lógico (LLC) IEEE 802.2

■ Un encabezado del Protocolo de acceso a la subred (SNAP) IEEE

La Figura 3-15 muestra una trama de Ethernet con estos encabezados adicionales. Tenga en cuenta que el SNAP

El campo Tipo de encabezado tiene el mismo propósito, con los mismos valores reservados, que el campo Ethernet.

Campo Tipo/Longitud.



Detección de errores

La última función de la capa de enlace de datos de Ethernet que se explica aquí es la detección de errores. Detección de errores es el proceso de descubrir si los bits de un marco cambiaron como resultado de ser enviados a través de red. Los

bits pueden cambiar por muchas razones pequeñas, pero generalmente ocurren errores como resultado de algún tipo de interferencia eléctrica. Como todos los protocolos de enlace de datos cubiertos en el Exámenes CCNA, Ethernet define un encabezado y un tráiler, y el tráiler contiene un campo utilizado con el fin de detectar errores.

El campo Ethernet Frame Check Sequence (FCS) en el tráiler de Ethernet, el único campo en el tráiler de Ethernet: permite que un dispositivo que recibe una trama de Ethernet detecte si los bits han cambiado durante la transmisión. Para detectar un error, el dispositivo emisor calcula una función matemática compleja, con el contenido del marco como entrada, poniendo el resultado en el campo FCS de 4 bytes de la trama. El dispositivo receptor hace los mismos cálculos en el marco; si es el cálculo coincide con el campo FCS en el cuadro, no se produjeron errores. Si el resultado no coincide con el campo FCS, se produjo un error y la trama se descarta.

Tenga en cuenta que la detección de errores no significa también la recuperación de errores. Ethernet define que el error la trama debe ser descartada, pero Ethernet no toma ninguna acción para hacer que la trama sea retransmitida. Otros protocolos, en particular TCP (como se describe en el Capítulo 6, “Fundamentos de Transporte TCP/IP, Aplicaciones y Seguridad”), puede notar la pérdida de datos y causar un error que se produzca la recuperación

- **Capítulo 4.- Fundamentals of WANs**

Tabla 4-1 “¿Ya lo sé?” Asignación de sección a pregunta de temas básicos

Foundation Topics Section	Questions
OSI Layer 1 for Point-to-Point WANs	1–4
OSI Layer 2 for Point-to-Point WANs	5, 6
Frame Relay and Packet-Switching Services	7, 8

Temas de la Fundación

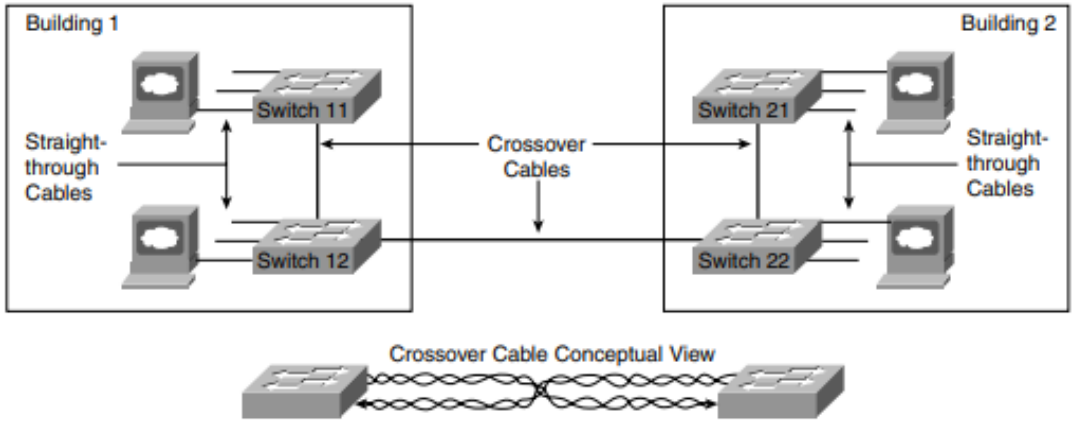
Como leyó en el capítulo anterior, las capas de enlace de datos y física de OSI trabajan juntas para entregar datos a través de una amplia variedad de tipos de redes físicas. estándares LAN y los protocolos definen cómo conectarse en red entre dispositivos que están relativamente cerca, por lo tanto, el término área local en el acrónimo LAN. Los estándares y protocolos de WAN definen cómo red entre dispositivos que están relativamente lejos, en algunos casos, incluso miles de millas de distancia, de ahí el término de área amplia en el acrónimo WAN.

Los temas de WAN de este capítulo describen principalmente cómo las redes empresariales usan las WAN para conectar sitios remotos. La Parte V de este libro cubre una gama más amplia de temas de WAN, incluidos tecnologías populares de acceso a Internet, como la línea de suscripción digital (DSL) y el cable, junto con una variedad de temas de configuración. La Guía de certificación oficial ICND2 cubre Frame Relay con mucho más detalle que este libro, así como los conceptos detrás de Internet privado virtual (VPN), que es una forma de usar Internet en lugar de los enlaces WAN tradicionales.

Capa 1 de OSI para WAN punto a punto

La capa física OSI, o Capa 1, define los detalles de cómo mover datos desde un dispositivo a otro. De hecho, mucha gente piensa en la capa 1 de OSI como "bits de envío". capas superiores encapsule 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 para transmitir realmente los bits a otro dispositivo. Un enlace WAN punto a punto actúa como un enlace troncal Ethernet entre dos conmutadores Ethernet de muchas maneras.

Por lo general, utiliza cables Ethernet directos entre los dispositivos del usuario final y los conmutadores. Para los enlaces troncales entre los interruptores, utiliza cables cruzados porque cada interruptor transmite en el mismo par de pines en el conector, por lo que el cable cruzado conecta la transmisión de un dispositivo emparejar con el par de recepción del otro dispositivo.



Ahora imagine que los edificios están a 1000 millas de distancia en lugar de uno al lado del otro. Tú inmediatamente se enfrentan a dos problemas:

■ Ethernet no admite ningún tipo de cableado que permita que un enlace troncal individual se ejecute 1000 millas

■ Incluso si Ethernet admitiera un enlace troncal de 1000 millas, usted no tiene derecho de paso necesitaba enterrar un cable sobre las 1000 millas de bienes raíces entre edificios.

Las LAN tienden a residir en un solo edificio o posiblemente entre edificios en un campus utilizando cableado óptico aprobado para Ethernet. las conexiones generalmente recorren distancias más largas que Ethernet: a través de la ciudad o entre ciudades.

A menudo, solo una o unas pocas empresas tienen los derechos para tender cables bajo tierra.

