Security+ Capítulo 1

Conceptos básicos y terminología de redes

OBJETIVOS DE CERTIFICACIÓN

1.01 Descripción de los dispositivos de red y el cableado

1.02 Descripción de TCP/IP

1.03 Prácticas recomendadas de seguridad de red

✓ Simulacro de dos minutos

Preguntas y respuestas

Cuando se prepare para su examen de certificación Security+, necesitará muchos conocimientos de redes, dispositivos de red y protocolos. Este capítulo revisa los conceptos básicos de las redes y garantiza que no solo esté familiarizado con las funciones de dispositivos como conmutadores y enrutadores, sino que también comprenda los conceptos básicos de los protocolos que existen en el conjunto de protocolos TCP / IP.

Este capítulo no está diseñado para ser una discusión completa de redes, lo que llevaría un libro entero. Aunque no es obligatorio, se recomienda que tenga experiencia en certificación de Network+ antes de realizar el examen de certificación de Security+.

OBJETIVO DE CERTIFICACIÓN 1.01

Descripción de los dispositivos de red y el cableado

Revisemos los fundamentos de los entornos de red repasando los conceptos de dispositivos de red y cableado. Es posible que no reciba preguntas directas sobre estos temas en el examen Security+, pero se espera que comprenda las implicaciones de seguridad del uso de los diferentes dispositivos y tipos de cables.

Mirando los dispositivos de red

Para realizar cualquier función de trabajo como profesional de la seguridad, debe estar familiarizado con una serie de dispositivos de red diferentes. Por ejemplo, se le puede solicitar que realice una auditoría de seguridad dentro de una organización, lo que implica identificar los dispositivos utilizados en la empresa y hacer recomendaciones sobre dispositivos más seguros para usar.

Concentrador

El concentrador de red es un dispositivo de red más antiguo que se usaba para conectar todos los sistemas en un entorno de red. El concentrador es un dispositivo de capa 1 del modelo OSI (Open Systems Interconnection) que simplemente recibe una señal de un sistema y luego envía la señal a todos los demás puertos del concentrador. Por ejemplo, mirando la Figura 1-1, puede ver que cuando el equipo A envía datos al equipo C, los datos se reciben en el puerto 1 del concentrador y luego se envían a todos los demás puertos.

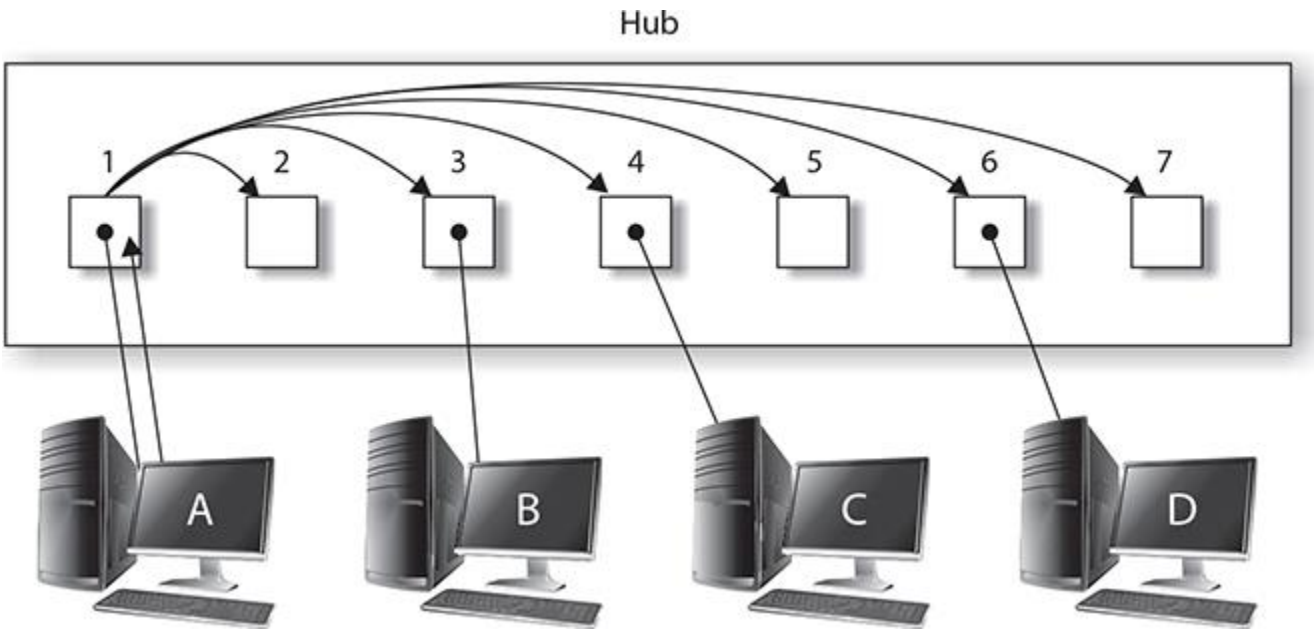


FIGURA 1-1

Observación del funcionamiento de un concentrador

El inconveniente del concentrador es que utiliza el ancho de banda al enviar los datos a todos los puertos del concentrador. ¿Por qué hacer eso si los datos tienen que enviarse solo a la computadora C? El otro inconveniente de un concentrador de red es que es un problema de seguridad si todos los sistemas de la red reciben los datos, aunque ignoran los datos porque no son para ellos. Las computadoras B y D podrían ver todo el tráfico en la red porque esas estaciones también reciben una copia del tráfico. Esta es una gran preocupación de seguridad y es una de las razones por las que la industria se ha alejado de los concentradores y utiliza conmutadores en su lugar.

Interruptor

Un conmutador de red es similar a un concentrador de red en el sentido de que se utiliza para conectar todos los sistemas en un entorno de red, pero la diferencia es que un conmutador es un dispositivo de capa 2 que filtra el tráfico por la dirección de capa 2. Recuerde del examen

Network+ que la dirección de capa 2 se conoce como la dirección de control de acceso a medios, o dirección MAC para abreviar. La dirección MAC es la dirección de hardware asignada a la tarjeta de red por el fabricante y se parece a 3C-97-0E-E3-52-5C.

Si observa el ejemplo anterior de la computadora A que envía datos a la computadora C con un conmutador que se está utilizando en su lugar, notará que el conmutador recibe los datos de la computadora A, pero luego filtra el tráfico enviando los datos solo al puerto en el que reside el sistema de destino, en este caso, el puerto 4 (consulte la Figura 1-2).

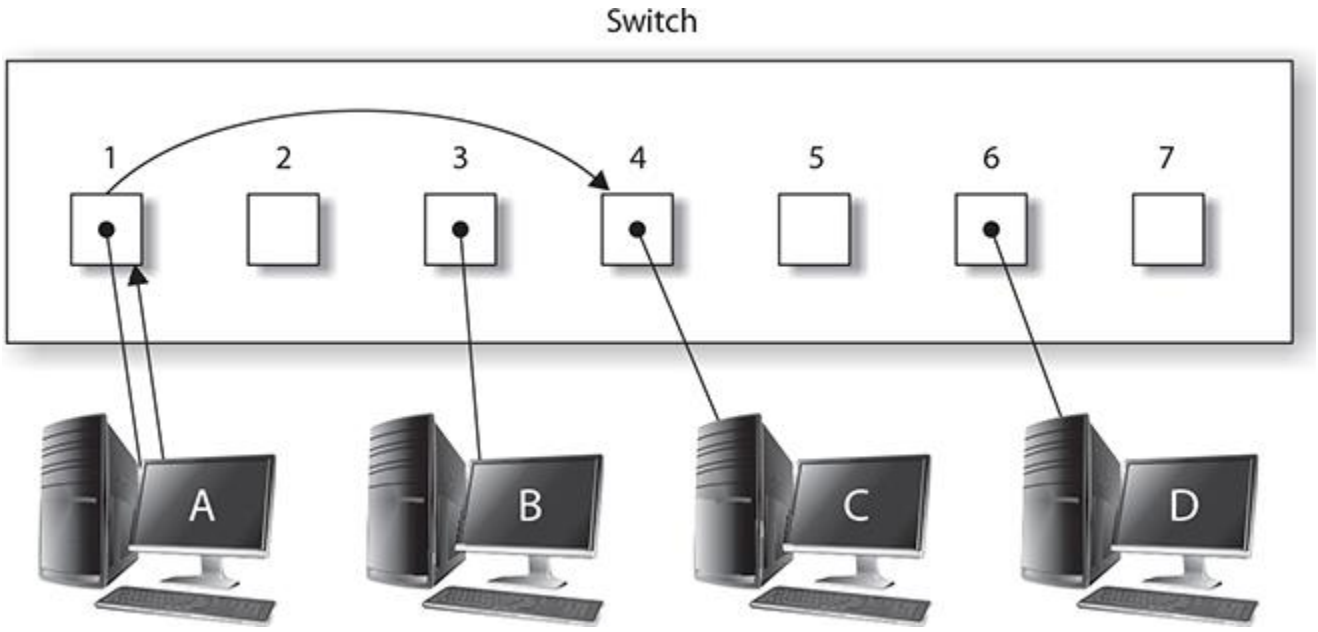


FIGURA 1-2

Observación de cómo un conmutador filtra el tráfico

El conmutador puede filtrar el tráfico porque almacena las direcciones MAC de cada sistema conectado al conmutador y a qué puerto está conectado ese sistema en la tabla de direcciones MAC. La tabla de direcciones MAC es una tabla almacenada en la memoria del conmutador y es responsable de rastrear a qué puertos está conectado cada sistema (consulte la Figura 1-3).

MAC address table

MAC	Port
00-1A-2C...	1
00-AB-BI...	3
00-2C-IB...	4
00-3B-4D...	6

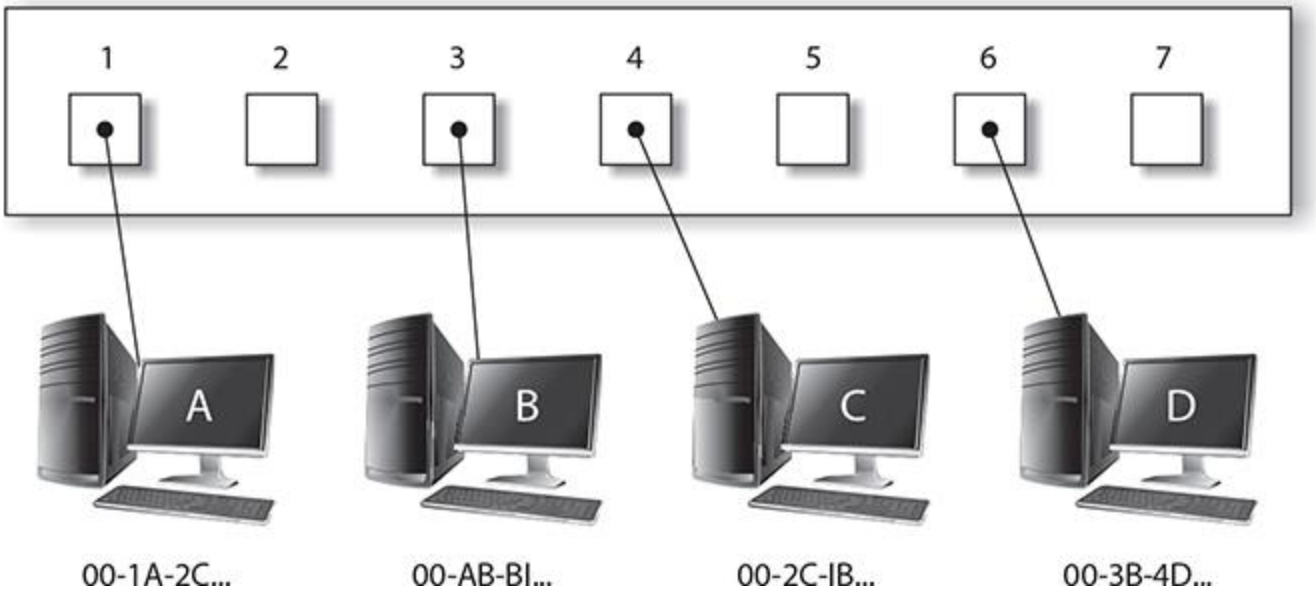


FIGURA 1-3

Mirando la tabla de direcciones MAC en un conmutador

Además de filtrar el tráfico enviando los datos solo al puerto en el que reside el sistema de destino, la mayoría de los conmutadores de red proporcionan los siguientes beneficios:

■ **Filtrado** Como se mencionó, un interruptor filtra el tráfico, lo que evita que otros capturen y vean información potencialmente confidencial.

■ **Duplicación de puertos** La duplicación de puertos, también conocida como supervisión de puertos, es una característica de algunos conmutadores que permite al administrador copiar el tráfico de otros puertos a un único puerto de destino (conocido como puerto de supervisión). Dado que el conmutador filtra el tráfico de forma predeterminada, el administrador no puede

supervisar el tráfico de red. Los proveedores de conmutadores tuvieron que idear una forma de copiar todo el tráfico a un solo puerto para que el administrador pudiera conectar su sistema de monitoreo a ese puerto. Los siguientes comandos se utilizan para configurar el puerto 12 (conocido como *interfaz)* en el conmutador para supervisar el tráfico enviado o recibido en los puertos 1 a 5:

```
HAL-SW1(config)#interface fastethernet 0/12
HAL-SW1(config-if)#port monitor fastethernet 0/1
HAL-SW1(config-if)#port monitor fastethernet 0/2
HAL-SW1(config-if)#port monitor fastethernet 0/3
HAL-SW1(config-if)#port monitor fastethernet 0/4
HAL-SW1(config-if)#port monitor fastethernet 0/5
```

■ **Seguridad portuaria** La seguridad portuaria es una característica de un conmutador de red que le permite configurar un puerto para una dirección MAC específica. Esto le permite controlar qué sistemas pueden conectarse a ese puerto en el conmutador. Cuando un sistema no autorizado se conecta al puerto del conmutador, el conmutador puede desactivar temporalmente el puerto hasta que el sistema correcto se conecte al conmutador o deshabilitar el puerto hasta que un administrador vuelva a habilitar el puerto. Los siguientes comandos se utilizan para configurar el puerto 6 en el conmutador Halifax para que acepte solo conexiones de una dirección MAC determinada. En este ejemplo, la dirección MAC es *aaaa.bbbb.cccc*, que reemplazaría con una dirección MAC real:

```
HAL-SW1(config)#interface f0/6
HAL-SW1(config-if)#switchport mode access
HAL-SW1(config-if)#switchport port-security
HAL-SW1(config-if)#switchport port-security mac-address aaaa
.bbbb.cccc
HAL-SW1(config-if)#switchport port-security maximum 1
HAL-SW1(config-if)#switchport port-security violation shutdown
```

■ **Capacidad para deshabilitar puertos** Si tiene puertos en el conmutador que no se están utilizando, es una práctica recomendada de seguridad deshabilitarlos para que no se puedan usar. Los siguientes comandos se utilizan para deshabilitar los puertos 7 a 12 en un switch Cisco con el comando **shutdown:**

```
HAL-SW1(config)#interface range f0/7–12
HAL-SW1(config-if-range)#shutdown
```

El examen de certificación Security+ no espera que conozca los comandos para configurar la seguridad del puerto o deshabilitar un puerto en un switch Cisco, pero sí espera que comprenda las características del switch que ofrecen seguridad.

Dominios de colisión Otra característica importante de un conmutador se conoce como dominio de *colisión,* que es un grupo de sistemas que comparten el mismo segmento de red y, por lo tanto, pueden hacer que sus datos colisionen entre sí. Todos los puertos de un concentrador crean un único dominio de colisión, pero cada puerto de un conmutador crea un dominio de colisión independiente. Por ejemplo, cuando se utiliza un concentrador de red, si dos sistemas enviaran datos al mismo tiempo, se provocaría una colisión de datos. Esto se debe a que el concentrador crea un segmento de red "compartido" al que todos los sistemas tienen acceso. Con un conmutador, cada puerto del conmutador crea un dominio de colisión independiente que es su propio segmento de red. Al conectar un sistema a un puerto en un conmutador, debido a que no hay ningún otro sistema en el segmento de red, no habrá colisiones de datos.

Para el examen, recuerde que un switch ofrece una gran seguridad porque filtra el tráfico enviando el tráfico solo al puerto en el que reside el sistema de destino. También debe poder describir características como la seguridad de puertos, la creación de reflejo de puertos y la capacidad de deshabilitar puertos no utilizados.