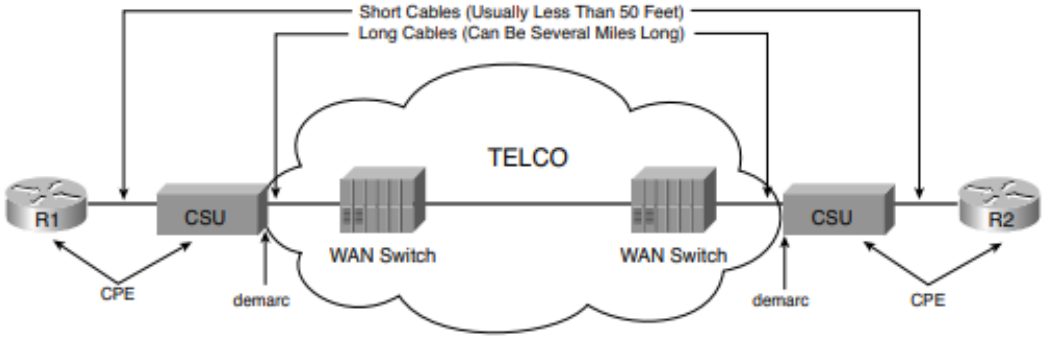
Los enlaces WAN punto a punto proporcionan conectividad básica entre dos puntos. Para obtener un enlace WAN punto a punto, trabajaría con un proveedor de servicios para instalar un circuito. que teléfono empresa o proveedor de servicios le brinda es similar a lo que tendría si hiciera una llamada telefónica entre dos sitios, pero nunca colgó. Los dos dispositivos en cada extremo del circuito WAN podría enviar y recibir bits entre sí en cualquier momento que lo deseen, sin necesidad de marcar un número de teléfono. Debido a que la conexión siempre está disponible, una conexión WAN punto a punto a veces se denomina circuito o línea arrendados porque tiene el derecho exclusivo de usar ese circuito, siempre y cuando sigas pagando por él.

Conexiones WAN desde el punto de vista del cliente

Los conceptos detrás de una conexión punto a punto son simples. Sin embargo, para entender completamente lo que hace el proveedor de servicios para construir su red para admitir su línea punto a punto, necesitaría 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 ICND1 examen se refiere a cómo se implementan las conexiones WAN entre la compañía telefónica y un sitio del cliente. En el camino, deberá aprender un poco sobre la terminología. Utilizado por el proveedor. La empresa de telecomunicaciones rara vez ejecuta una cable de 1000 millas para usted entre los dos sitios.

En cambio, ya ha construido una gran red e incluso conecta cables adicionales desde la oficina central (CO) local hasta su edificio (una CO es solo un edificio donde la empresa de telecomunicaciones ubica los dispositivos utilizados para crear su propia red). A pesar de todo de lo que hace la empresa de telecomunicaciones dentro de su propia red, lo que recibe es el equivalente a un

circuito arrendado de cuatro hilos entre dos edificios



Por lo general, los enrutadores se conectan a un dispositivo llamado unidad de servicio de canal externo/servicio de datos.

Unidad (CSU/DSU). El enrutador se conecta a la CSU/DSU con un cable relativamente corto, generalmente menos de 50 pies de largo, porque las CSU/DSU generalmente se colocan en un rack cerca el enrutador El cable mucho más largo de cuatro hilos de la empresa de telecomunicaciones se conecta a la CSU/DSU. Eso el cable sale del edificio, atravesando los cables ocultos (típicamente enterrados) que a veces veo a los trabajadores de la compañía telefónica arreglando al lado de la carretera. El otro extremo de eso el cable termina en la CO, y el cable se conecta a un dispositivo de CO llamado genéricamente WAN cambiar.

En los Estados Unidos, la demarcación suele ser donde la empresa de telecomunicaciones finaliza físicamente el conjunto de dos pares trenzados dentro del edificio del cliente. Por lo general, el cliente le pide a la empresa de telecomunicaciones que terminar el cable en una habitación en particular, y la mayoría, si no todas, las líneas de la empresa de telecomunicaciones en ese edificio terminan en la misma habitación.

El término equipo en las instalaciones del cliente (CPE) se refiere a los dispositivos que están en el sitio del cliente, desde la perspectiva de la empresa de telecomunicaciones. Por ejemplo, tanto la CSU/DSU como el enrutador son CPE dispositivos en este caso.

La demarcación no siempre reside donde se muestra en la Figura 4-3. En algunos casos, la empresa de telecomunicaciones en realidad podría poseer la CSU/DSU, y la demarcación estaría en el lado del enrutador de la CSU/ ESD. En algunos casos hoy en día, la empresa de telecomunicaciones incluso posee y administra el enrutador en el sitio del cliente, moviendo nuevamente el punto que sería considerado el demarca. Independientemente de dónde esté el demarc se encuentra desde una perspectiva legal, el término CPE todavía se refiere al equipo en la empresa de telecomunicaciones ubicación del cliente.

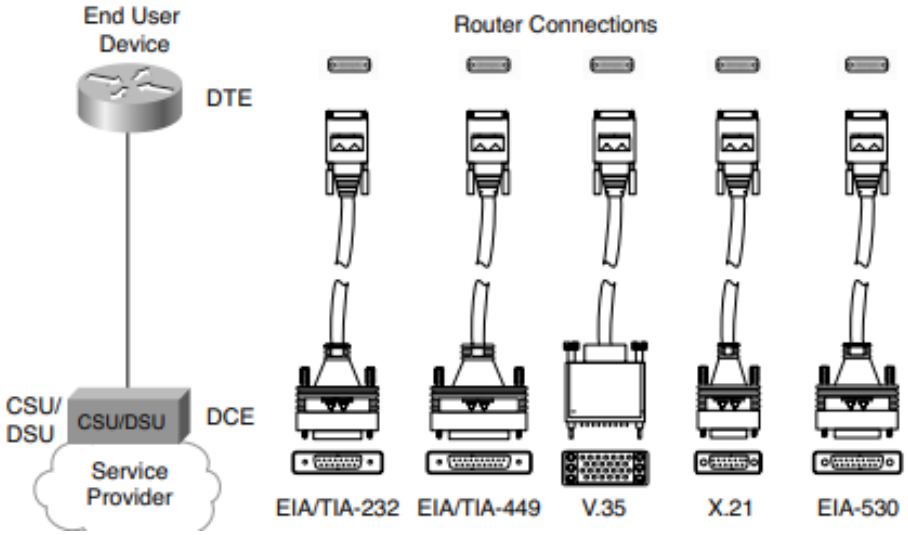
Estándares de cableado WAN

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

Las interfaces seriales sincrónicas en los enrutadores Cisco utilizan una variedad de interfaces físicas patentadas. Tipos de conectores, como el conector D-Shell de 60 pines que se muestra en la parte superior del cable dibujos en la figura 4-4. El cable que conecta el enrutador a la CSU/DSU utiliza un conector que se ajusta a la interfaz serial del enrutador en el lado del enrutador y un conector WAN estandarizado ptg6885603

Capa 1 de OSI para WAN punto a punto 85

Tipo que coincida con la interfaz CSU/DSU en el extremo CSU/DSU del cable.