VLAN La mayoría de los switches de hoy en día admiten una característica conocida como LAN virtual (VLAN). El propósito de una VLAN es crear múltiples redes dentro de un conmutador de red. Una forma de hacerlo es colocando puertos en el switch en agrupaciones de VLAN. Cuando un sistema está conectado a un puerto en el switch, se convierte en miembro de la VLAN a la que está asociado el puerto. El punto importante es que cuando un sistema es miembro de una VLAN, no puede comunicarse con sistemas en otra VLAN. Es como si cada VLAN tuviera su propio switch sin conexión a otro switch. La figura 1-4 muestra un conmutador configurado en dos VLAN. En este ejemplo, el equipo A sólo puede comunicarse con el equipo B porque son los únicos sistemas de VLAN1. El equipo A y el equipo B no pueden comunicarse con el equipo C y el equipo D porque no se permite la comunicación a través de VLAN sin un enrutador.

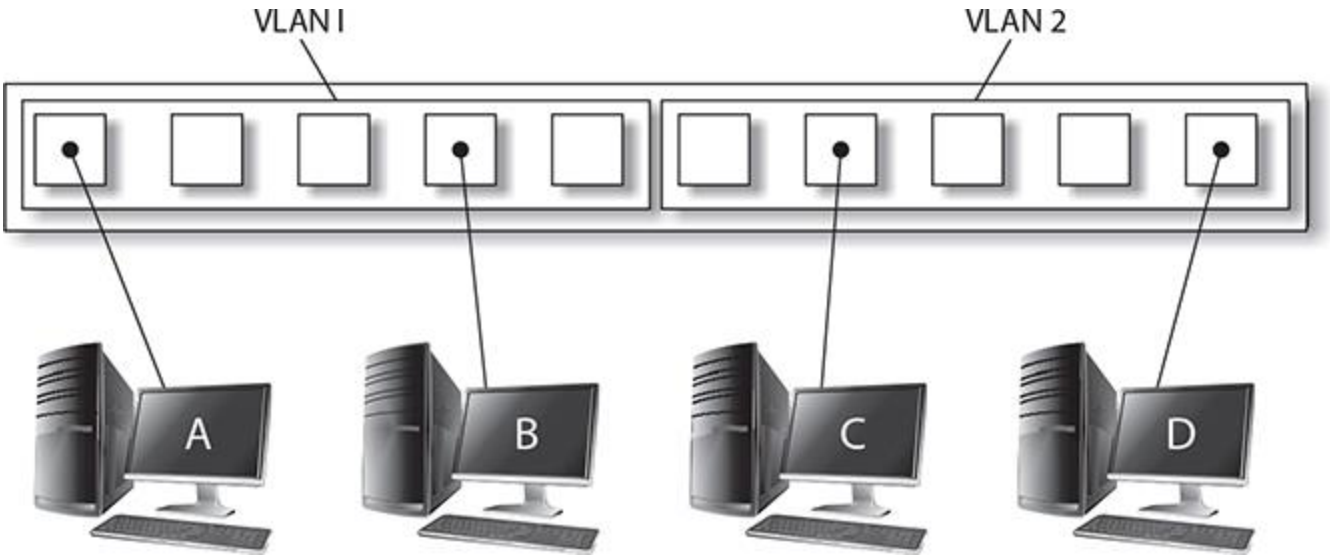


FIGURA 1-4

Observación de las VLAN en un conmutador

El código siguiente muestra cómo configurar VLAN en un switch Cisco Catalyst. En este ejemplo se muestran dos VLAN: PrivateLAN y WebServers:

```
HAL-SW1>enable
HAL-SW1#config term
HAL-SW1(config)#vlan 2
HAL-SW1(config-vlan)#name PrivateLAN
HAL-SW1(config-vlan)#exit
HAL-SW1(config)#vlan 3
HAL-SW1(config-vlan)#name WebServers
HAL-SW1(config-vlan)#exit
```

Una vez que se han creado las VLAN, se colocan diferentes puertos en VLAN particulares. Por ejemplo, los siguientes comandos colocan los puertos 18 a 24 en la VLAN de WebServers:

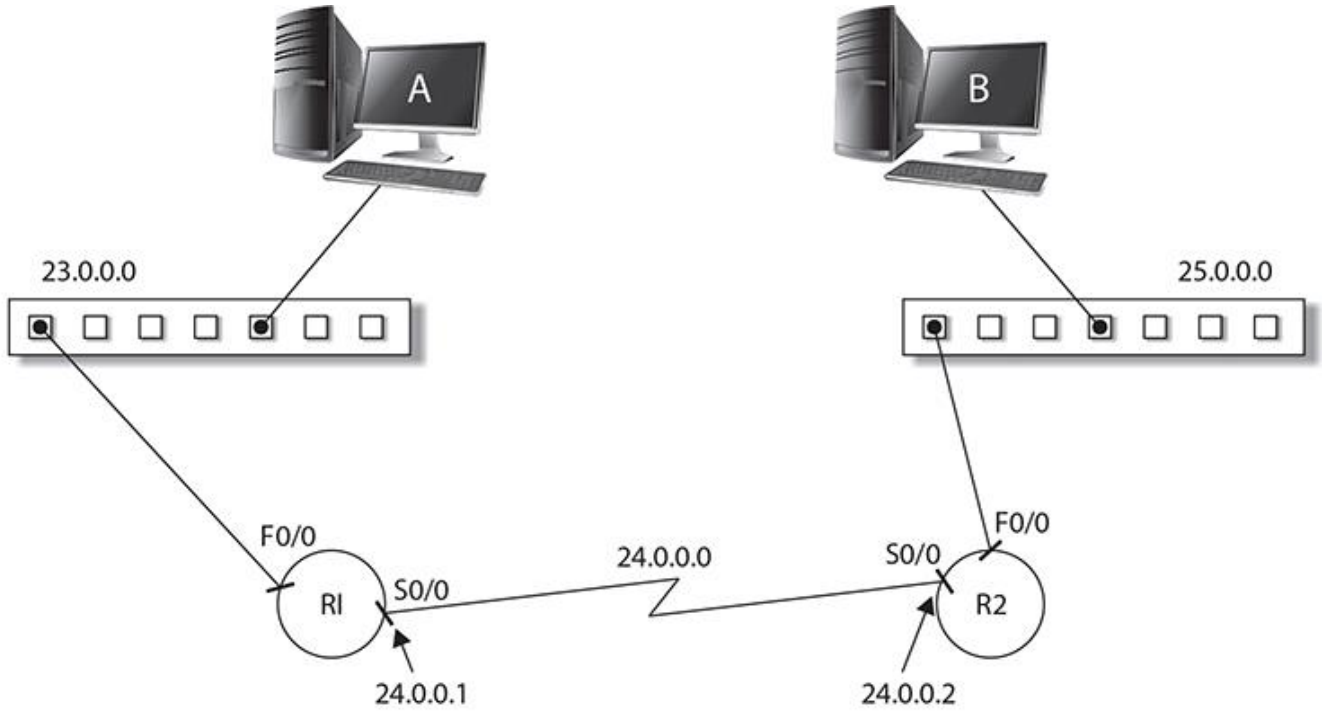
```
HAL-SW1(config-if-range)#interface range f0/18 – 24
HAL-SW1(config-if-range)#switchport access vlan 3
```

Cabe señalar que puede vincular varios conmutadores y crear VLAN en todos los conmutadores. Por ejemplo, puede tener algunos puertos en cada uno de los conmutadores 1, 2 y 3 que forman parte de la VLAN de WebServers. El puerto de enlace ascendente que conecta los switches transportará el tráfico VLAN a cada switch.

Para el examen, recuerde que las VLAN son una forma de crear límites de comunicación en la red. De forma predeterminada, los sistemas de una VLAN no pueden comunicarse con los sistemas de otra VLAN.

Enrutador

Un enrutador es un dispositivo de capa 3 que es responsable de enrutar o enviar datos de una red a otra red. El router utiliza una tabla de enrutamiento que reside en su memoria para determinar las redes a las que sabe cómo enviar datos. La figura 1-5 muestra una topología de red y la tabla de enrutamiento en un enrutador. Observe en la figura que para que el enrutador R1 envíe datos a la red 25.0.0.0, debe enviar los datos a la dirección 24.0.0.2, como lo indica la tabla de enrutamiento.



Routing table

Network	Path
23.0.0.0	F0/0
24.0.0.0	S0/0
25.0.0.0	24.0.0.2

FIGURA 1-5 Los

routers utilizan tablas de enrutamiento para entregar datos.

La siguiente lista de código muestra la tabla de enrutamiento en un router Cisco mediante el comando **show ip route.** Observe en el listado que hay tres rutas; las rutas a la red 23.0.0.0 y 24.0.0.0 se conocen porque el enrutador está conectado a esas redes (observe la **C** a la izquierda). Además, se ha configurado una ruta estática (código **S,**a la izquierda) que el administrador agregó para pasar datos al sistema 24.0.0.2 para llegar a la red 25.0.0.0.

```
HAL-R1#show ip route
Codes: C—connected, S—static, I—IGRP, R—RIP, ...
 (Additional codes omitted for briefness)
Gateway of last resort is not set
S   25.0.0.0 [1/0] via 24.0.0.2
C   24.0.0.0/8 is directly connected, Serial0/0/0
C   23.0.0.0/8 is directly connected, FastEthernet0/1
```

Los enrutadores son excelentes dispositivos de red porque definen el límite de la red creando lo que se llama un dominio de *difusión,* que es un grupo de sistemas que pueden recibir los mensajes de difusión de los demás. Un mensaje de difusión es un mensaje destinado a todos los sistemas, y el enrutador se coloca estratégicamente en la red para mantener esos mensajes de difusión dentro de la red porque el tráfico de difusión no pasa a través del enrutador.

Equilibrador de carga

Un *equilibrador de carga* es un dispositivo que está diseñado para dividir la carga entre componentes como servidores o enrutadores. El equilibrio de carga es el concepto de tratar de mejorar el rendimiento. En lugar de tener un solo servidor o dispositivo que maneje todo el trabajo, tiene varios servidores o dispositivos entre los que se divide la carga de trabajo. Esto aumenta el rendimiento general porque tiene más sistemas trabajando al mismo tiempo para manejar todas las solicitudes entrantes.

Los equilibradores de carga tienen una serie de opciones que le permiten configurar cómo funciona el equilibrador de carga:

■ **Round-robin** Envía la solicitud de un cliente a cada servidor back-end en orden. El equilibrador de carga tiene una lista de servidores y simplemente los revisa en orden.

■ **Affinity** Controla si todas las solicitudes de un cliente van al mismo servidor en el equilibrador de carga o si cada solicitud puede enrutarse a un servidor diferente. La afinidad esencialmente vincula a un cliente a un servidor en particular.

■ **Persistencia** Este es otro método utilizado para asociar un cliente con un servidor específico dentro del equilibrador de carga. Con persistencia, la cookie de sesión del usuario se utiliza para garantizar que el mismo servidor esté manejando todas las solicitudes del cliente (esto también se conoce como sesión adhesiva). Esta cookie de sesión podría provenir de la aplicación o del propio equilibrador de carga.

■ **Programación** Especifica qué algoritmo se utilizará para enviar la solicitud a uno de los nodos. La programación utiliza una serie de valores de configuración, como round-robin, afinidad y carga de CPU, para determinar a qué servidor enviar la solicitud.

Activo/Pasivo vs. Activo/Activo Hay dos configuraciones comunes para el equilibrio de carga. Con una configuración *activa/pasiva,* un sistema, llamado nodo, maneja todo el trabajo (el nodo activo), mientras que el otro nodo (el nodo pasivo) está en espera, listo para hacerse cargo si el nodo activo falla. Si el nodo activo falla, el nodo pasivo se convierte en el nodo activo y maneja toda la carga de trabajo. Con una configuración *activa/activa,* ambos nodos están en línea y pueden manejar solicitudes, esencialmente dividiendo la carga de trabajo. Si se produce un error en un nodo, el otro nodo controla toda la carga de trabajo hasta que se recupera el nodo con error. Con ambas configuraciones, se pueden incluir más de dos nodos para una redundancia adicional.

Con ambas configuraciones, el equilibrador de carga tiene una dirección IP asignada (conocida como *IP virtual)*y se configuran todos los clientes para que envíen solicitudes a la IP virtual asignada al equilibrador de carga. Cuando el equilibrador de carga recibe una solicitud enviada a la IP virtual, reenvía la solicitud a un nodo activo en el equilibrador de carga.

DNS Round-Robin Otra técnica de equilibrio de carga se conoce como DNS round-robin. Con round-robin, la solución de equilibrio de carga simplemente envía la solicitud al siguiente servidor de su lista. El problema con el round robin es que la solución no verifica si ese servidor está realmente en funcionamiento sin problemas. Un ejemplo de equilibrio de carga round-robin es el uso del Sistema de Nombres de Dominio (DNS). Puede crear varios registros DNS con el mismo nombre pero diferentes direcciones IP, y el servidor DNS enviará una dirección IP diferente con cada respuesta a los clientes. El problema es que el servidor DNS no verifica que esas direcciones IP sean utilizadas por los sistemas que están en funcionamiento.

Firewalls y servidores proxy

Aprenderá más sobre firewalls y servidores proxy en el Capítulo 8,pero esta sección le brinda una descripción rápida del propósito de un firewall y un servidor proxy para presentarlos como dispositivos de red.

Un *firewall* es un dispositivo de red que controla qué tráfico puede entrar o salir de la red. El firewall filtra el tráfico en función de las reglas que coloque en el firewall que indiquen qué tráfico está permitido o no para entrar o salir de la red. Normalmente, se comienza con una

regla de denegación de todo que indica que todo el tráfico está denegado, a menos que especifique lo contrario mediante la creación de una regla para un tipo específico de tráfico.

Para el examen Security+, recuerde que un servidor proxy realiza la solicitud del recurso de Internet en nombre del usuario y, por lo general, la empresa filtra y registra qué sitios web han visitado los usuarios.

Un *servidor proxy* es un dispositivo al que todos los clientes envían su tráfico de Internet y, a continuación, el servidor proxy envía las solicitudes a Internet en nombre de los usuarios. El servidor proxy normalmente también implementa la traducción de direcciones de red (NAT), lo que ayuda a mantener la estructura de red interna privada del mundo exterior. Hay proxies transparentes que no requieren que el usuario se autentique, pero también hay productos de servidor proxy que requieren que el cliente se autentique antes de poder navegar por Internet. Esto ayuda a controlar los sitios que puede visitar cada usuario y también permite al administrador del proxy registrar qué sitios está visitando cada usuario. Como nota final sobre los servidores proxy, también hay proxies inversos, que le permiten recibir todo el tráfico entrante (como el tráfico a un servidor web), analizar las solicitudes y solo permitir que las solicitudes seguras y válidas lleguen al servidor web.

Descripción del cableado de red

El cableado es el medio de transmisión de los datos enviados entre hosts en la LAN. Los sistemas en la LAN se pueden conectar entre sí utilizando una variedad de tipos de cables, como el par trenzado sin blindada y la fibra. Cada tipo de cable tiene sus propias ventajas y desventajas, que examinará en esta sección.

Los dos tipos principales de medios de cable que se pueden utilizar para conectar sistemas a una red son el cable de par trenzado y el cable de fibra óptica. Las velocidades de transmisión admitidas en cada uno de estos medios físicos se miden en millones de bits por segundo, o megabits por segundo (Mbps).

Cable de par trenzado

Hoy en día, el cableado de par trenzado domina el concurso de popularidad. El cableado de par trenzado recibe su nombre de tener cuatro pares de cables que se retuercen para ayudar a reducir la diafonía o la interferencia de dispositivos eléctricos externos. La diafonía es la interferencia de los cables adyacentes. La figura 1-6 muestra un cable de par trenzado. Así como hay dos formas de cable coaxial, hay dos formas de cableado de par trenzado: par trenzado sin blindaje (UTP) y par trenzado blindado (STP).

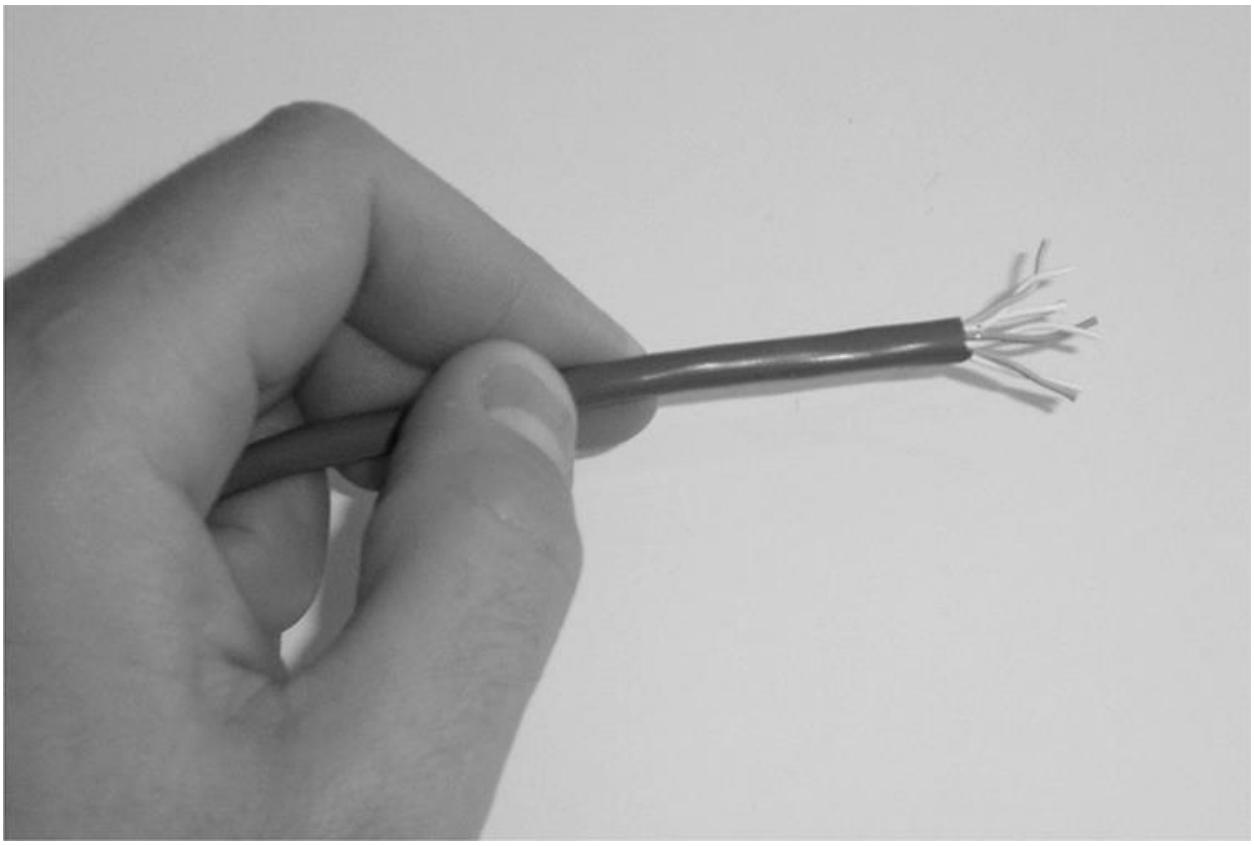


FIGURA 1-6

Cable de par trenzado sin blindar (UTP)

Cable de par trenzado sin blindada Los cables UTP le son familiares si ha trabajado con cable telefónico. El cable de par trenzado típico para uso en red contiene cuatro pares de cables. Cada miembro del par de cables contenidos en el cable se tuerce alrededor del otro. Los giros en los cables ayudan a proteger contra la interferencia electromagnética. La distancia máxima de UTP es de 100 metros.

El cable UTP utiliza pequeños conectores de plástico designados como jack 45 registrado, más a menudo conocido como RJ-45. RJ-45 es similar a los conectores telefónicos, excepto que en lugar de cuatro cables, como se encuentra en el sistema doméstico, el conector RJ-45 de red contiene ocho contactos, uno por cada cable en un cable UTP.

Puede ser fácil confundir el conector RJ-45 con el conector RJ-11. El conector RJ-11 es un conector telefónico y tiene cuatro contactos; por lo tanto, hay cuatro cables que se encuentran en el cable telefónico. Con RJ-45 y RJ-11, necesitará una herramienta de engarce especial al crear los cables para hacer contacto entre los pines del conector y los cables dentro del cable.

El cable UTP es más fácil de instalar que el coaxial porque puede tirar de él por las esquinas más fácilmente debido a su flexibilidad y pequeño tamaño. Sin embargo, el cable de par trenzado es

más susceptible a la interferencia que el coaxial y no debe usarse en entornos que contengan dispositivos eléctricos grandes.

El cableado UTP tiene diferentes sabores conocidos como grados o categorías. Cada categoría de cableado UTP fue diseñada para un tipo específico de comunicación o velocidad de transferencia. La Tabla 1-1 resume las diferentes categorías de UTP, la más popular hoy en día es CAT 5e, que puede alcanzar velocidades de transferencia de más de 1.000 Mbps, o 1 gigabit por segundo (Gbps).

TABLA 1-1

Cableado de categoría UTP diferente

UTP Category	Purpose	Transfer Rate
Category 1	Voice only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps (1,000 Mbps)
Category 6	Data	10 Gbps

Cuando trabaje en una red que utiliza cableado UTP, se encontrará con diferentes tipos de cable para diferentes propósitos. Por ejemplo, a veces usará un cable recto o un cable cruzado.

Cable recto El cableado CAT 5 UTP generalmente utiliza solo cuatro cables al enviar y recibir información en la red. Los cuatro cables de los ocho que se utilizan son los cables 1, 2, 3 y 6. La Figura 1-7 muestra los pines de transmisión y recepción en una computadora y los pines en un interruptor, que es a lo que normalmente conectará las computadoras. Cuando se configura el cable para el mismo pin en cada extremo del cable, esto se conoce como cable recto.

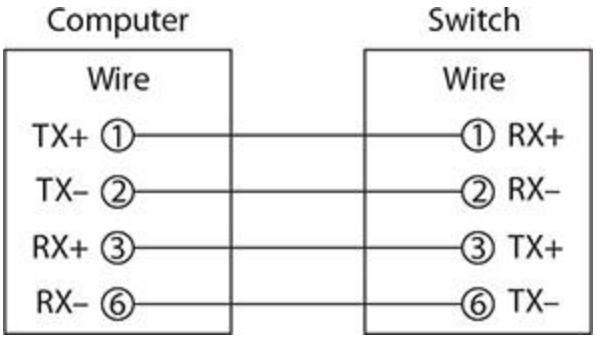


FIGURA 1-7

Diagrama de pines para un cable recto

Notarás en la figura que los cables 1 y 2 se utilizan para transmitir datos (TX) desde el ordenador, mientras que los cables 3 y 6 se utilizan para recibir información (RX) en el ordenador. También notará que el pin de transmisión (TX) en la computadora está conectado al pin de recepción (RX) en el interruptor a través de los cables 1 y 2. Esto es importante porque desea asegurarse de que los datos enviados desde el equipo sean recibidos por el conmutador. También debe asegurarse de que los datos enviados desde el conmutador se reciban en la computadora, por lo que notará que los pines de transmisión (TX) en el interruptor están conectados a los pines de recepción (RX) en la computadora a través de los cables 3 y 6. Esto permitirá que la computadora reciba información del interruptor.

Lo último a tener en cuenta sobre la Figura 1-7 es que el pin 1 en la computadora está conectado al pin 1 en el interruptor por el mismo cable, de ahí el término *directo.* Notarás que todos los pines se emparejan directamente con el otro lado en la Figura 1-7.

Cable cruzado En algún momento, es posible que deba conectar dos sistemas informáticos directamente juntos sin el uso de un conmutador de tarjeta de red a tarjeta de red. O puede encontrar que necesita conectar un interruptor a otro interruptor. En cualquier escenario en el que esté conectando dispositivos similares entre sí, no podría usar un cable recto porque el pin de transmisión en un extremo estaría conectado al pin de transmisión en el otro extremo, como se muestra en la Figura 1-8. ¿Cómo podría una computadora recoger los datos no enviados a los pines de recepción? Dado que esto no funcionará, deberá cambiar el cableado del cable a lo que se conoce como cable cruzado.

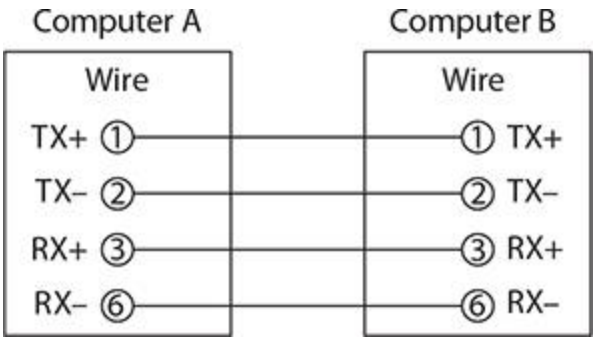


FIGURA 1-8

El uso de un cable recto para conectar dos computadoras no funcionará.

Para conectar dos sistemas directamente entre sí sin el uso de un interruptor, deberá crear un cable cruzado conmutando los cables 1 y 2 con los cables 3 y 6 en un extremo del cable, como se muestra en la Figura 1-9. Notará que los pines de transmisión en la Computadora A están conectados a los pines de recepción en la Computadora B, lo que permite que la Computadora A envíe datos a la Computadora B. Lo mismo se aplica a la computadora B para enviar a la computadora A: los pines 1 y 2 en la computadora B están conectados a los pines 3 y 6 en la computadora A para que la computadora A pueda recibir datos de la computadora B.

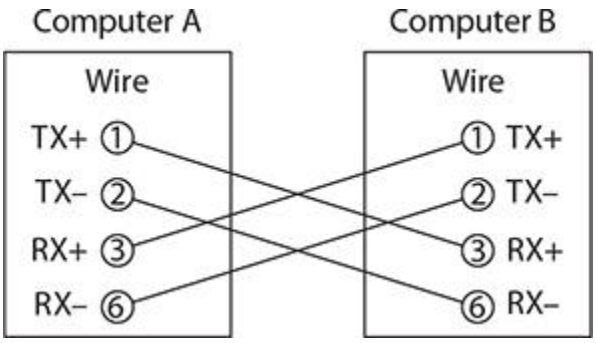


FIGURA 1-9

Diagrama de pines de un cable cruzado

on the job **La mayoría de los administradores de red usarán un determinado color de cable (como amarillo) para representar los cables cruzados y usarán un cable de color diferente para representar los cables rectos para evitar confundir los dos tipos de cableado.**

Cable blindado de par trenzado El cable STP es muy similar al cableado UTP, pero se diferencia del UTP en que utiliza una capa de aislamiento dentro de la camisa protectora, lo que ayuda a mantener la calidad de la señal.

Cable de fibra óptica

El segundo tipo de cableado a discutir es el cableado de fibra óptica. El cableado de fibra óptica es diferente al par trenzado porque el par trenzado utiliza un cable de cobre para transportar la señal eléctrica. Los cables de fibra óptica utilizan fibras ópticas que transportan señales de datos digitales en forma de pulsos de luz modulados. Una fibra óptica consiste en un cilindro de vidrio extremadamente delgado, llamado núcleo, rodeado por una capa concéntrica de vidrio, conocida como el revestimiento. Hay dos fibras por cable: una para transmitir y otra para recibir. El núcleo también puede ser un plástico transparente de calidad óptica, y el revestimiento puede estar hecho de gel que refleja las señales en la fibra para reducir la pérdida de señal.

Hay dos tipos de cables de fibra óptica:

■ **Fibra monomodo (SMF)** Utiliza un solo rayo de luz, conocido como modo, para transportar la transmisión a largas distancias

■ **Fibra multimodo (MMF)** Utiliza múltiples rayos de luz (modos) simultáneamente, con cada rayo de luz corriendo en un ángulo de reflexión diferente para llevar la transmisión a distancias cortas

Recuerde para el examen que la fibra óptica es un tipo de cable más seguro de usar porque no lleva una señal eléctrica, sino que transporta datos como pulsos de luz.

El cable de fibra óptica admite hasta 1.000 estaciones y puede transportar la señal hasta y más allá de los 2 kilómetros. Los cables de fibra óptica también son altamente seguros de la interferencia externa de cosas como transmisores de radio, soldadores de arco, luces fluorescentes y otras fuentes de ruido eléctrico. Por otro lado, el cable de fibra óptica es, con mucho, el más caro de estos métodos de cableado, y es poco probable que una red pequeña necesite estas características.

Los cables de fibra óptica pueden utilizar muchos tipos de conectores, como el conector de punta recta (ST), el conector Lucent (LC) y el conector de abonado (SC). El conector ST se basa en el conector de estilo BNC, pero tiene un cable de fibra óptica en lugar de un cable de cobre. El conector SC es cuadrado y algo similar a un conector RJ-45, mientras que el conector LC es la mitad del tamaño del conector SC y está diseñado para áreas donde se utiliza mucho cableado, como un panel de conexión.

Independientemente del tipo de conector, el cable de fibra óptica funciona a la misma velocidad, que suele ser de 1.000 Mbps y más rápida. Lo único de lo que debe preocuparse es

que el conector coincida con el dispositivo al que se está conectando, ya que los dos tipos de conectores no son intercambiables.

Al prepararse para el examen Security+, a veces es útil tener una tabla que enumere las diferencias entre los tipos de cable. La Tabla 1-2 resume los diferentes tipos de cables; asegúrese de revisarlo para el examen Security+.

TABLA 1-2

Resumen de los tipos de cables

Cable	Max Distance	Transfer Rate	Connector Used
CAT 3 (UTP)	100 m	10 Mbps	RJ-45
CAT 5 (UTP)	100 m	100 Mbps	RJ-45
CAT 5e	100 m	1 Gbps	RJ-45
CAT 6	100 m	10 Gbps	RJ-45
Fiber-optic	2 km	1+ Gbps	SC, ST, or LC

EJERCICIO 1-1

Revisión de componentes de red

En este ejercicio, pondrá en uso su conocimiento de los cables y dispositivos de red haciendo coincidir los términos con el escenario apropiado.

Device	Scenario
____ Switch	A. A group of systems that can have their data collide with one another
____ Load balancer	B. A communication boundary
____ UTP	C. A layer-3 device that sends data from one network to another
____ Port security	D. A layer-2 device that filters traffic based on MAC address
____ VLAN	E. A device that is used to split the workload between multiple servers
____ Router	F. A cable type that carries pulses of light
____ Collision domain	G. A type of cable that has copper wires divided into pairs
____ Fiber-optic	H. Controlling which MAC addresses can connect to the switch

OBJETIVO DE CERTIFICACIÓN 1.02

Descripción de TCP/IP

Ahora que comprende algunos de los diferentes tipos de dispositivos de red que se utilizan en las redes y los tipos de cable que se utilizan, cambiemos de dirección hablando del protocolo TCP / IP. Como profesional de la seguridad, es fundamental que no solo esté familiarizado con el protocolo TCP/IP, sino que también comprenda cómo se produce la comunicación en una red TCP/IP. Comencemos con una revisión rápida de los conceptos básicos del protocolo.

Revisión del direccionamiento IP

TCP/IP requiere un poco de conocimiento para configurar los sistemas correctamente. Al configurar TCP/IP, debe conocer la configuración de la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Comencemos con la dirección IP.

Dirección IP

La dirección IP es un valor de 32 bits que identifica de forma única el sistema en la red (o Internet). Una dirección IP se ve similar en apariencia a 192.168.1.15. Los cuatro valores decimales de una dirección IP están separados por puntos decimales. Cada valor se compone de 8 bits (1 y 0), por lo que con cuatro valores decimales, 8 bits × 4 = la dirección de 32 bits.

Dado que cada uno de los valores decimales está formado por 8 bits (por ejemplo, el 192), nos referimos a cada uno de los valores decimales como un octeto. Cuatro octetos están en una dirección IP. Es muy importante entender que los cuatro octetos en una dirección IP se dividen en dos partes: un *ID de red* y un *ID de host.* La máscara de subred determina el número de bits que componen el ID de red y el número de bits que componen el ID de host. Veamos cómo funciona esto.

Máscara de subred

Al mirar una máscara de subred, si hay un 255 en un octeto, entonces el octeto correspondiente en la dirección IP es parte del ID de red. Por ejemplo, si tuviera una dirección IP de 192.168.1.15 y una máscara de subred de 255.255.255.0, los tres primeros octetos conformarían el ID de red y el último octeto sería el ID de host. El ID de red asigna una dirección única a la propia red, mientras que el ID de host identifica de forma única el sistema en la red. La Tabla 1-3 resume este ejemplo.