Velocidades de reloj, sincronización, DCE y DTE

Un ingeniero de redes empresariales que desea instalar una nueva línea alquilada punto a punto entre dos enrutadores tiene varias tareas que realizar. En primer lugar, el ingeniero de redes se pone en contacto con un proveedor de servicios y ordena el circuito. Como parte de ese proceso, el ingeniero de redes especifica qué tan rápido debe funcionar el circuito, en kilobits por segundo (kbps). Mientras

que la empresa de telecomunicaciones instala el circuito, el ingeniero compra dos CSU/DSU, instala uno en cada sitio y configura cada CSU/DSU.

Para que el enlace funcione, los distintos dispositivos deben sincronizar sus relojes para que funcionen exactamente a la misma velocidad, un proceso llamado sincronización. Los circuitos síncronos imponen orden de tiempo en los extremos de envío y recepción del enlace. Esencialmente, todos los dispositivos aceptan probar para funcionar exactamente a la misma velocidad, pero es costoso construir dispositivos que realmente puedan operar a exactamente la misma velocidad. Por lo tanto, los dispositivos funcionan casi a la misma velocidad y escuchan el velocidad del otro dispositivo en el otro lado del enlace. Un lado hace pequeños ajustes en su tasa para que coincida con el otro lado.

La sincronización ocurre entre las dos CSU/DSU en una línea alquilada al tener una CSU/ DSU (la esclava) ajusta su reloj para que coincida con la frecuencia de reloj de la otra CSU/DSU (la maestra)..

El proceso funciona casi como las escenas de las novelas de espionaje en las que los espías sincronizan sus relojes; en este caso, los dispositivos de red sincronizan sus relojes varias veces por segundo.

Construcción de un enlace WAN en un laboratorio

En una nota práctica, al comprar cables seriales de Cisco, puede elegir un DTE o un cable DCE. Usted elige el tipo de cable en función de si el enrutador actúa como DTE o DCE. En la mayoría de los casos, con un enlace WAN real, el enrutador actúa como DTE, por lo que el enrutador debe usar un cable DTE para conectar a la CSU/DSU.

Puede construir un enlace serial en un laboratorio sin usar ninguna CSU/DSU, pero para hacerlo, un enrutador debe suministrar fichaje. Al construir un laboratorio para estudiar para cualquiera de los exámenes de Cisco, no necesita comprar CSU/DSU u ordenar un circuito WAN. Puedes comprar dos enrutadores, un cable serie DTE para un enrutador y un cable serie DCE para el otro, y conecte los dos cables.

El enrutador con el cable DCE puede configurarse para proporcionar reloj, lo que significa que no necesita una CSU/DSU. Entonces, puede construir una WAN en su laboratorio doméstico, ahorrando cientos de dólares al no comprar CSU/DSU. Los cables DTE y DCE se pueden conectar a cada otro (el cable DCE tiene conector hembra y el cable DTE tiene conector macho) y a los dos enrutadores.

Velocidades de enlace que ofrecen las empresas de telecomunicaciones

No importa cómo los llame (telcos, PTT, proveedores de servicios), estas empresas no simplemente le permiten elegir la velocidad exacta de un enlace WAN. En cambio, los estándares definen qué tan rápido un se puede ejecutar un enlace punto a punto.

El mecanismo original utilizado para convertir la voz analógica en una señal digital se llama pulso. modulación de código (PCM). PCM define que una señal de voz analógica entrante debe ser muestreado 8000 veces por segundo, y cada muestra debe estar representada por un código de 8 bits.

Entonces, se necesitaban 64.000 bits para representar 1 segundo de voz. Cuando las telecos del mundo construyeron sus primeras redes digitales, eligieron una velocidad de transmisión de referencia de 64 kbps porque ese era el ancho de banda necesario para una sola llamada de voz. El término señal digital el nivel 0 (DS0) se refiere al estándar para una sola línea de 64 kbps.

Hoy en día, la mayoría de las empresas de telecomunicaciones ofrecen líneas arrendadas en múltiplos de 64 kbps. En los Estados Unidos, lo digital el estándar de nivel de señal 1 (DS1) define una sola línea que admite 24 DS0, más 8 kbps canal aéreo, para una velocidad de 1.544 Mbps. (Un DS1 también se denomina línea T1).

La otra opción es un servicio de señal digital de nivel 3 (DS3), también llamado línea T3, que contiene 28 DS1.

Otras partes del mundo usan estándares diferentes, con Europa y Japón usando estándares que tener 32 DS0, llamada línea E1, con una línea E3 con 16 E1.

Capa 2 de OSI para WAN punto a punto

Los protocolos WAN utilizados en los enlaces seriales punto a punto brindan la función básica de los datos. Entrega 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 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 y identifica el tipo de paquete, HDLC define la trama. El

encabezado HDLC incluye una dirección campo y un campo de tipo de protocolo, con el tráiler que contiene una secuencia de verificación de trama (FCS) campo. La figura 4-6 describe el marco HDLC estándar y el marco HDLC que es Cisco propiedad.

Protocolo punto a punto

La Unión Internacional de Telecomunicaciones (UIT), anteriormente conocida como la Unión Consultiva Comité de Tecnologías Internacionales de Telecomunicaciones (CCITT), definido por primera vez HDLC. Más tarde, el Grupo de Trabajo de Ingeniería de Internet (IETF) vio la necesidad de otra información Protocolo de capa de enlace para uso entre enrutadores a través de un enlace punto a punto. En RFC 1661, el IETF creó el Protocolo punto a punto (PPP).

Comparando los conceptos básicos, PPP se comporta de manera muy similar a HDLC. El encuadre parece idéntico al estructurar el HDLC propiedad de Cisco. Hay un campo de Dirección, pero el direccionamiento no asunto. PPP descarta las tramas con errores que no pasan la verificación de FCS.

Además, PPP utiliza un campo de tipo de protocolo de 2 bytes. Sin embargo, debido a que el campo Tipo de protocolo es parte del estándar para PPP, cualquier proveedor que cumpla con el estándar PPP puede comunicarse con otros productos de proveedores. Entonces, al conectar un enrutador Cisco al enrutador de otro proveedor a través de un enlace serie punto a punto, PPP es el protocolo de capa de enlace de datos de elección.