TABLA 1-3

Identificación de las partes de ID de red e ID de host de una dirección IP

	Octet 1	Octet 2	Octet 3	Octet 4
IP address	192	168	1	15
Subnet mask	255	255	255	0
Address portion	N	N	N	H

Puede ver en la Tabla 1-3 que el ID de red (que se muestra con una *N)* es 192.168.1, y el ID de host es el último octeto con un valor de 15. Esto significa que este sistema está en la red 192.168.1, y cualquier otro sistema en la misma red tendrá el mismo ID de red.

Para usar un ejemplo diferente, si tuviera una máscara de subred de 255.0.0.0, significaría que el primer octeto de la dirección IP se usa como la parte de ID de red, mientras que los últimos tres octetos son la parte de ID de host de la dirección IP.

Entonces, ¿cuál es el propósito de la máscara de subred? O mejor aún, ¿por qué tenemos una máscara de subred que divide la dirección IP en una ID de red y una ID de host? Porque cuando un sistema como 192.168.1.15 con una máscara de subred de 255.255.255.0 envía un dato a 192.198.45.10, el sistema de envío primero debe determinar si el equipo de destino existe en la misma red. Para ello, compara los datos de red (véase el cuadro 1-4); si los datos de red son los mismos, entonces ambos sistemas existen en la misma red, y un sistema puede enviar al otro sin el uso de un enrutador. Si los sistemas existen en diferentes redes, los datos deberán pasarse al enrutador para que el enrutador pueda enviar los datos a la otra red.

TABLA 1-4

Identificación de dos sistemas en diferentes redes utilizando las máscaras de subred

	Octet 1	Octet 2	Octet 3	Octet 4
IP address #1	192	168	1	15
Subnet mask	255	255	255	0
IP address #2	192	198	45	10

Puerta de enlace predeterminada

Cuando su sistema desea enviar datos a otro sistema en la red, mira su propio ID de red y lo compara con la dirección IP del sistema de destino. Si tienen el mismo ID de red, los datos se envían directamente desde su sistema al sistema de destino. Si los dos sistemas están en redes diferentes, el sistema debe pasar los datos al enrutador para que el enrutador pueda enviar los datos al enrutador del sistema de destino.

¿Cómo sabe su sistema qué router usar? La respuesta es "la puerta de enlace predeterminada". La puerta de enlace predeterminada es la dirección IP del enrutador que puede enviar datos desde su red.

Para comunicarse en Internet, el sistema deberá configurarse con una dirección IP, una máscara de subred y una puerta de enlace predeterminada. Si solo necesita comunicarse con otros sistemas de su red, solo necesitará una dirección IP y una máscara de subred.

Clases de direcciones

Cada dirección IP pertenece a una clase de dirección distinta. La comunidad de Internet definió estas clases para acomodar redes de varios tamaños. La clase a la que pertenece la dirección IP determina inicialmente las partes del ID de red y del ID de host de la dirección, junto con el número de hosts que se admiten en esa red. Las diferentes direcciones de clase se denominan clase A, clase B, clase C, clase D y clase E. Esta sección detalla cada clase de direcciones.

Direcciones de Clase A Una dirección de clase A tiene una máscara de subred predeterminada de 255.0.0.0, lo que significa que el primer octeto es el identificador de red y los últimos tres octetos pertenecen a la parte del identificador de host de la dirección. Cada octeto puede contener 256 valores posibles (0–255), por lo que una dirección de clase A admite 16.777.216 hosts en la red (256 × 256 × 256). En realidad, solo hay 16.777.214 direcciones válidas para usar en los sistemas porque se reservan dos direcciones en cada red IP: las direcciones con todos los bits de host establecidos en 0 (el ID de red) y con todos los bits de host establecidos en 1 (la dirección de difusión). Por lo tanto, con una dirección de clase A, no podrá asignar *n*.0.0.0 o *n*.255.255.255 (donde *n* es su ID de red) a ningún host de la red.

Siempre se puede identificar una dirección de clase A porque el valor del primer octeto se encuentra entre 1 y 126. Una dirección que comienza con 127 también es una dirección de clase A, pero no se le permite usar ninguna dirección que comience con 127 porque está reservada para la dirección de bucle invertido (más información sobre la dirección de bucle invertido más adelante en este capítulo). Por ejemplo, la dirección IP de 12.56.87.34 es una dirección de clase A porque el primer octeto es 12, que se encuentra dentro del rango de 1 a 126.

Direcciones de clase B Las direcciones de clase B tienen una máscara de subred predeterminada de 255.255.0.0, lo que significa que los dos primeros octetos son el ID de red y los dos últimos octetos son la parte del ID de host de la dirección. Esto significa que podemos tener 65.536 hosts (256 × 256) en la red. ¡Ah, pero espera! No olvides quitar las dos direcciones reservadas, por lo que nos da 65.534 direcciones que se pueden asignar a hosts en la red.

Debido a la cantidad de hosts que se admiten en una dirección de clase B, generalmente se encuentra que una empresa mediana tiene una dirección de clase B. Puede identificar una dirección de clase B porque el primer octeto comienza con un número que se encuentra entre 128 y 191.

Direcciones de clase C Las direcciones de clase C tienen una máscara de subred de 255.255.255.0, lo que significa que los tres primeros octetos son el ID de red y el último octeto es el ID de host. Tener solo un octeto como ID de host significa que una dirección de clase C puede admitir solo 254 hosts (256 – 2) en la red.

Puede identificar una dirección de clase C porque tiene un valor para el primer octeto que oscila entre 192 y 223. Por ejemplo, una dirección IP de 202.45.8.6 es una dirección de clase C porque 202 se encuentra entre 192 y 223. También sabemos que este sistema tiene una máscara de subred de 255.255.255.0 porque es una dirección de clase C.

Direcciones de clase D Las direcciones de clase D se utilizan para tipos especiales de aplicaciones en la red conocidas como *aplicaciones de multidifusión.* Estas aplicaciones envían datos a varios sistemas al mismo tiempo enviando datos a la dirección de multidifusión, y cualquier persona que se haya registrado con esa dirección recibirá los datos. Una dirección de multidifusión es para lo que se utilizan las direcciones de clase D, por lo que no las asignará específicamente a los hosts de la red para la comunicación de red normal.

Las direcciones de clase D tienen un valor en el primer octeto que oscila entre 224 y 239. Con tantos rangos, la clase D tiene el potencial de 268.435.456 grupos de multidifusión únicos a los que los usuarios pueden suscribirse desde una aplicación de multidifusión.

Direcciones de clase E Lo curioso de las direcciones de clase E es que fueron diseñadas solo con fines experimentales, por lo que nunca verá una dirección de clase E en una red. Las direcciones de clase E tienen un primer octeto con un valor que cae en el rango de 240 a 247.

DENTRO DEL EXAMEN

¿Recuerdas las clases de dirección?

Aunque el examen de certificación de Network+ le evalúa los conceptos de configuración y direccionamiento IP, aún necesita conocer el concepto de clases de dirección para responder a las preguntas relacionadas en el examen de certificación de Security+. En los párrafos siguientes se revisa la información clave sobre las clases de direcciones.

Las direcciones de clase A tienen una dirección IP en la que el primer octeto está entre 1 y 126. Las direcciones de clase A también tienen una máscara de subred predeterminada de 255.0.0.0. Tenga en cuenta también que esta máscara de subred se puede mostrar como /8 al final de la dirección; por ejemplo, 12.0.0.10/8 significa que los primeros 8 bits componen la máscara de subred.

Las direcciones de clase B tienen una dirección IP en la que el valor del primer octeto está entre 128 y 191. Las direcciones de clase B tienen una máscara de subred predeterminada de 255.255.0.0 o se pueden mostrar como /16 al final de la dirección.

Las direcciones de clase C tienen una dirección IP en la que el valor del primer octeto está entre 192 y 223. Además, las direcciones de clase C tienen una máscara de subred predeterminada de 255.255.255.0, que se puede mostrar como /24 al final de la dirección.

Ahora que está familiarizado con las diferentes direcciones de clase, eche un vistazo a la Tabla 1-5,que resume las clases de direcciones. Asegúrese de conocerlos para el examen.

TABLA 1-5

Revisión de clases de direcciones

	First Octet Value	Subnet Mask	# of Hosts per Network
Class A	1–127	255.0.0.0	16,777,214
Class B	128–191	255.255.0.0	65,534
Class C	192–223	255.255.255.0	254

Direcciones especiales

Ha aprendido que no se le permite tener un host asignado a una dirección IP que tenga un valor de 127 en el primer octeto. Esto se debe a que el intervalo de direcciones de clase A de 127 se ha reservado para la dirección de bucle invertido.

La *dirección de bucle* invertido se utiliza para hacer referencia al sistema local, también conocido como localhost. Si desea comprobar que el software TCP/IP se ha inicializado en el sistema local, aunque no tenga una dirección IP, puede hacer ping a la dirección de bucle invertido, que normalmente se denomina 127.0.0.1.

Una *dirección privada* es una dirección que se puede asignar a un sistema pero que no se puede utilizar para ningún tipo de conectividad a Internet. Las direcciones privadas son direcciones no ondables, por lo que cualquier sistema que las utilice no podrá funcionar fuera de la red. Los siguientes son los tres intervalos de direcciones que son los intervalos de direcciones privadas:

■ 10.0.0.0 a 10.255.255.255

■ 172.16.0.0 a 172.31.255.255

■ 192.168.0.0 a 192.168.255.255

No poder enrutar datos a través de Internet cuando se usan estas direcciones no supondrá un problema, porque siendo realistas, tendrá estas direcciones privadas detrás de un servidor de traducción de direcciones de red (NAT) que traducirá la dirección privada a una dirección pública que se puede enrutar en Internet.

Los clientes de Windows admiten una característica conocida como *direccionamiento IP privado automático (APIPA).* Esta característica establece que cuando un cliente no puede ponerse en contacto con un servidor de Protocolo de configuración dinámica de host (DHCP), los clientes de Windows se configuran automáticamente con un 169.254. *x*. *y* dirección. Si algo está mal con el servidor DHCP y todos los sistemas de la red no pueden obtener una dirección del servidor DHCP, todos los clientes se asignarán una dirección dentro del rango de direcciones 169.254 y luego podrán comunicarse entre sí.

APIPA no asigna una puerta de enlace predeterminada, por lo que no podrá acceder a los recursos de una red remota e Internet, pero aún puede comunicarse con los sistemas de su red. Al solucionar problemas para averiguar por qué una máquina no puede comunicarse en la red, observe los sistemas que tienen el 169.254. *x*. *y* rango de direcciones porque significa que no pudieron encontrar un servidor DHCP.

Direcciones no válidas

No solo debe estar familiarizado con los rangos de direcciones privadas en TCP / IP, sino que también debe poder identificar direcciones no válidas. Una dirección no válida es una dirección que no se permite asignar a un host en la red, como un sistema o enrutador. Desde el punto de vista del examen de certificación, debe poder identificar estas direcciones no válidas. Las siguientes se consideran direcciones no válidas:

■ **Cualquier dirección que comience con 127** Una dirección IP que comience con 127 está reservada para la dirección de bucle invertido y no se puede asignar a un sistema. Un ejemplo de este tipo de dirección no válida es 127.50.10.23.

■ **Todos los bits de host establecidos** en 0 No se le permite asignar a un sistema una dirección IP que tenga todos los bits en la parte de ID de host establecida en 0 porque este es el ID de red. Un ejemplo de este tipo de dirección no válida es 131.107.0.0.

■ **Todos los bits de host establecidos en 1** No se le permite asignar a un sistema una dirección IP que tenga todos los bits de host establecidos en 1 porque corresponde a la dirección de difusión de la red. Un ejemplo de este tipo de dirección no válida es 131.107.255.255.

■ **Una dirección duplicada** No se le permite asignar a un sistema una dirección que otro sistema está utilizando porque esto da como resultado un error de "dirección IP duplicada".

EJERCICIO 1-2

Descripción de direcciones válidas

En este ejercicio, practicará la identificación de direcciones válidas registrando si cada una de las siguientes direcciones es válida. Una dirección válida es una dirección que se puede asignar a un sistema de la red. Si una dirección no es válida, debe especificar por qué.

Address	Valid?
10.0.40.10	
127.54.67.89	
131.107.34.0	
45.12.0.0	
216.83.11.255	
63.256.4.78	
200.67.34.0	
131.107.23.255	

Descripción de los protocolos TCP/IP

Ahora que comprende los fundamentos del direccionamiento IP, hablemos de los diferentes protocolos que existen en el conjunto de protocolos TCP / IP. Como profesional de la seguridad que será responsable de configurar firewalls y listas de acceso en los enrutadores, es fundamental que comprenda cada uno de los protocolos TCP / IP.

Protocolo de control de transmisión

El Protocolo de Control de Transmisión (TCP) es responsable de proporcionar comunicación orientada a la conexión y de garantizar la entrega de los datos (conocida como entrega confiable). La comunicación orientada a la conexión implica primero establecer una conexión entre dos sistemas y luego garantizar que los datos enviados a través de la conexión lleguen al destino. TCP se asegura de que los datos lleguen a su destino retransmitiendo cualquier dato que se pierda o esté dañado. TCP es utilizado por aplicaciones que requieren un transporte confiable, pero este transporte tiene más sobrecarga que un protocolo sin conexión debido a la construcción de la sesión y la supervisión y retransmisión de cualquier dato a través de esa sesión.

Otro factor a recordar sobre TCP es que el protocolo requiere que el destinatario acuse recibo exitoso de los datos. Por supuesto, todos los reconocimientos, conocidos como ACK, generan tráfico adicional en la red, lo que reduce la cantidad de datos que se pueden pasar dentro de un marco de tiempo determinado. La sobrecarga adicional involucrada en la creación, monitoreo y finalización de la sesión TCP vale la certeza de que TCP asegurará que los datos lleguen a su destino.

TCP garantiza que los datos se entreguen mediante lo que se conoce como números de secuencia y números de reconocimiento. Un número de *secuencia* es un número asignado a cada pieza de datos que se envía. Después de que un sistema recibe un dato, reconoce que ha recibido los datos enviando un mensaje de confirmación al remitente, siendo el número de secuencia original el número de confirmación del mensaje de respuesta.

Apretón de manos tcp de tres vías Antes de que un sistema pueda comunicarse a través de TCP, primero debe establecer una conexión con el sistema remoto. Para establecer una conexión con el sistema remoto, TCP utiliza lo que se denomina protocolo de enlace tcp de tres vías. Estas son las tres fases del apretón de manos tcp de tres vías (como se muestra en la Figura 1-10):

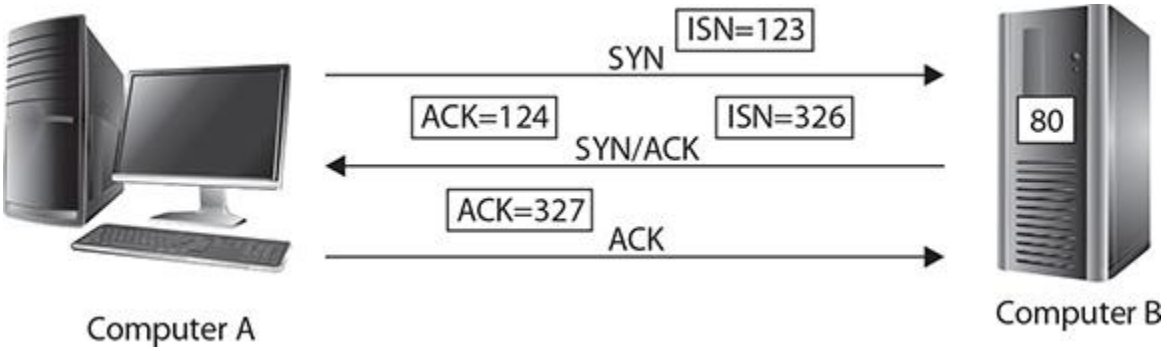


FIGURA 1-10

El apretón de manos de tres vías TCP

■ **SYN** En la primera fase, el sistema de envío envía un mensaje SYN al sistema receptor. A cada paquete enviado se le asigna un número de secuencia único. El mensaje SYN contiene el *número de secuencia inicial (ISN),* que es el primer número de secuencia que se utilizará. En este ejemplo, el equipo A se conecta al sitio web en el equipo B, por lo que se envía un mensaje SYN al puerto 80 del equipo B.

■ **SYN/ACK** La segunda fase se conoce como la fase SYN/ACK, porque este mensaje está reconociendo el primer mensaje pero al mismo tiempo está indicando su número de secuencia inicial. En este ejemplo, el equipo B envía de vuelta el mensaje SYN/ACK que reconoce que ha recibido el paquete 123 (al reconocer que 124 es el siguiente número de secuencia), pero también ha especificado que su ISN es 326.

■ **ACK** La fase final del apretón de manos de tres vías es el mensaje de confirmación, que reconoce que se ha recibido el paquete enviado en la segunda fase. En este ejemplo, el equipo A envía el ACK para confirmar que ha recibido el paquete 326 al reconocer que el siguiente paquete será el número de secuencia 327.

Para ver una captura de paquete del apretón de manos de tres vías, vea el video incluido en los recursos en línea que acompañan a este libro.

Desconectarse de una sesión TCP Así como TCP tiene un apretón de manos de tres vías para crear una conexión entre dos sistemas que desean comunicarse, TCP también tiene un proceso

para que un participante se desconecte de la conversación. Mirando la Figura 1-11,puede ver que si la computadora A desea desconectarse de una sesión TCP, primero debe enviar una marca FIN para indicar que desea finalizar la conversación.

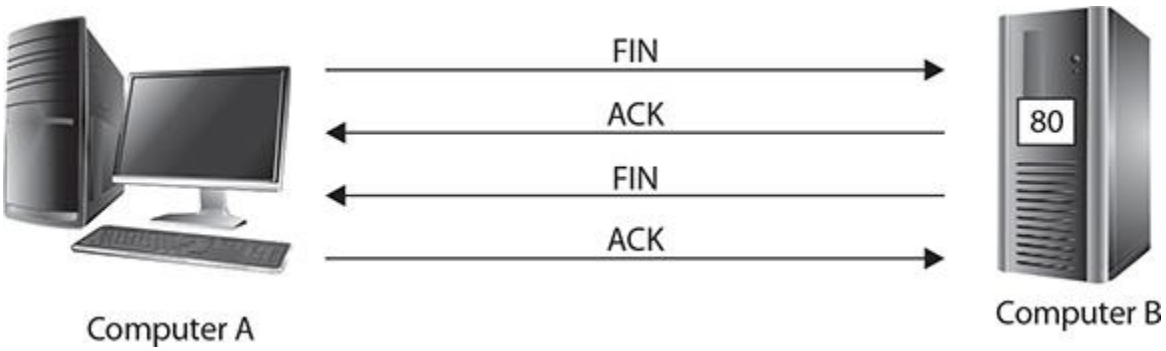


FIGURA 1-11

Terminación de una conexión TCP

Cuando el equipo B recibe el mensaje FIN, responde con un acuse de recibo y, a continuación, envía su propio mensaje FIN al equipo A. Como paso final de este proceso, el equipo A debe reconocer que ha recibido el mensaje FIN del equipo B. Esto es similar a hablar con alguien por teléfono: para terminar la conversación, te despides y luego esperas a que la otra persona se despida antes de colgar. Describo esto como terminar la conversación de una manera "educada".

También hay una manera de terminar una conversación de una manera "descortés". Volviendo a la analogía telefónica: puedes terminar la conversación descortésmente colgando el teléfono sin despedirte. En el mundo TCP, puede "colgar" enviando un mensaje TCP con el indicador RST (restablecer) establecido.

Puertos TCP Cuando las aplicaciones utilizan TCP para comunicarse a través de la red, cada aplicación debe identificarse de forma única mediante un número de puerto. Un *puerto* es una dirección única asignada a la aplicación. Cuando un cliente desea comunicarse con una de esas aplicaciones (también conocida como servicio), el cliente debe enviar la solicitud al número de puerto apropiado en el sistema.

Como profesional de la seguridad, es fundamental que conozca algunos de los números de puerto utilizados por los servicios populares. La Tabla 1-6 identifica los números de puerto TCP comunes que debe conocer para el examen de certificación Security+.

TABLA 1-6

Puertos TCP populares

Port	Service	Description
20	FTP Data	Port used by FTP to send data to a client.
21	FTP Control	Port used by FTP commands sent to the server.
22	SSH	Port used by Secure Shell (SSH) to encrypt remote access communication. It typically is used as a secure replacement to Telnet.
23	Telnet	Port used by Telnet to remotely connect to a system such as a server or router.
25	SMTP	Port used to send Internet e-mail.
53	DNS	Port used for DNS zone transfers.
80	HTTP	Internet protocol for delivering web pages to the browser.
110	POP3	Port used by POP3, which is the Internet protocol to read e-mail.
139	NetBIOS	Port used by the NetBIOS session service. It is used to establish a connection between two systems for NetBIOS communication.
143	IMAP	Port used by IMAP, which is a newer Internet protocol to read e-mail.
443	HTTPS	Port used for secure web traffic.
3389	RDP	Port used by Remote Desktop Protocol (RDP) for remote administration of a Windows system.

Banderas TCP El protocolo TCP utiliza indicadores TCP para identificar tipos importantes de paquetes. Los siguientes son los indicadores TCP comunes con los que debe estar familiarizado para el examen de certificación Security+:

■ **SYN** El indicador SYN se asigna a cualquier paquete que forme parte de las fases SYN del apretón de manos de tres vías.

■ **ACK** El indicador de acuse de recibo reconoce que se ha recibido un paquete anterior.

■ **PSH** El indicador push está diseñado para forzar datos en una aplicación.

■ **URG** El indicador urgente especifica que un paquete es un paquete urgente.

■ **FIN** El indicador de finalización especifica que desea finalizar o finalizar la conexión. Esto termina una conexión TCP cortésmente, como decir adiós para terminar una llamada telefónica.

■ **RST** El indicador de restablecimiento se utiliza para finalizar una conversación TCP de manera descortés. Esto es como colgar el teléfono sin decir adiós.

Como profesional de la seguridad y alguien que realiza el examen Security+, debe estar familiarizado con las diferentes banderas TCP porque le ayudarán a comprender los diferentes tipos de escaneos de puertos cubiertos en el Capítulo 4.

La figura 1-12 muestra los indicadores de una captura de paquetes. Tenga en cuenta que en lugar de mostrar el indicador real, el Monitor de red interpreta el valor y se muestra una descripción. Por ejemplo, en lugar de ver el indicador URG establecido en cero, verá el primer indicador establecido en cero con una descripción de "Sin datos urgentes".

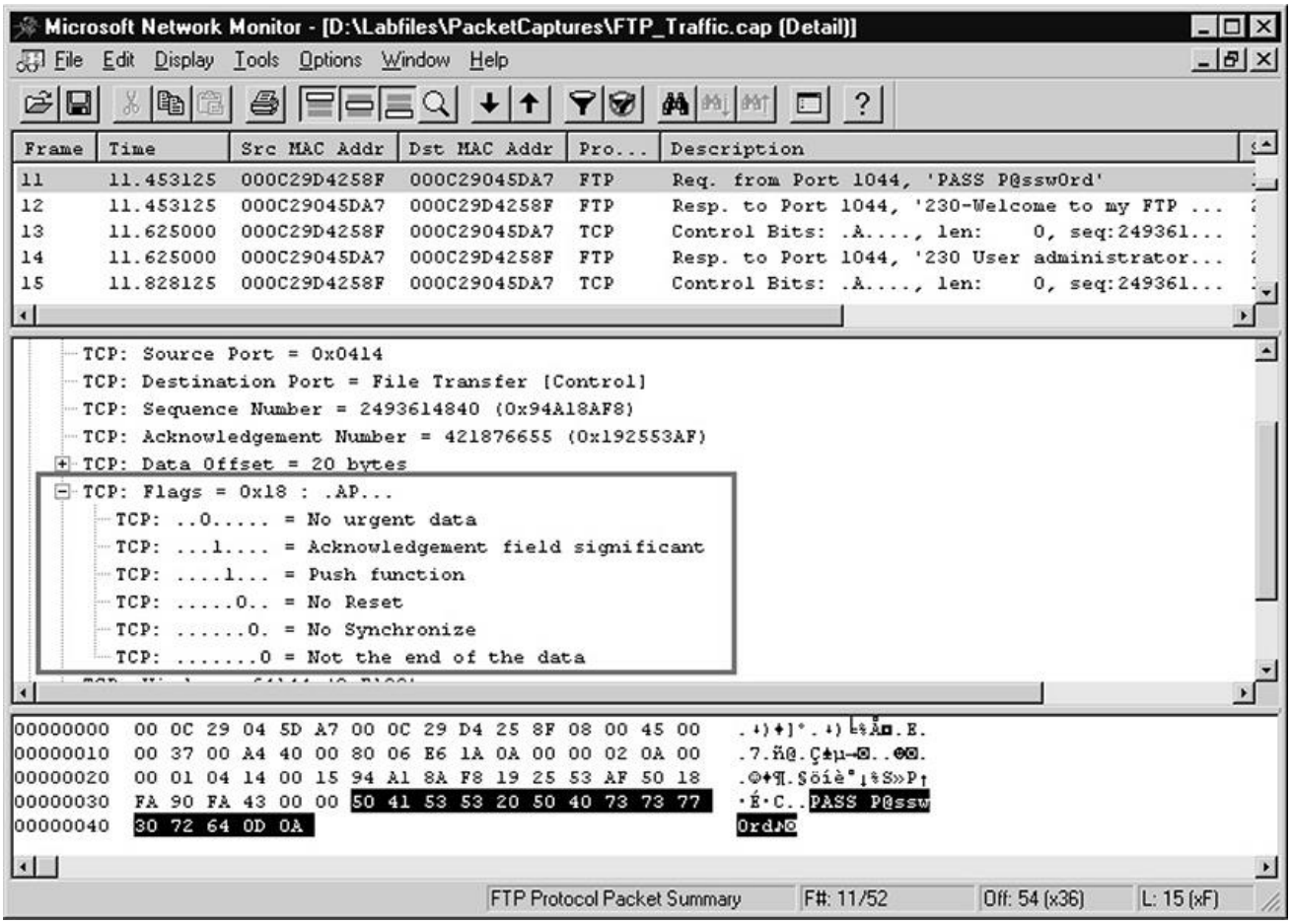


FIGURA 1-12 Indicadores

TCP en el encabezado TCP

Encabezado TCP Cada paquete que se envía mediante el protocolo TCP tiene asignado un encabezado TCP, que contiene información relacionada con TCP, como el puerto de origen, el puerto de destino y los indicadores TCP. La figura 1-13 muestra los diferentes campos en el encabezado TCP. A continuación se realiza una descripción rápida de cada campo:

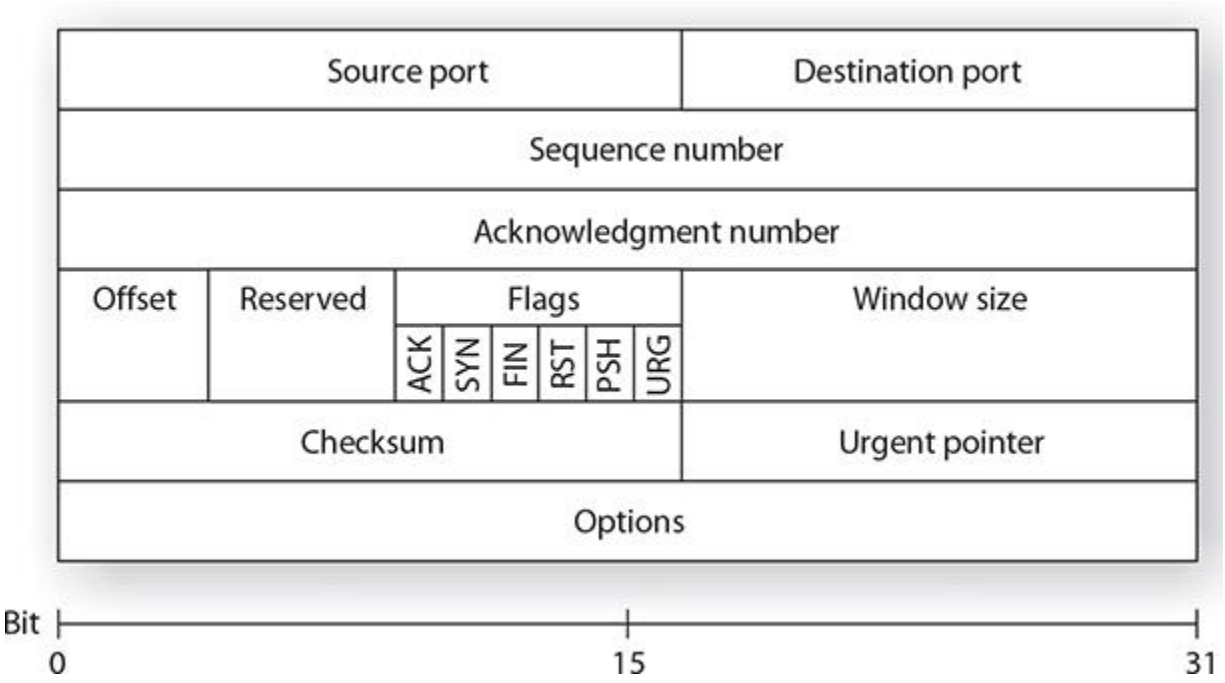


FIGURA 1-13

El encabezado TCP

■ **Puerto de origen** Este campo de 16 bits identifica el número de puerto del sistema de envío.

■ **Puerto de destino** Este campo de 16 bits identifica el número de puerto al que está destinado el paquete en el sistema de destino.

■ **Número de secuencia** Este campo de 32 bits identifica el número de secuencia del paquete.

■ **Número de confirmación** Este campo de 32 bits identifica el paquete que este paquete está reconociendo.

■ **Desplazamiento** Este campo de 4 bits indica dónde comienzan los datos.

■ **Reservado** Este campo de 6 bits siempre se establece en 0 y fue diseñado para su uso futuro.

■ **Banderas** Este campo de 6 bits es donde se almacenan las banderas TCP. Hay un campo de 1 bit para cada una de las banderas mencionadas anteriormente en esta sección.

■ **Tamaño de la ventana** Este campo de 16 bits determina la cantidad de información que se puede enviar antes de que se espere un acuse de recibo.

■ **Suma de comprobación** Este campo de 16 bits se utiliza para verificar la integridad del encabezado TCP.

■ **Puntero urgente** Este campo de 16 bits se utiliza solo si se establece el indicador URG y es una referencia a la última información que es urgente.

■ **Opciones** Este es un campo de longitud variable que especifica cualquier configuración adicional que pueda ser necesaria en el encabezado TCP.

TCP y UDP se consideran protocolos de capa 4 (transporte).

Vea el video incluido en los recursos en línea que acompañan a este libro que revisa el contenido de la cabecera TCP.

Protocolo de datagramas de usuario

El Protocolo de datagramas de usuario (UDP) es utilizado por aplicaciones que no quieren preocuparse por garantizar que los datos lleguen al sistema de destino. UDP se utiliza para la comunicación sin conexión (no confiable), lo que significa que los datos se envían al destino y no se hace ningún esfuerzo para rastrear el progreso del paquete y si ha llegado al destino.

Puertos UDP Al igual que TCP, UDP utiliza números de puerto para identificar diferentes tipos de tráfico. En la Tabla 1-7 se identifican algunos ejemplos de tráfico UDP y los puertos utilizados.

TABLA 1-7

Puertos UDP populares

Port	Service	Description
53	DNS	UDP port 53 is used for DNS queries.
67 and 68	DHCP	UDP port 67 is used by the DHCP service, and UDP port 68 is used by client requests.
69	TFTP	Trivial File Transfer Protocol is used to download files without requiring authentication.
137 and 138	NetBIOS	UDP 137 and 138 are used by the NetBIOS name service and datagram service.
161	SNMP	UDP port 161 is used by the Simple Network Management Protocol.