Servicios de conmutación de paquetes y retransmisión de tramas

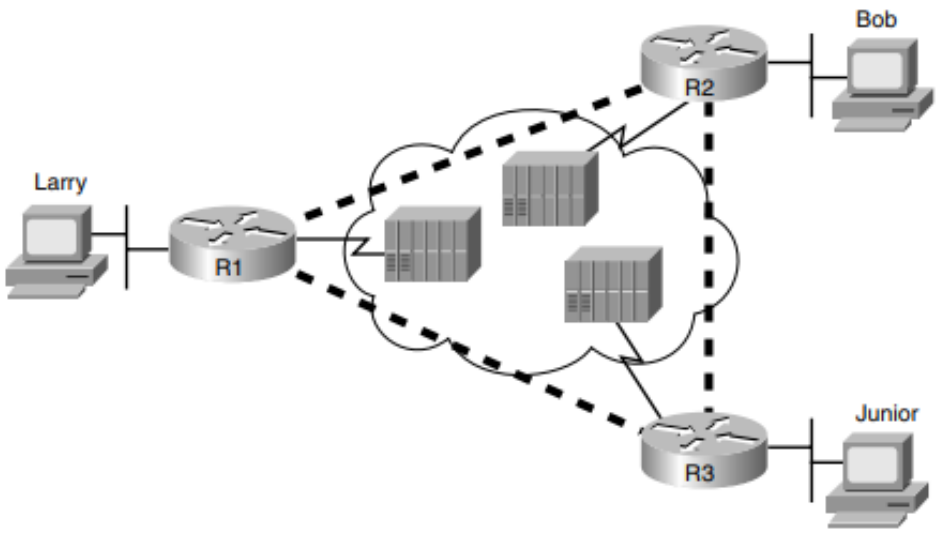
Los proveedores de servicios ofrecen una clase de servicios WAN, diferentes de las líneas arrendadas, que se pueden categorizados como servicios de conmutación de paquetes. En un servicio de conmutación de paquetes, WAN física existe conectividad, similar a una línea arrendada.

Sin embargo, una empresa puede conectar un gran número de enrutadores al servicio de conmutación de paquetes, usando un solo enlace serial de cada enrutador en el servicio de conmutación de paquetes. Una vez conectado, cada enrutador puede enviar paquetes a todos los demás enrutadores, al igual que todos los dispositivos conectados a un concentrador o conmutador Ethernet pueden enviar datos directamente entre sí.

Ya sabes, podemos instalar Frame Relay en su lugar. Solo necesitará una interfaz serial en R1 y una CSU/DSU. Para escalar a 100 sitios, es posible que necesite dos o tres seriales más interfaces en R1 para obtener más ancho de banda, pero

eso es todo. Y por cierto, porque tu arrendado las líneas funcionan a 128 kbps hoy, le garantizamos que puede enviar y recibir esa cantidad datos hacia y desde cada sitio. Actualizaremos la línea a velocidad R1 a T1 (1.544 Mbps).

Cuando tenga más de 128 kbps de tráfico en un sitio, ¡adelante, envíelo!



Muchos clientes de un único proveedor de servicios de Frame Relay comparten el Frame Relay de ese proveedor.

Red de retransmisión. Originalmente, las personas con redes de líneas arrendadas eran reacias a migrar a Frame Relay porque estarían compitiendo con otros clientes por el proveedor capacidad dentro de la red del proveedor de servicios. Para hacer frente a estos temores, Frame Relay está diseñado con el concepto de tasa de información comprometida (CIR). Cada VC tiene un CIR, lo cual es una garantía por parte del proveedor de que un VC en particular obtiene al menos ese ancho de banda.

Puede pensar en el CIR de un VC como el ancho de banda o la frecuencia de reloj de un circuito punto a punto, excepto que es el valor mínimo; de hecho, puede enviar más, en la mayoría de los casos.

Incluso en esta red de tres sitios, probablemente sea menos costoso usar Frame Relay que usar enlaces punto a punto. Ahora imagine una red mucho más grande, con 100 sitios, que necesita cualquier conectividad. ¡Un diseño de enlace punto a punto requeriría 4950 líneas alquiladas! Además, tú necesitarías 99 interfaces seriales por enrutador.

Por el contrario, con un diseño de Frame Relay, podría tener 100 enlaces de acceso a switches Frame Relay locales (1 por enrutador) con 4950 VC

funcionando los enlaces de acceso. Además, solo necesitaría una interfaz serial en cada enrutador.

La topología Frame Relay es más fácil de implementar para el proveedor de servicios, le cuesta menos al proveedor, y hace un mejor uso del núcleo de la red del proveedor. Como era de esperar, eso hace que sea menos costoso para el cliente de Frame Relay también. Para conectar muchos sitios WAN, Frame la retransmisión es simplemente más rentable que las líneas arrendadas.

- **Capítulo 5.- Fundamentals of IPv4 Addressing and Routing**

La capa física OSI (Capa 1) define cómo transmitir bits sobre un tipo particular de red física. La capa de enlace de datos OSI (Capa 2) define el entramado, direccionamiento, detección de errores y reglas sobre cuándo usar el medio físico. aunque son importante, estas dos capas no definen cómo entregar datos entre dispositivos que existen lejos el uno del otro, con muchas redes físicas diferentes ubicadas entre los dos ordenadores.

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 físico red a la que está conectado cada equipo terminal, e independientemente de los tipos de redes físicas utilizadas entre las dos computadoras, la capa de red define cómo reenviar, o enrutar, datos entre las dos computadoras.

Temas de la Fundación

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. 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 utilizadas, proporcionando a cada dispositivo (al menos) una dirección. 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 el grupo de direcciones en la red, lo que a su vez permite el enrutamiento (reenvío) proceso para que funcione bien.

Descripción general de las funciones de la capa de red

Un protocolo que define el enrutamiento y el direccionamiento lógico se considera una capa de red, o Capa 3, protocolo. OSI define un protocolo único de capa 3 llamado red sin conexión services (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 Internet (IP), Novell Internetwork Packet Exchange (IPX) o AppleTalk Datagram Protocolo de entrega (DDP). Hoy en día, el único protocolo de Capa 3 que se usa ampliamente es el Protocolo de capa de red TCP/IP—específicamente, IP.

El trabajo principal de IP es enrutar datos (paquetes) desde el host de origen al host de destino.

Debido a que una red puede necesitar reenviar una gran cantidad de paquetes, el proceso de enrutamiento IP es muy simple. IP no requiere acuerdos generales ni mensajes antes de enviar un paquete, haciendo de IP un protocolo sin conexión.

Lógica de PC1: envío de datos a un enrutador cercano

En este ejemplo, ilustrado en la Figura 5-1, la PC1 tiene algunos datos para enviar a la PC2. Porque PC2 no está en la misma Ethernet que PC1, PC1 necesita enviar el paquete a un enrutador que está conectado a la misma Ethernet que la PC1. El remitente envía una trama de enlace de datos a través del medio al enrutador cercano; esta trama incluye el paquete en la porción de datos de la trama. ese marco utiliza el direccionamiento de la capa de enlace de datos (capa 2) en el encabezado del enlace de datos para garantizar que el enrutador recibe la trama.

El punto principal aquí es que la computadora que creó los datos no sabe mucho sobre la red: cómo llevar los datos a algún enrutador cercano. Usando una analogía de la oficina de correos, es como saber cómo llegar a la oficina de correos local, pero nada más. Asimismo, PC1 necesita saber solo cómo llevar el paquete a R1, no el resto de la ruta utilizada para enviar el paquete a PC2.