Encabezado UDP Debido a que el Protocolo de datagramas de usuario no tiene que acusar recibo de un paquete, la estructura del encabezado UDP es mucho más simple que el encabezado TCP. Por ejemplo, el encabezado UDP no necesita un número de secuencia o número de confirmación; tampoco necesita indicadores para indicar paquetes especiales, como un mensaje SYN, porque no hay un protocolo de enlace de tres vías (porque UDP no tiene conexión). La figura 1-14 muestra el encabezado UDP con una lista de los siguientes campos:

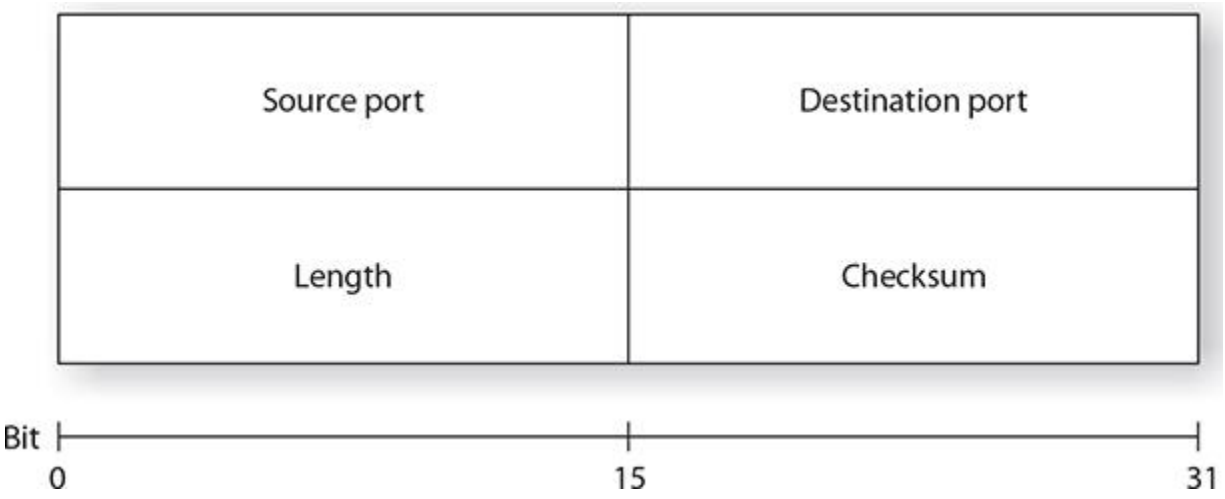


FIGURA 1-14

El encabezado UDP

■ **Puerto de origen** Campo de 16 bits que indica el puerto utilizado por la aplicación de envío en el sistema de envío

■ **Puerto de destino** Campo de 16 bits que indica el puerto utilizado por la aplicación en el sistema de destino

■ **Longitud** Un campo de 16 bits que especifica el tamaño del encabezado UDP en bytes

■ **Suma de comprobación** Un campo de 16 bits utilizado para verificar la integridad del encabezado UDP

Vea el video incluido en los recursos en línea que acompañan a este libro para ver el encabezado UDP.

Protocolo de Internet

El Protocolo de Internet (IP) proporciona entrega de paquetes para protocolos más altos en el modelo. Es un sistema de entrega sin conexión que hace un intento de "mejor esfuerzo" para entregar los paquetes al destino correcto. IP no garantiza la entrega de los paquetes, eso es responsabilidad de los protocolos de transporte; IP simplemente envía los datos.

IP es un protocolo de capa 3 del modelo OSI y es responsable del direccionamiento lógico y el enrutamiento.

El Protocolo de Internet también es responsable del direccionamiento lógico y el enrutamiento de TCP / IP y, por lo tanto, se considera un protocolo de capa 3 del modelo OSI. El Protocolo de Internet en el enrutador es responsable de decrementar (generalmente por un valor de 1) el TTL (tiempo de vida) del paquete para evitar que se ejecute en un "bucle de red". Los sistemas operativos Windows tienen un TTL predeterminado de 128.

Aunque el modelo OSI es más un tema de Network+, es importante recordarlo para el examen Security+ porque sirve como fondo que puede ayudarlo a comprender las tecnologías de red, como los dispositivos de red y las listas de control de acceso. Por ejemplo, si comprende el modelo OSI y lee una pregunta de examen que se refiere a una tecnología de firewall que puede filtrar en función de la información de capa 3 o capa 4, entonces sabe que la tecnología puede filtrar en función de las direcciones IP de origen y destino (capa 3) y la información del puerto TCP o UDP (capa 4).

Encabezado IP El encabezado IP del paquete contiene información que ayuda al paquete a llegar desde el origen hasta el destino. La siguiente es una lista de los campos y su significado, mientras que la Figura 1-15 muestra la estructura del encabezado IP:

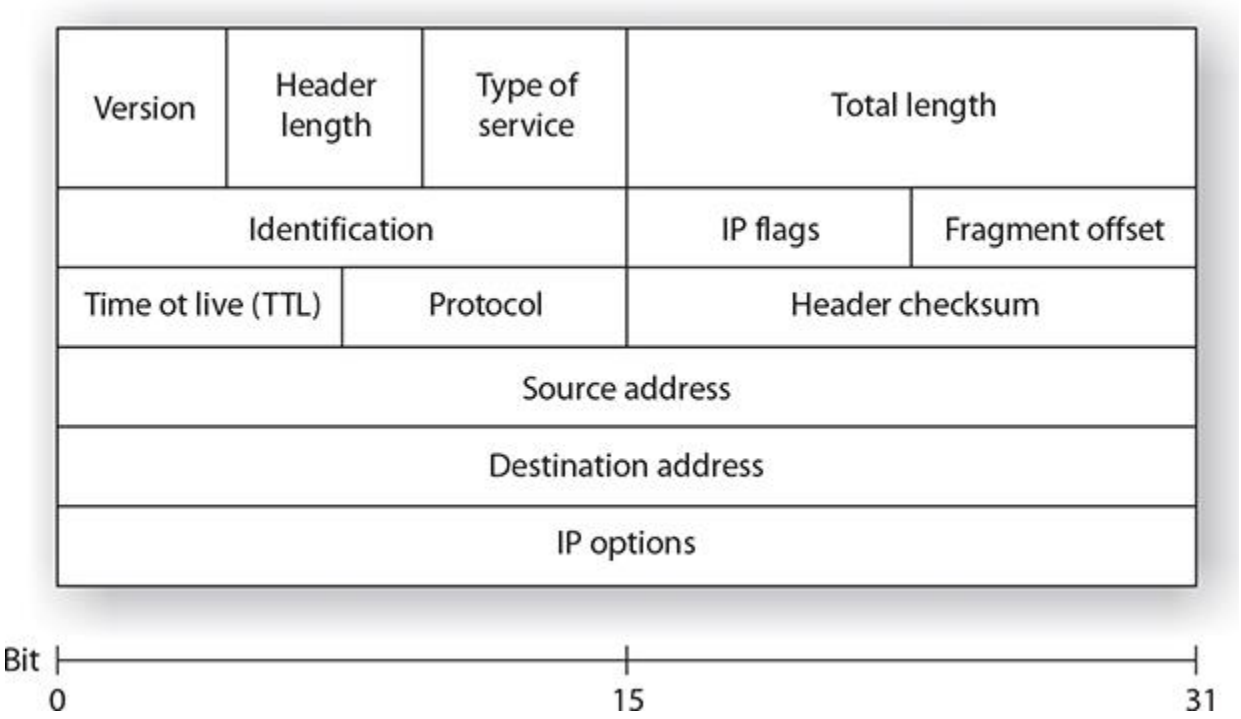


FIGURA 1-15

El encabezado IP

■ **Versión** Un campo de 4 bits que identifica la versión de IP que se está utilizando (por ejemplo, 4 o 6).

■ **Longitud del encabezado** Un campo de 4 bits que indica el tamaño del encabezado IP.

■ **Tipo de servicio** Un campo de 8 bits que indica cómo el sistema debe manejar el paquete. Por ejemplo, si la opción de retardo bajo se especifica aquí, significa que el sistema debe tratar con el paquete de inmediato.

■ **Longitud total** Un campo de 16 bits que indica el tamaño del encabezado IP.

■ **Identificación** Un campo de 16 bits. Las redes solo pueden manejar paquetes de un tamaño máximo específico, conocido como *unidad de transmisión máxima (MTU),* por lo que el sistema puede romper los datos que se envían en múltiples fragmentos. Este campo identifica de forma única el fragmento.

■ **Indicadores IP** Un campo de 3 bits que especifica cómo se van a tratar los fragmentos. Por ejemplo, una bandera de Más fragmentos (MF) indica que vendrán más fragmentos. Además, un bit conocido como Don't Fragment (DF) especifica no fragmentar el paquete.

■ **Desplazamiento de fragmentos** Campo de 13 bits que especifica el orden en que se volverán a unir los fragmentos cuando se ensambla el paquete.

■ **Tiempo de vida (TTL)** Campo de 8 bits que especifica cuándo caducará el paquete. El TTL es un valor que se disminuye con cada enrutador por el que pasa el paquete. Cuando el TTL alcanza 0, el paquete se descarta.

■ **Protocolo** Campo de 8 bits que especifica qué protocolo de capa 4 (TCP o UDP) debe utilizar el paquete.

■ **Suma de comprobación del encabezado** Un campo de 16 bits que verifica la integridad del encabezado IP.

■ **Dirección de** origen Campo de 32 bits que representa la dirección IP del sistema de envío. Así es como el sistema receptor sabe a dónde enviar el mensaje de respuesta.

■ **Dirección de destino** Campo de 32 bits que representa la dirección IP del sistema al que está destinado el paquete.

■ **Opciones de IP** Un campo de longitud variable utilizado para especificar cualquier otra configuración en el encabezado IP.

Vea el video incluido en los recursos en línea que acompañan a este libro para ver una demostración de los campos IP comunes en el encabezado IP.

Protocolo de mensajes de control de Internet

El Protocolo de mensajes de control de Internet (ICMP) permite a los sistemas de una red TCP/IP compartir información de estado y error. Puede utilizar la información de estado para detectar problemas de red. Los mensajes ICMP se encapsulan dentro de datagramas IP para que puedan enrutarse a través de una red. Dos programas que utilizan mensajes ICMP son ping y traceroute (Linux) o tracert (Windows).

Puede usar ping para enviar solicitudes de eco ICMP a una dirección IP y esperar las respuestas de eco ICMP. Ping informa del intervalo de tiempo entre el envío de la solicitud y la recepción de la respuesta. Con ping, puede determinar si un sistema IP en particular en su red está funcionando correctamente. Puede usar muchas opciones diferentes con la utilidad ping.

ICMP es el protocolo del conjunto de protocolos TCP/IP que es responsable de los informes de errores y estado. Programas como ping y tracert utilizan ICMP.

Tracert rastrea la ruta tomada a un host en particular. Esta utilidad puede ser muy útil en la solución de problemas de internetworks. Tracert envía solicitudes de eco ICMP a una dirección IP mientras incrementa el campo TTL en el encabezado IP en un recuento de 1 después de comenzar en 1 y luego analizar los errores ICMP que se devuelven. Cada solicitud de eco posterior debe llevar una más a la red antes de que el campo TTL alcance 0 y el enrutador intente reenviarlo un mensaje de error "Tiempo ICMP excedido".

Tipos y códigos ICMP ICMP no utiliza números de puerto, sino que utiliza tipos y códigos ICMP para identificar los diferentes tipos de mensajes. Por ejemplo, un mensaje de solicitud de eco que utiliza la solicitud de ping utiliza el tipo ICMP 8, mientras que la respuesta de ping vuelve con un mensaje de tipo 0 de ICMP.

Algunos de los tipos de ICMP se desglosan en niveles más finos con diferentes códigos en el tipo. Por ejemplo, ICMP tipo 3 es un mensaje de destino inaccesible, pero debido a que hay muchas razones posibles por las que un destino es inalcanzable, el tipo se subdivide en diferentes códigos. Cada código es para un mensaje diferente en el tipo (consulte la Tabla 1-8).

TABLA 1-8

Tipos y códigos comunes de ICMP

Type	Code	Description
0—Echo Reply	0	Echo reply message
3—Destination Unreachable	0 1 2 3	Destination network Destination host unreachable Destination protocol unreachable Destination port unreachable
8—Echo Request	0	Echo request message

Para ser bueno en el monitoreo de redes y la identificación de tráfico sospechoso, debe comprender cada uno de los encabezados de protocolo discutidos en este capítulo. Para el examen, sepa que ICMP tipo 8 es utilizado por el mensaje de solicitud de eco e ICMP tipo 0 se utiliza por respuesta de eco.

Encabezado ICMP El encabezado ICMP es un encabezado muy pequeño en comparación con el encabezado IP y el encabezado TCP. La figura 1-16 muestra el encabezado ICMP y una lista de los campos sigue:

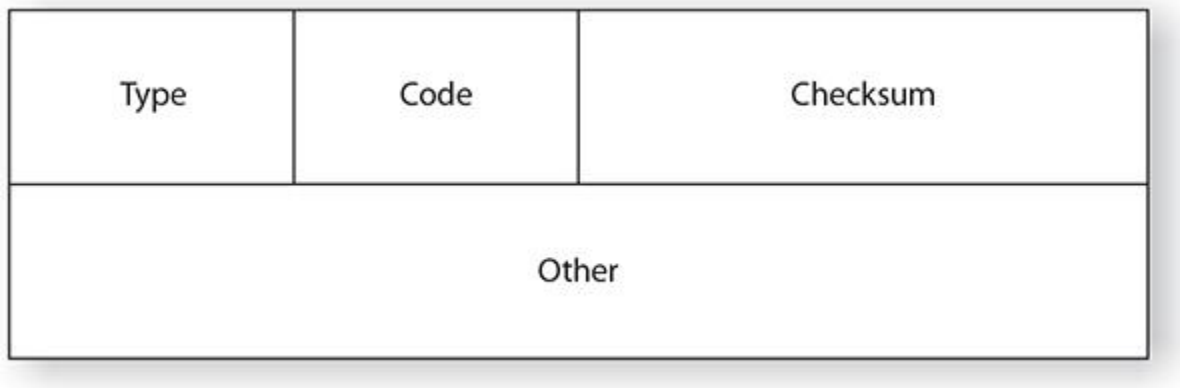


FIGURA 1-16

El encabezado ICMP

■ **Tipo** Un campo de 8 bits que indica el tipo ICMP que se está utilizando.

■ **Código** Un campo de 8 bits que indica el código ICMP que se está utilizando.

■ **Suma de comprobación** Campo de 16 bits que se utiliza para verificar la integridad del encabezado ICMP.

■ **Otro** Campo que almacena cualquier dato dentro del encabezado ICMP. Por ejemplo, los sistemas operativos de Microsoft colocan parte del alfabeto en este campo para los mensajes de solicitud de eco.

Vea el video incluido en los recursos en línea que acompañan a este libro para ver una demostración que muestra los tipos y códigos ICMP.

Protocolo de resolución de direcciones

El Protocolo de resolución de direcciones (ARP) proporciona una resolución de dirección lógica a dirección física en una red TCP/IP, que está convirtiendo la dirección IP en una dirección MAC.

Para lograr esta hazaña, ARP envía un mensaje de difusión con un paquete de solicitud ARP que contiene la dirección IP del sistema que está tratando de encontrar. Todos los sistemas de la red local ven el mensaje, y el sistema que posee la dirección IP para la que ARP está buscando responde enviando su dirección física al sistema de origen en un paquete de respuesta ARP. La combinación de direcciones físicas/IP se almacena en la memoria caché ARP del sistema de origen para su uso futuro.

Todos los sistemas mantienen cachés ARP que incluyen asignaciones de direcciones IP a direcciones físicas. La caché ARP siempre se comprueba para una asignación de dirección IP a dirección física antes de iniciar una difusión.

ARP es responsable de convertir una dirección IP (dirección de capa 3) a la dirección MAC física (dirección de capa 2).

EJERCICIO 1-3

Visualización de la información del protocolo con Wireshark

En este ejercicio, descargará e instalará Wireshark desde www.wireshark.org. En este escenario, está utilizando Wireshark para supervisar el tráfico FTP para determinar si el tráfico de inicio de sesión está cifrado (que no lo está).

Instalación de Wireshark

1. Descargue e instale la última versión de Wireshark desde www.wireshark.org. Acepte todas las opciones predeterminadas al realizar la instalación.