Lógica de R1 y R2: enrutamiento de datos a través de la red R1 y R2 usan el mismo proceso general para enrutar el paquete. La tabla de enrutamiento para cualquier un protocolo de capa de red particular contiene una lista de agrupaciones de direcciones de capa de red. En cambio, de una sola entrada en la tabla de enrutamiento por dirección de capa de red de destino individual, hay es una entrada de tabla de enrutamiento por grupo. El enrutador compara la capa de red de destino dirección en el paquete a las entradas en la tabla de enrutamiento y hace una coincidencia.

Direccionamiento de capa de red (capa 3)

Los protocolos de la capa de red definen el formato y el significado de las direcciones lógicas. (El término dirección lógica no se refiere realmente a si las direcciones tienen sentido, sino más bien a contrastar estas direcciones con las direcciones físicas.) Cada computadora que necesita comunicar tendrá (al menos)

una dirección de capa de red para que otras computadoras puedan enviar paquetes de datos a esa dirección, esperando que la red entregue el paquete de datos a la computadora correcta.

Una característica clave de las direcciones de capa de red es que fueron diseñadas para permitir agrupación de direcciones. En otras palabras, algo sobre el valor numérico de una dirección implica un grupo o conjunto de direcciones, todas las cuales se consideran en el mismo grupo.

Con las direcciones IP, este grupo se denomina red o subred. Estas agrupaciones funcionan solo como los códigos zip (postales) de USPS, lo que permite que los enrutadores (clasificadores de correo) enruten (clasifiquen) lotes rápidamente de paquetes (cartas).

El proceso ARP

Tan pronto como un host conozca la dirección IP del otro host, es posible que el host emisor necesite saber la dirección MAC utilizada por la otra computadora. Por ejemplo, Hannah todavía necesita saber la Dirección MAC de Ethernet utilizada por 10.1.1.2, por lo que Hannah emite algo llamado ARP.

ETH IP Datos de anuncios UDP ETH

- Dirección MAC de destino = Dirección MAC de origen = 0200.1111.1111
- Información que Hannah necesita aprender
- Dirección IP de destino = Dirección IP de origen = 10.1.1.1 DNS Hannah Jessie
- 10.1.1.2
- 0200.2222.2222
- ptg6885603

Utilidades de la capa de red 129

Transmisión. Una transmisión ARP se envía a una dirección Ethernet de transmisión, por lo que todos en la LAN lo recibe Debido a que Jessie está en la misma LAN, recibe la transmisión ARP. Porque la dirección IP de Jessie es 10.1.1.2 y la transmisión ARP está buscando la dirección MAC asociada con 10.1.1.2, Jessie responde con su propia dirección MAC.

Ahora Hannah sabe las direcciones IP y Ethernet de destino que debe usar cuando enviando marcos a Jessie, y el paquete que se muestra en la Figura 5-12 se puede enviar con éxito.

Los hosts pueden o no necesitar ARP para encontrar la dirección MAC del host de destino en función de la lógica de enrutamiento de dos pasos utilizada por un host.

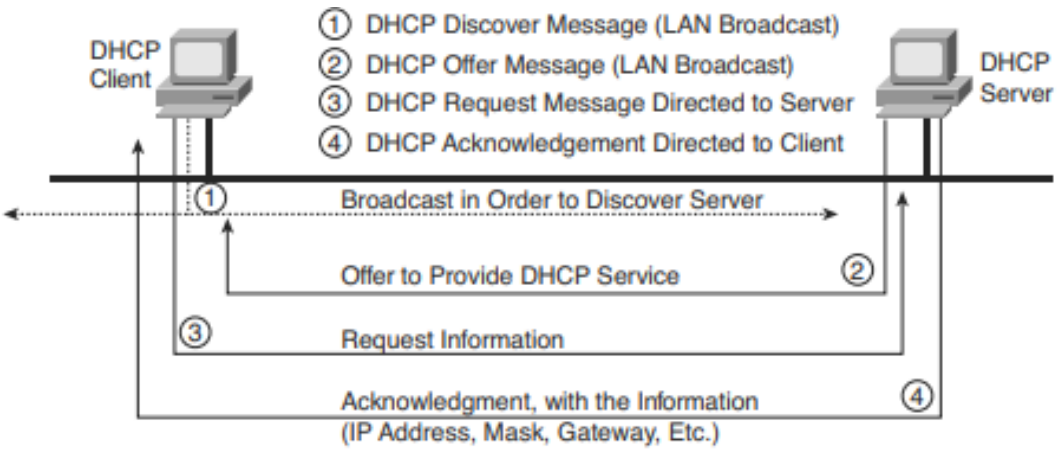
Si el host de destino está en la misma subred, el host de envío envía un ARP en busca de la dirección MAC del host de destino, sin embargo, si el host de envío

está en una subred diferente a la del host de destino, la lógica de enrutamiento del host de envío hace que el host de envío necesite reenviar el paquete a su puerta de enlace predeterminada.

Además, los hosts necesitan usar ARP para encontrar direcciones MAC solo de vez en cuando. Cualquier dispositivo que usa IP debe retener, o almacenar en caché, la información aprendida con ARP, colocando la información en su caché ARP. Cada vez que un host necesita enviar un paquete encapsulado en un marco de Ethernet, primero verifica su caché ARP y usa la dirección MAC que se encuentra allí.

Si la información correcta no aparece en la memoria caché ARP, el host puede usar ARP para descubrir la dirección MAC utilizada por una dirección IP particular. Además, un host aprende información ARP cuando recibiendo un ARP también.

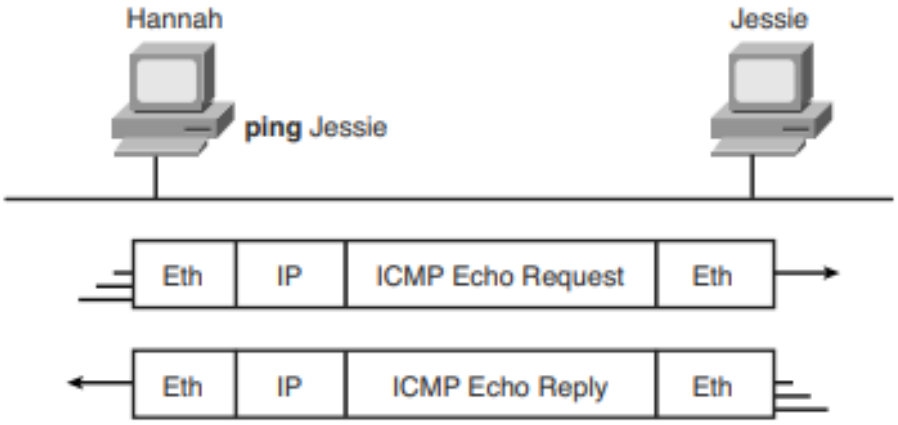
Por ejemplo, el proceso ARP que se muestra en la figura 5-14 da como resultado tanto Hannah como Jessie aprenden la dirección MAC del otro host.