Visualización de datos de paquetes con Wireshark

2. Inicie Wireshark en su sistema.

3. Una vez que se inicia Wireshark, abra un archivo de captura seleccionando Archivo | Abrir.

4. En el cuadro de diálogo Abrir, abra el archivo FTP_Traffic.cap ubicado en la carpeta Labfiles\PacketCaptures.

5. Se muestra el contenido de la captura de paquetes. La pantalla se divide en tres secciones: Lista de paquetes (arriba), Detalles de paquetes (centro) y Bytes de paquetes (abajo). Observe que se capturan 52 paquetes (números enumerados en el lado izquierdo en la sección Lista de paquetes ubicada en la parte superior de la pantalla) (también puede ver "Paquetes: 52" en la barra de estado). En la sección superior de la pantalla, seleccione el paquete 4 y observe que es el primer paquete FTP (busque en la columna Protocolo).

6. Observe en la columna Información que los tres primeros paquetes son el apretón de manos tcp de tres vías (SYN, SYN/ ACK, ACK). Puede ver esto mirando la columna Protocolo primero para ver TCP y luego en la columna Información para ver la descripción de SYN, SYN / ACK y finalmente ACK.

7. Seleccione el paquete 8. Observe que en la columna Información puede ver el nombre de usuario que se utiliza para iniciar sesión en el servidor FTP. ¿Cuál es el nombre de usuario?
_____

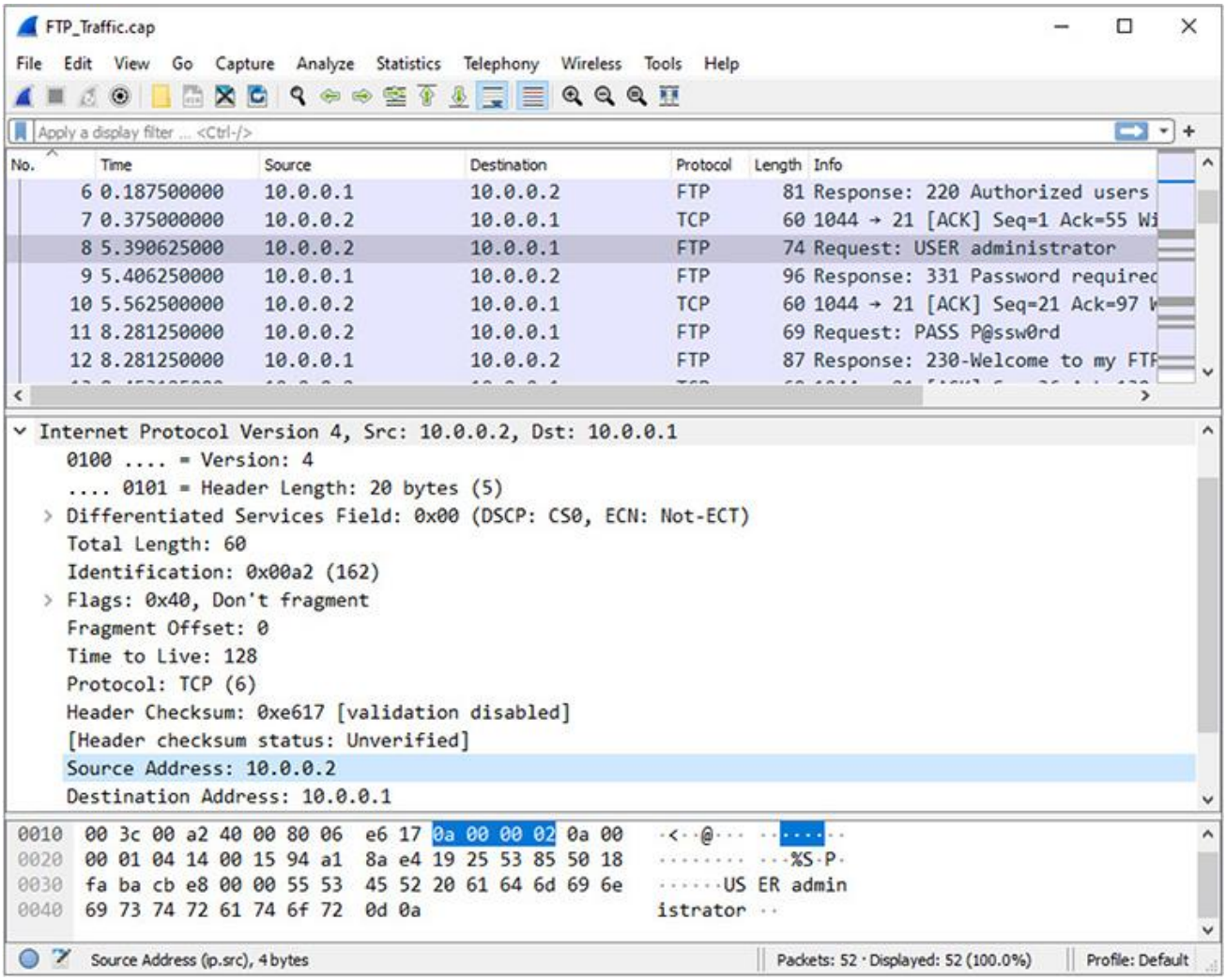
8. Asegúrese de que el paquete 8 siga seleccionado en la ventana Lista de paquetes.

9. Observe que debajo de la ventana Lista de paquetes tiene la ventana Detalles del paquete que muestra los detalles del paquete para el paquete seleccionado. Observe también que debajo de la ventana Detalles del paquete hay otra ventana conocida como la ventana Detalles de byte, que le muestra los datos hexaciédices para el paquete seleccionado.

10. Expanda la sección Protocolo de Internet versión 4 en la ventana Detalles del paquete para ver el encabezado IP del paquete y registrar la siguiente información:

Dirección IP de origen: _____

Dirección IP de destino: _____



11. Expanda el encabezado TCP en Detalles del paquete y busque la siguiente información:

Puerto de origen: _____

Puerto de destino: _____

Número de secuencia: _____

Conjunto de banderas: _____

12. Seleccione el paquete 11 y localice la contraseña FTP en la captura de paquetes. ¿Cuál es la contraseña que se está utilizando? (Busque en la columna Información de la ventana Lista de paquetes o en la sección FTP en la ventana Detalles del paquete). _____

13. Cierre Wireshark.

Descripción de los protocolos de capa de aplicación

Al prepararse para el examen de certificación Security+, debe comprender varios protocolos que utilizan las aplicaciones para la comunicación. En esta sección, aprenderá acerca de los protocolos comunes utilizados por las aplicaciones de Internet y las aplicaciones de red.

HTTP y HTTPS

El Protocolo de transferencia de hipertexto (HTTP) se utiliza en Internet para permitir a los clientes solicitar páginas web de servidores web y para permitir la interacción del cliente con esos servidores web. HTTP es un protocolo sin estado, lo que significa que los servidores web no son conscientes de lo que un cliente ha solicitado o no ha solicitado y no pueden rastrear a los usuarios que han solicitado contenido específico. Este sistema no permite una buena interacción con el servidor web, pero sí permite recuperar las páginas HTML almacenadas en los sitios web. Para ayudar en el seguimiento de las solicitudes del cliente, utilizamos cookies: pequeños archivos almacenados en la computadora cliente que permiten que el servidor web almacene datos sobre el cliente que el cliente enviará de vuelta con cada solicitud al servidor.

El Protocolo de transferencia de hipertexto seguro (HTTPS) le permite conectarse a un sitio web y recibir y enviar contenido en un formato cifrado utilizando Secure Sockets Layer (SSL), o su sucesor *Transport Layer Security (TLS).* HTTPS se usa más comúnmente en sitios de comercio electrónico para permitirle enviar información personal, especialmente números de tarjetas de crédito y otros datos confidenciales, sin preocuparse de que un hacker de Internet esté viendo esta información. Puede determinar cuándo se está utilizando HTTPS porque la dirección del sitio web comienza con https:// y no http://, que marca el protocolo HTTP normal. Otra señal de que HTTPS está en uso es que aparece un candado en la barra de direcciones del navegador: el bloqueo está cerrado o bloqueado (como se muestra en la Figura 1-17).

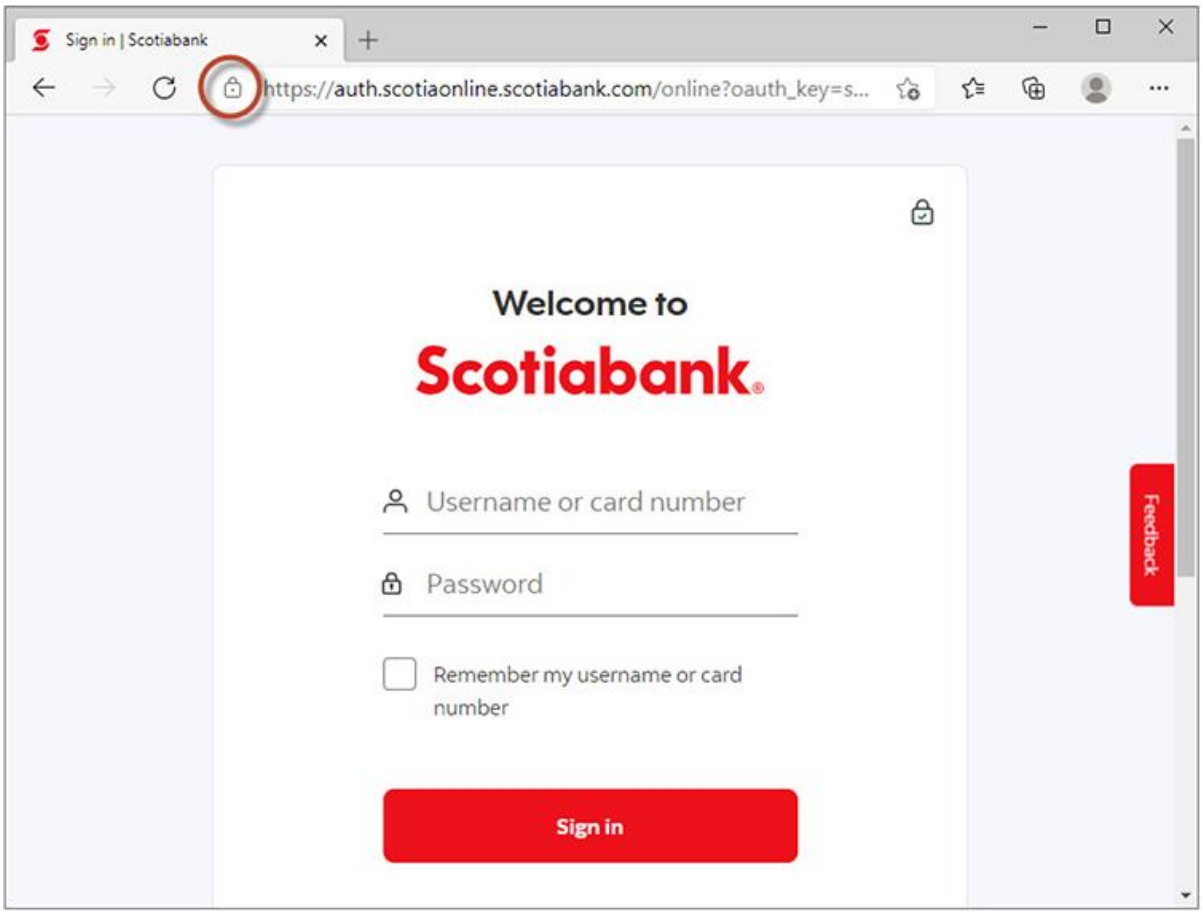


FIGURA 1-17

Identificación del uso del tráfico seguro por el icono de candado en el navegador

Para el examen, recuerde que HTTP usa el puerto TCP 80, mientras que HTTPS usa el puerto TCP 443.

Normalmente, HTTPS no se utiliza para un sitio de comercio electrónico completo porque los procesos de cifrado y descifrado ralentizan el tiempo de conexión, por lo que solo la parte del sitio que solicita información personal utiliza HTTPS.

DNS

El servicio Sistema de nombres de dominio (DNS) se utiliza para convertir nombres de dominio completos (FQDN) en direcciones IP. Al acceder a sitios o servidores de Internet en Internet, utilice nombres como www.gleneclarke.com para conectarse al sistema. Antes de intentar una

conexión, el sistema consulta un servidor DNS a través del puerto UDP 53 y solicita al servidor DNS la dirección IP de ese sistema. Una vez que su sistema tiene la dirección IP del sistema de destino, realiza una conexión a ese sistema utilizando la dirección IP.

SMTP

El Protocolo simple de transferencia de correo (SMTP) se utiliza para enviar o enrutar correo a través de una red TCP/IP como Internet. La mayoría de los productos de servidor de correo electrónico admiten SMTP (puerto TCP 25) para enviar correo electrónico fuera de la empresa y a Internet.

POP3

El Protocolo de oficina de correos versión 3 (POP3) es el protocolo de Internet utilizado para recuperar el correo electrónico de un servidor de correo hasta el cliente POP3 a través del puerto TCP 110. El correo electrónico se "abre" o se descarga en el cliente después de que el cliente se haya autenticado en su buzón. POP3 tiene capacidades limitadas en lo que respecta al soporte de carpetas. Un cliente POP3 solo admite una bandeja de entrada, una bandeja de salida, elementos enviados y elementos eliminados. Si se requiere compatibilidad adicional con carpetas, deberá utilizar un cliente IMAP4.

POP3 e IMAP4 son los protocolos de Internet para leer el correo electrónico, mientras que SMTP es el protocolo de Internet para el envío de correo electrónico.

IMAP4

El Protocolo de acceso a mensajes de Internet versión 4 (IMAP4) es otro protocolo similar a POP3 que permite a los clientes recuperar mensajes de un servidor de correo mediante el puerto TCP 143. IMAP4 permite carpetas adicionales distintas de las cuatro básicas proporcionadas con POP3. Por ejemplo, puede utilizar un cliente IMAP4 para conectarse a carpetas públicas almacenadas en un servidor de Microsoft Exchange.

SNMP

El Protocolo simple de administración de redes (SNMP) es un estándar de Internet que proporciona un método simple para administrar de forma remota prácticamente cualquier dispositivo de red que admita SNMP a través del puerto UDP 161. Un dispositivo de red puede ser una tarjeta de red en un servidor; un programa o servicio que se ejecuta en un servidor; o un dispositivo de red como un concentrador, conmutador o enrutador.

El estándar SNMP define un enfoque de dos niveles para la administración de dispositivos de red: un sistema de administración central y la base de información de administración (MIB) ubicada en el dispositivo administrado. El sistema de gestión puede supervisar una o varias MIB, lo que permite la gestión centralizada de una red. Desde un sistema de administración, puede ver valiosas estadísticas de rendimiento y operación de dispositivos de red, lo que le permite diagnosticar el estado de la red sin salir de su oficina.

El objetivo de un sistema de gestión es proporcionar una gestión de red centralizada. Cualquier computadora que ejecute software de administración SNMP se conoce como un sistema de administración. Para que un sistema de gestión pueda realizar una gestión de red centralizada, debe ser capaz de recopilar y analizar muchos tipos de datos, incluidos los siguientes:

■ Identificación y estadísticas del protocolo de red

■ Identificación dinámica de los ordenadores conectados a la red (denominado *descubrimiento)*)

■ Datos de configuración de hardware y software

■ Estadísticas de rendimiento y uso del equipo

■ Eventos informáticos y mensajes de error

■ Estadísticas de uso de programas y aplicaciones

FTP

El Protocolo de transferencia de archivos (FTP) es un protocolo TCP/IP que existe para cargar y descargar archivos entre servidores FTP y clientes. Al igual que Telnet y ping, FTP puede establecer una conexión a un equipo remoto utilizando el nombre de host o la dirección IP y debe resolver los nombres de host en direcciones IP para establecer la comunicación con el equipo remoto.

Para el examen, recuerde que FTP es un protocolo que utiliza dos puertos. El puerto TCP 21 lleva los comandos FTP de un sistema a otro, mientras que el puerto TCP 20 es responsable de transferir los datos entre dos hosts en una sesión FTP.

Cuando TCP/IP está instalado en el sistema, hay una utilidad FTP disponible, pero una serie de clientes FTP de interfaz gráfica de usuario (GUI) de terceros también están disponibles para

todos los sistemas operativos. Si usa FTP mucho, un cliente FTP GUI podría ahorrarle mucho tiempo y frustración al tratar con comandos FTP.