ICMP Echo y el comando ping

Después de haber implementado una red, necesita una forma de probar la conectividad IP básica sin depender de ninguna aplicación para funcionar. La herramienta principal para probar conectividad de red es el comando ping. ping (Packet Internet Groper) utiliza Internet Protocolo de mensajes de control (ICMP), que envía un mensaje llamado solicitud de eco ICMP a otra dirección IP.

La computadora con esa dirección IP debería responder con un eco ICMP responder. Si eso funciona, ha probado con éxito la red IP. En otras palabras, sabes que la red puede entregar un paquete de un host a otro y viceversa. ICMP no confiar en cualquier aplicación, por lo que realmente solo prueba la conectividad IP básica: las capas 1, 2 y 3 de el modelo OSI. La figura 5-16 describe el proceso básico.



CAPÍTULO 6

Fundamentos de TCP/IP

Transporte, Aplicaciones y Seguridad

Protocolos TCP/IP de capa 4: TCP y UDP

La capa de transporte OSI (Capa 4) define varias funciones, las más importantes son la recuperación de errores y el control de flujo.

La diferencia clave entre TCP y UDP es que, TCP brinda una amplia variedad de servicios a las aplicaciones, mientras que UDP no.

La Tabla 6-2 enumera las funciones principales admitidas por TCP y/o UDP.

Key Topic

Table 6-2 *TCP/IP Transport Layer Features*

Function	Description
Multiplexing using ports	Function that allows receiving hosts to choose the correct application for which the data is destined, based on the port number.
Error recovery (reliability)	Process of numbering and acknowledging data with Sequence and Acknowledgment header fields.
Flow control using windowing	Process that uses window sizes to protect buffer space and routing devices.
Connection establishment and termination	Process used to initialize port numbers and Sequence and Acknowledgment fields.
Ordered data transfer and data segmentation	Continuous stream of bytes from an upper-layer process that is "segmented" for transmission and delivered to upper-layer processes at the receiving device, with the bytes in the same order.

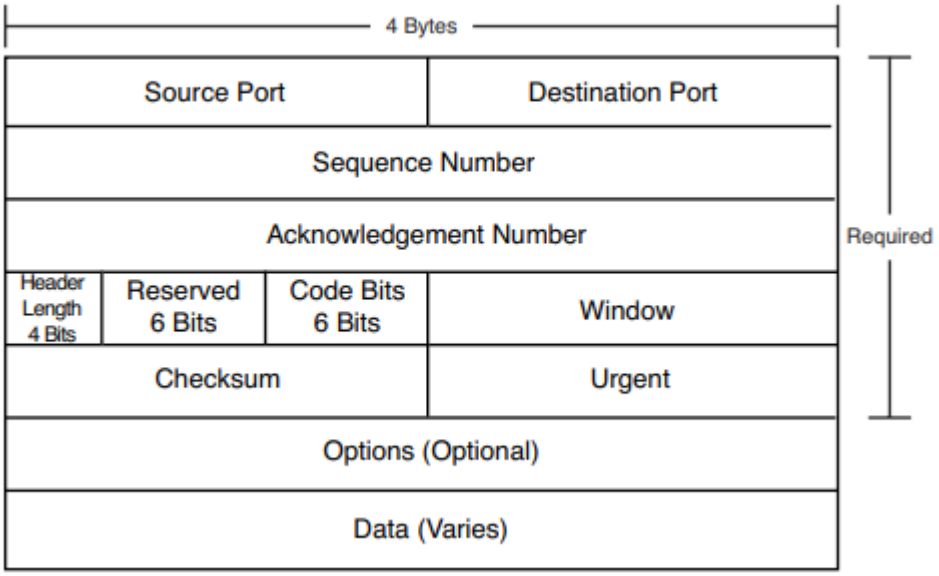
Next, this section describes the features of TCP, followed by a brief comparison to UDP.

Protocolo de Control de Transmisión

TCP, como se define en RFC 793, cumple las funciones enumeradas en la Tabla 6-2 a través de mecanismos en las computadoras de punto final. TCP se basa en IP para la entrega de datos de un extremo a otro, incluidos los problemas de enrutamiento. En otras palabras, TCP realiza solo una parte de las funciones necesarias para entregar los datos entre aplicaciones.

La Figura 6-1 muestra los campos en el encabezado TCP.

Figure 6-1 *TCP Header Fields*



Multiplexación mediante números de puerto TCP

La multiplexación por TCP y UDP implica el proceso de cómo piensa una computadora cuando recibe datos. La multiplexación TCP y UDP permite que la computadora receptora sepa a qué aplicación entregar los datos.

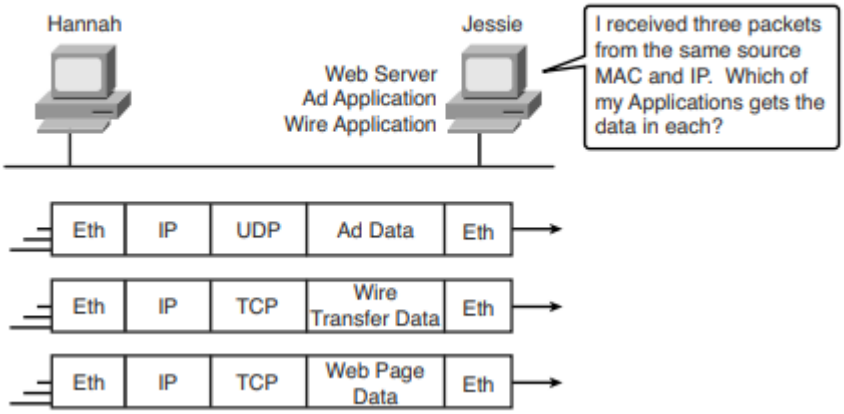
La Figura 6-2 muestra la red de muestra, con Jessie ejecutando tres aplicaciones:

■ Una aplicación de publicidad basada en UDP

■ Una aplicación de transferencia bancaria basada en TCP

■ Una aplicación de servidor web TCP

Figure 6-2 *Hannah Sending Packets to Jessie, with Three Applications*



La multiplexación se basa en un concepto llamado socket. Un socket consta de tres cosas:

■ Una dirección IP

■ Un protocolo de transporte

■ Un número de puerto

Figure 6-3 *Hannah Sending Packets to Jessie, with Three Applications Using Port Numbers to Multiplex*

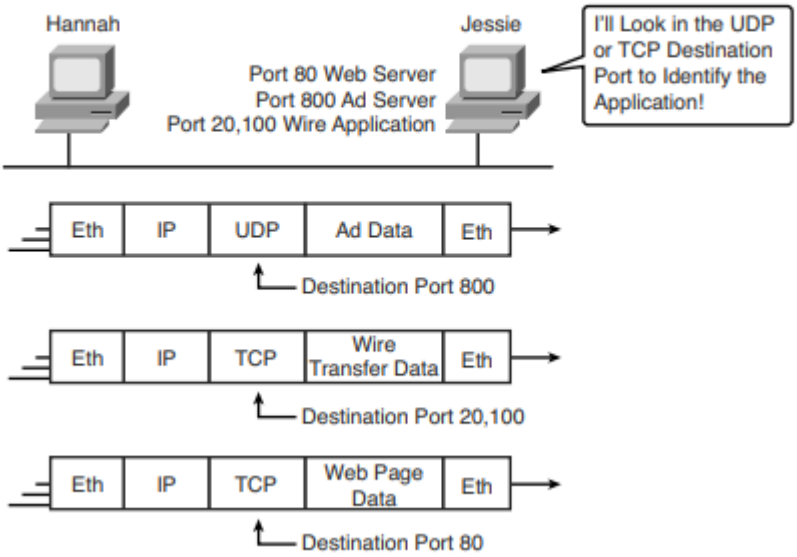
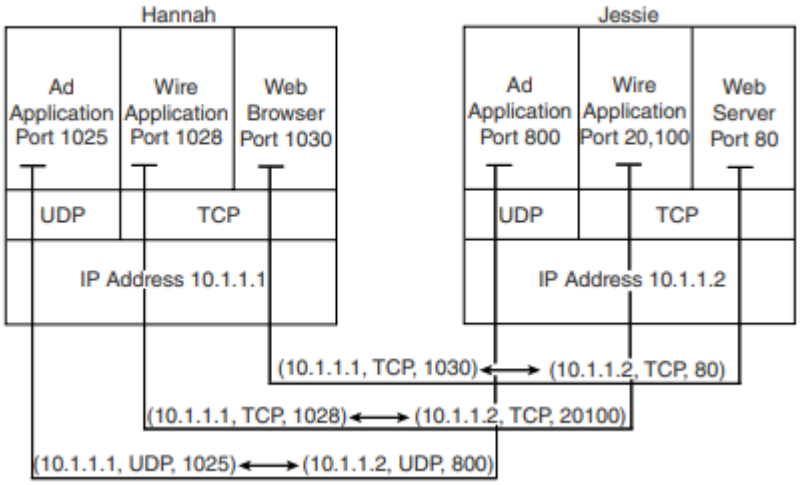


Figure 6-4 *Connections Between Sockets*



Aplicaciones populares de TCP/IP

La aplicación World Wide Web (WWW) existe a través de navegadores web que acceden al contenido disponible en los servidores web.

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.

Tradicionalmente, para mover archivos hacia y desde un enrutador o conmutador, Cisco utilizaba el Protocolo trivial de transferencia de archivos (TFTP). TFTP define un protocolo para la transferencia básica de archivos, de ahí la palabra "trivial".

TCP realiza la recuperación de errores, mientras que UDP no lo hace.

El Protocolo simple de transporte de correo (SMTP)

El Protocolo de oficina de correos versión 3 (POP3), ambos utilizados para transferir correo, requieren una entrega garantizada, por lo que utilizan TCP.

La Tabla 6-3 enumera varias aplicaciones populares y sus números de puerto conocidos.

Table 6-3 *Popular Applications and Their Well-Known Port Numbers*

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH

continues

Table 6-3 *Popular Applications and Their Well-Known Port Numbers (Continued)*

Port Number	Protocol	Application
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384–32,767	UDP	RTP-based Voice (VoIP) and Video

Recuperación de errores (confiabilidad)

TCP proporciona una transferencia de datos confiable, que también se denomina confiabilidad o recuperación de errores, según el documento que lea.

Control de flujo mediante ventanas

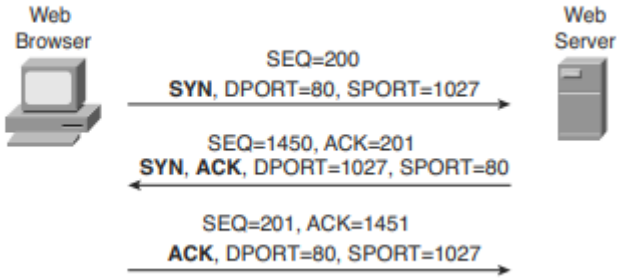
TCP implementa el control de flujo aprovechando los campos Secuencia y Reconocimiento en el encabezado TCP, junto con otro campo llamado campo Ventana. Este campo de Ventana implica el número máximo de bytes no reconocidos que pueden estar pendientes en cualquier instante de tiempo.

Establecimiento y terminación de la conexión

El establecimiento de la conexión TCP ocurre antes de que cualquiera de las otras funciones TCP pueda comenzar a funcionar. El establecimiento de la conexión se refiere al proceso de inicialización de los campos de secuencia y reconocimiento y de acuerdo sobre los números de puerto utilizados.

La Figura 6-8 muestra un ejemplo de flujo de establecimiento de conexión.

Figure 6-8 *TCP Connection Establishment*



TCP establece y finaliza las conexiones entre los puntos finales, mientras que UDP no lo hace.

Segmentación de datos y transferencia ordenada de datos

Las aplicaciones necesitan enviar datos. A veces, los datos son pequeños; en algunos casos, un solo byte. En otros casos, como con una transferencia de archivos, los datos pueden ser millones de bytes.

TCP maneja el hecho de que una aplicación puede darle millones de años para enviar segmentando los datos en partes más pequeñas, llamadas segmentos.

El receptor TCP realiza el reensamblado cuando recibe los segmentos.

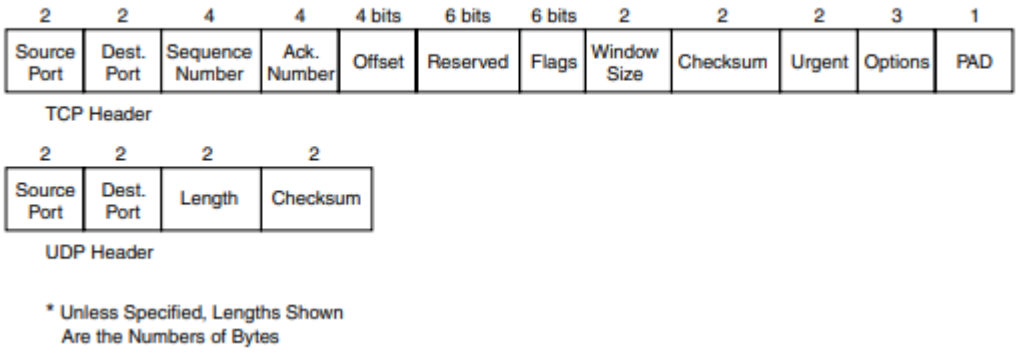
Protocolo de datagramas de usuario

UDP proporciona un servicio para que las aplicaciones intercambien mensajes. A diferencia de TCP, UDP no tiene conexión y no proporciona confiabilidad, ventanas, reordenación de los datos recibidos y segmentación de grandes porciones de datos en el tamaño correcto para la transmisión.

La transferencia de datos UDP se diferencia de la transferencia de datos TCP en que no se realiza ningún reordenamiento ni recuperación.

La Figura 6-10 muestra los formatos de encabezado TCP y UDP.

Figure 6-10 *TCP and UDP Headers*



Necesidades de QoS y el impacto de las aplicaciones TCP/IP

El término calidad de servicio (QoS) se refiere a todo el tema de lo que necesita una aplicación del servicio de red. Cada tipo de aplicación se puede analizar en términos de sus requisitos de QoS en la red, por lo que si la red cumple con esos requisitos, la aplicación funcionará bien.

La World Wide Web, HTTP y SSL

La World Wide Web (WWW) consta de todos los servidores web conectados a Internet en el mundo, además de todos los hosts conectados a Internet con navegadores web.

Localizadores universales de recursos

Para que un navegador muestre una página web, el navegador debe identificar el servidor que tiene la página web, además de otra información que identifica la página web en particular.

Cada URL define el protocolo utilizado para transferir datos, el nombre del servidor y la página web particular en ese servidor. La URL se puede dividir en tres partes:

■ El protocolo aparece antes de //.

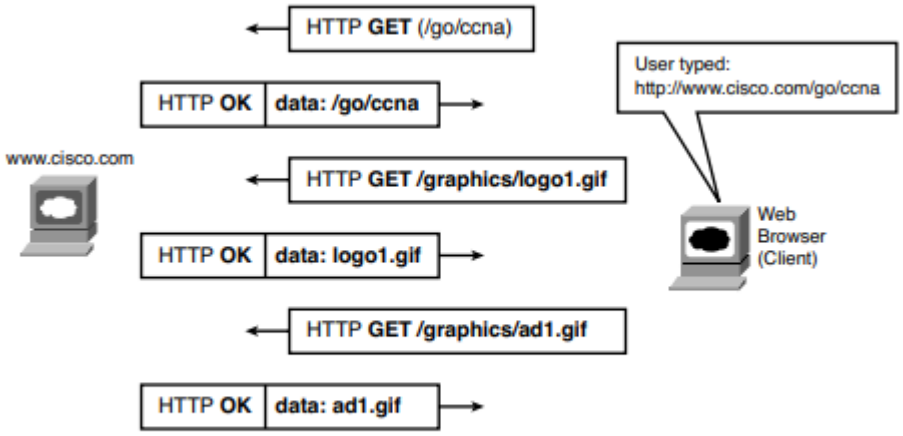
■ El nombre de host aparece entre // y /.

■ El nombre de la página web aparece después de /.

Transferencia de archivos con HTTP

Después de que un cliente web (navegador) haya creado una conexión TCP a un servidor web, el cliente puede comenzar a solicitar la página web del servidor. La mayoría de las veces, el protocolo utilizado para transferir la página web es HTTP. El protocolo de capa de aplicación HTTP, definido en RFC 2616, define cómo se pueden transferir archivos entre dos computadoras.

Figure 6-13 *Multiple HTTP Get Requests/Responses*

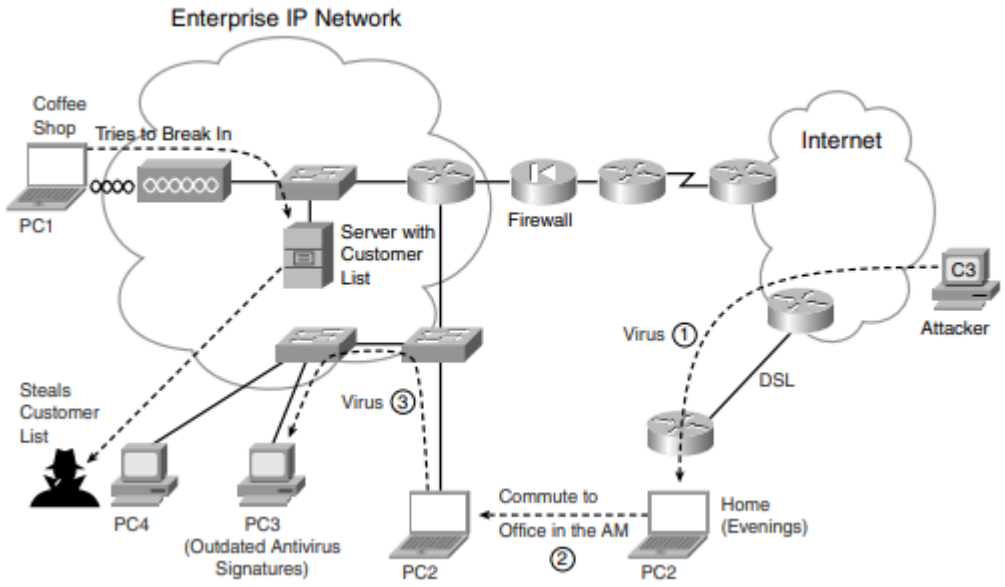


This chapter ends with an introduction to network security.

Seguridad de la red

La seguridad es claramente un gran problema y requiere una atención seria.

Figure 6-15 *Common Security Issues in an Enterprise*



Redes privadas virtuales (VPN)

La última clase de herramienta de seguridad presentada en este capítulo es la red privada virtual (VPN), que podría llamarse mejor WAN privada virtual.

Figure 6-17 *Sample VPNs*

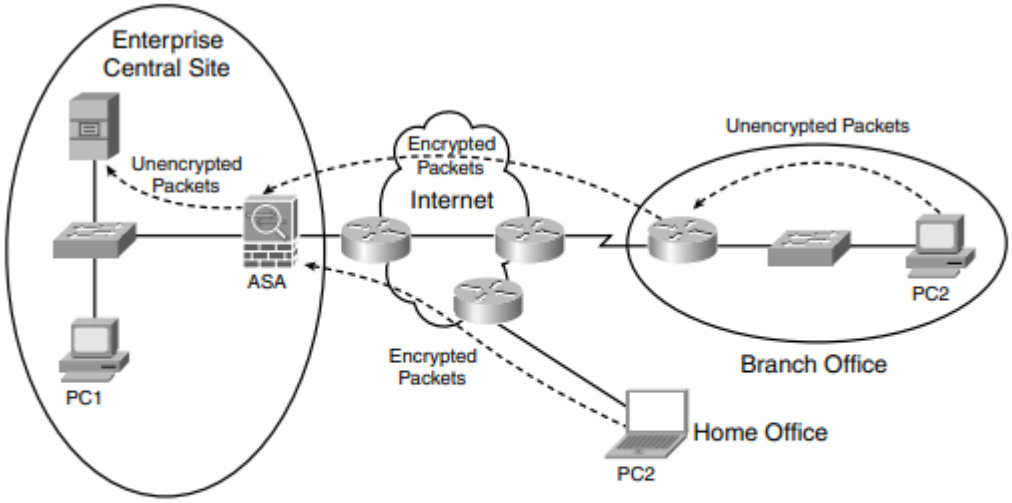


Figure 6-17 shows how VPNs can use end-to-end encryption, in which the data remains encrypted while being forwarded through one or more routers. Additionally, link encryption can be used to encrypt data at the data link layer, so the data is encrypted only as it passes over one data link. Chapter 11, "Wireless LANs," shows an example of link encryption.