TFTP

El Trivial File Transfer Protocol (TFTP) es un protocolo simple en comparación con FTP y solo admite la lectura y escritura en archivos. TFTP no admite características como la enumeración del contenido del directorio o la autenticación. TFTP utiliza UDP como protocolo de transporte y FTP utiliza TCP. TFTP se utiliza normalmente para copiar la configuración del enrutador y el conmutador desde el dispositivo al servidor TFTP a través del puerto UDP 69. TFTP también se puede utilizar para arrancar un dispositivo cargando la configuración que se almacena en un servidor TFTP.

SFTP

El Protocolo seguro de transferencia de archivos (SFTP) es un protocolo interactivo de transferencia de archivos similar a FTP, pero cifra todo el tráfico entre el cliente SFTP y el servidor SFTP. SFTP admite características adicionales como la autenticación y compresión de clave pública. A diferencia de TFTP, SFTP admite una serie de comandos en su shell interactivo, como enumerar el contenido del directorio, crear directorios, descargar archivos y cargar archivos.

Telnet

Telnet es un protocolo de emulación de terminal que se ejecuta en el puerto TCP 23 y permite a un cliente ejecutar o emular el programa que se ejecuta en el servidor. Varios dispositivos le permiten "telnet" en el dispositivo y realizar la administración remota del dispositivo de red utilizando el conjunto de comandos disponible para la sesión Telnet.

SSH

Secure Shell (SSH) es un programa utilizado para crear un shell, o sesión, con un sistema remoto utilizando una conexión segura a través del puerto TCP 22. Una vez establecida la sesión remota, el cliente puede ejecutar comandos dentro de este shell y copiar archivos en el sistema local. El propósito principal de SSH es admitir shells remotos con soporte para autenticación segura y comunicación cifrada; por lo tanto, se debe usar SSH en lugar de Telnet porque Telnet utiliza comunicación no cifrada.

PC

El Protocolo de copia segura (SCP) es responsable de copiar archivos desde un servidor remoto al sistema local a través de una conexión segura, asegurando que los datos en tránsito se mantengan confidenciales. Varios productos SCP utilizan una conexión SSH para garantizar la seguridad de la operación de copia segura.

NTP

El Protocolo de tiempo de red (NTP) se utiliza para sincronizar los relojes de los equipos en una red o en Internet. Esto se logra configurando un servidor para que sea el servidor de tiempo, que luego es el servidor desde el cual todas las demás PC de la red sincronizan su tiempo.

En redes Windows anteriores, puede administrar la sincronización de hora colocando un comando en un script de inicio de sesión para sincronizar la hora en el cliente con el servidor de hora. Utilice el siguiente comando:

```
NET TIME \\computername /SET
```

Las redes de Microsoft más recientes, como las redes de Active Directory, tienen el emulador PDC (controlador de dominio principal) que proporciona la hora a todos los servidores y clientes automáticamente, por lo que no es necesario crear un script de inicio de sesión para que los clientes sincronicen la hora con el servidor de tiempo. Los emuladores de PDC también pueden recuperar su tiempo de los servidores NTP de Internet.

Los servidores de tiempo en Internet le permiten sincronizar el reloj de su PC con la hora exacta que mantienen los relojes atómicos. La sincronización horaria tiene en cuenta la configuración de zona horaria de su sistema operativo y le permite sincronizar con un servidor de hora incluso si no está configurado para su zona horaria local.

LDAP

El Protocolo ligero de acceso a directorios (LDAP) es el protocolo TCP/IP para el acceso a servicios de directorio que es compatible con servicios de directorio comunes como Active Directory de Microsoft. LDAP es un protocolo que permite a los clientes LDAP conectarse a la base de datos de red, o directorio, y consultar la base de datos para obtener información sobre sus objetos, como cuentas de usuario e impresoras. Por ejemplo, un usuario de la red podría encontrar el número de teléfono de otro usuario mediante LDAP.

LDAP es el protocolo estándar de la industria para acceder a un servicio de directorio y es compatible con servicios de directorio como Active Directory de Microsoft. LDAP utiliza el puerto TCP 389 de forma predeterminada.

NetBIOS

Network Basic Input/Output System (NetBIOS) es una interfaz de programación de aplicaciones (API) que se utiliza para realizar llamadas de red a sistemas remotos y para la funcionalidad de

administración de sesiones. NetBIOS es un protocolo de capa de sesión instalado con otros protocolos enrutables como TCP/IP para permitir que el tráfico NetBIOS viaje a través de las redes. NetBIOS tiene dos modos de comunicación:

■ **Modo de sesión** Utilizado para la comunicación orientada a la conexión en la que NetBIOS sería responsable de establecer una sesión con el sistema de destino, monitorear la sesión para detectar cualquier error en la transmisión y luego recuperarse de esos errores retransmitiendo cualquier dato que se haya perdido o esté dañado.

■ **Modo de datagrama** Utilizado para la comunicación sin conexión en la que no se necesita una sesión. El modo de datagrama también se utiliza para cualquier difusión de NetBIOS. El modo de datagrama no admite servicios de detección y corrección de errores, que por lo tanto son responsabilidad de la aplicación que utiliza NetBIOS.

Microsoft utiliza nombres NetBIOS, también conocidos como nombres de equipo, como método para identificar sistemas en la red. Un nombre NetBIOS puede tener un máximo de 16 bytes de longitud: 15 bytes para el nombre y 1 byte para el sufijo del nombre NetBIOS (un código al final del nombre que representa el servicio en ejecución). El nombre del equipo NetBIOS debe ser único en la LAN.

Protocolos de almacenamiento en red

Múltiples protocolos permiten que un sistema se comunique con un dispositivo de almacenamiento en disco ubicado en la red:

■ **Fibre Channel** Tecnología que transmite datos de hasta 128 Gbps y utiliza cables ópticos especiales para conectar los dispositivos de almacenamiento compartido a los servidores.

■ **iSCSI** Internet Small Computer Systems Interface es un protocolo basado en IP utilizado para comunicarse con dispositivos de almacenamiento. El tráfico iSCSI transporta comandos de disco SCSI desde un host a un dispositivo de almacenamiento en la red. El beneficio de iSCSI en comparación con Fibre Channel es que no necesita hardware especial para conectarse a la solución de disco compartido; puede utilizar la infraestructura de red existente, junto con iSCSI, para comunicarse con discos compartidos en la red. Es una práctica recomendada ejecutar iSCSI sobre una infraestructura de red dedicada para obtener el mejor rendimiento mientras se utiliza hardware de red convencional.

■ **FCoE** Fibre Channel over Ethernet es un protocolo utilizado para transportar comandos Fibre Channel a través de una red Ethernet en tramas Ethernet. Es importante tener en cuenta que Fibre Channel se ejecuta en la capa 2, por lo que no es enrutable en todas las redes IP (mientras que iSCSI está basado en IP, por lo que es enrutable).

Descripción de IPv6

El examen Security+ se centra en TCP/IP versión 4 (IPv4) para cualquier contenido relacionado con TCP/IP, pero se espera que entienda cómo han cambiado las cosas con IPv6. La primera diferencia importante está en el esquema de direccionamiento: IPv4 se basa en un esquema de direcciones de 32 bits, mientras que IPv6 se basa en un esquema de direcciones de 128 bits.

Partes de Internet ya están utilizando IPv6, y nuevas áreas se están actualizando a diario. IPv6 se basa en un esquema de direcciones de 128 bits porque el esquema de direcciones de 32 bits de IPv4 demostró no crear suficientes direcciones. Uno de los enfoques del protocolo IPv6 fue abordar la escasez de direcciones que existe con IPv4, por lo que el protocolo utiliza un esquema de direcciones de 128 bits.

IPv4 utiliza un esquema de direccionamiento de 32 bits, mientras que IPv6 es un esquema de direcciones de 128 bits que utiliza un formato de dirección hexadecimal. Para el examen Security+, deberá conocer los conceptos básicos sobre el esquema de direcciones IPv6.

Direcciones IPv6

Una dirección IPv6 es una dirección de 128 bits que se muestra en formato hexadecimal y no en la notación decimal punteada utilizada por IPv4. La dirección IPv6 se divide en ocho grupos de 16 bits, cada uno separado por dos puntos (:). A continuación se muestra un ejemplo de una dirección IPv6:

```
65b3:b834:45a3:0000:0000:762e:0270:5224
```

Una dirección IPv6 no admite mayúsculas y minúsculas y no es necesario colocar ceros iniciales al principio de la dirección cuando se hace referencia a un sistema que tiene ceros iniciales al principio. También puede reemplazar los ceros consecutivos por dos puntos dobles (::) al hacer referencia a una dirección que tiene un grupo de ceros en la dirección. Por ejemplo, la dirección de bucle invertido en IPv6 es 0:0:0:0:0:0:0:1 y se puede acortar a ::1, con **el ::** reemplazando todos los ceros consecutivos al principio de la dirección. Este proceso se conoce como *compresión de ceros.* Tenga en cuenta que puede comprimir la dirección solo una vez, por lo que si hay varias partes de la dirección con ceros consecutivos, puede comprimir solo una parte.

Para el examen Security+, debe saber que IPv6 utiliza un espacio de direcciones de 128 bits. También se le puede pedir que identifique la dirección de bucle invertido IPv6, 0:0:0:0:0:0:0:1.

IPv6 utiliza tres tipos de direcciones:

■ **Unicast** Utilizado para la comunicación uno a uno.

■ **Multidifusión** Se utiliza para enviar datos a un grupo de sistemas.

■ **Anycast** Aplicado a un grupo de sistemas que prestan un servicio. Los clientes que envían datos a la dirección anycast podrían tener los datos enviados a cualquiera de los sistemas que forman parte de la dirección anycast.

Para complicar la vida, debe estar familiarizado con los diferentes tipos de direcciones de unidifusión para el examen Security+: la unidifusión global, la unidifusión local del sitio y las direcciones de unidifusión local de enlace manejan diferentes tipos de tráfico de unidifusión. A continuación se presenta un desglose rápido de cada uno de los diferentes tipos de direcciones de unidifusión:

■ **Unidifusión** global Una dirección IPv6 pública que se puede enrutar en Internet. La dirección asignada al host debe ser única en Internet. Este tipo de dirección es equivalente a una dirección IP pública con IPv4.

■ **unidifusión local** del sitio Una dirección privada para el protocolo IPv6; la dirección siempre comienza con *FEC0*. Asignar una dirección local de sitio a un sistema equivale a usar una dirección privada en IPv4, como 10.0.0.0. La dirección local del sitio no se puede utilizar para comunicarse fuera del sitio o la red local y no es accesible para otros sitios o sistemas en Internet.

■ **Enlace-unidifusión local** Una dirección que se autoasigna y se utiliza para comunicarse solo con otros nodos en el enlace. Las direcciones locales de enlace siempre comienzan con *FE80.* Este tipo de dirección es equivalente a una dirección APIPA con IPv4.

Debe estar familiarizado con dos de las direcciones reservadas en IPv6: la dirección de bucle invertido, que es 0:0:0:0:0:0:0:1 (o ::1), y la dirección de un sistema sin dirección especificada, 0:0:0:0:0:0:0:0 (o ::).

Protocolos IPv6

No solo ha cambiado el esquema de direcciones con IPv6, sino también los protocolos que existen en el conjunto de protocolos IPv6. Aquí hay un desglose rápido de algunos de los protocolos utilizados en el conjunto de protocolos IPv6.

IPv6 La nueva versión de IP se encarga de las funciones de direccionamiento lógico y enrutamiento, como es el caso de IPv4. Es un protocolo sin conexión que se basa en protocolos de capa superior como TCP para garantizar la entrega.

ICMPv6 El protocolo ICMP es responsable de la información de error y estado, como en IPv4, pero se ha cambiado. ICMPv6 usa códigos, mientras que ICMPv4 usa tipos y códigos. Para ICMPv6, cada código indica el tipo de mensaje. Los códigos del 0 al 127 son utilizados por los mensajes de error, mientras que los códigos 128 a 255 son para los mensajes de información. Por ejemplo, el mensaje de solicitud de eco es el código 128 con ICMPv6 y el mensaje de respuesta de eco es el código 129.

ICMPv6 ha ampliado sus características sobre lo que está disponible con IPv4. Debe estar familiarizado con las dos características siguientes del protocolo ICMPv6:

■ **Multicast Listener Discovery (MLD)** Reemplaza el protocolo de multidifusión en IPv4 conocido como Internet Group Management Protocol (IGMP) y se utiliza para la comunicación multicast

■ **Neighboring Discovery (ND)** Reemplaza ARP de IPv4 al realizar la misma función, pero también es responsable del descubrimiento de enrutadores vecinos, la asignación automática de direcciones y la detección de direcciones duplicadas, por nombrar algunas características

IPv6 ha sido totalmente rediseñado y ofrece muchas características nuevas adicionales, pero para el examen Security +, solo necesita preocuparse por lo básico. Puede encontrar más información sobre IPv6 en http://technet.microsoft.com/library/dd379473.aspx.

Implicaciones de IPv6

El examen Security+ espera que comprenda las implicaciones de seguridad del uso de IPv6. Aquí hay un resumen de algunas de las preocupaciones de seguridad con IPv6:

■ **Falta de experiencia** Debido a que IPv6 todavía es relativamente nuevo en la mayoría de las redes, existe una falta de experiencia y comprensión completa de los tipos de vulnerabilidades de seguridad que pueden existir en la implementación del protocolo. Esto significa que comprender cómo protegerse contra los ataques IPv6 también es una preocupación para el personal de TI que es nuevo en el protocolo.

■ **Complejidad del protocolo** La complejidad del conjunto de protocolos IPv6 en comparación con IPv4 se suma al número de posibles vías de ataque para los hackers sobre lo que vimos con IPv4. Por ejemplo, IPv6 no solo tiene DHCPv6 para la asignación de direcciones IP, sino que también tiene *configuración automática de direcciones sin estado (SLAAC),* que es otra tecnología que podría presentar una vía de ataque diferente para los piratas informáticos.

■ Compatibilidad con dispositivos de **seguridad IPv6** Una de las otras consideraciones es con los dispositivos de seguridad que protegen los activos de nuestra empresa. ¿Están estos dispositivos de seguridad actualizados con las características de IPv6 y puede utilizar el conjunto de características del dispositivo de seguridad de la misma manera que IPv4 e IPv6? Es posible que falte la compatibilidad con IPv6 para las características de seguridad del dispositivo.

■ **Vulnerabilidades de doble pila** Debido a que las empresas se están moviendo lentamente a IPv6, también necesitarán tener IPv4 en ejecución. Esto significa que está ejecutando dos protocolos diferentes al mismo tiempo, cada uno con su propio conjunto de problemas de seguridad a tener en cuenta. Un riesgo común de ejecutar ambos protocolos es que su empresa puede centrarse en bloquear IPv4 pero no darse cuenta de que IPv6 se carga de forma predeterminada en sus sistemas y dispositivos de red. Si no bloquea IPv6 también, corre el riesgo de ser vulnerable a ataques a través del protocolo IPv6.

EJERCICIO 1-4

Identificación de protocolos en TCP/IP

En este ejercicio, practicará la identificación de los diferentes protocolos TCP/IP asociando el protocolo con el escenario correspondiente.

Protocol	Scenario
____ TCP	A. Converts FQDNs to IP addresses
____ IP	B. Responsible for error reporting and status information
____ DNS	C. Protocol used to download files
____ HTTPS	D. Responsible for network monitoring and management
____ UDP	E. Converts logical address to physical address
____ FTP	F. Protocol used for secure web traffic
____ ICMP	G. Responsible for unreliable delivery
____ ARP	H. Responsible for logical addressing and routing
____ SNMP	I. Responsible for reliable delivery

OBJETIVO DE CERTIFICACIÓN 1.03

Prácticas recomendadas de seguridad de red

Este capítulo le ha expuesto a una serie de conceptos, protocolos y dispositivos de red para que actúen como una revisión de Network+, pero lo que es más importante, para asegurarse de que comprende los conceptos clave de red relacionados con algunos de los temas de seguridad de

capítulos posteriores. Antes de pasar al siguiente capítulo, quiero resumir algunos puntos clave que rodean las mejores prácticas de seguridad con dispositivos y protocolos de red.

Uso del dispositivo

Anteriormente en el capítulo, aprendió sobre el propósito de dispositivos como enrutadores, conmutadores y servidores proxy. Los siguientes son algunos puntos clave que debe recordar que involucran el uso de dispositivos de red para ayudar a crear un entorno de red seguro.

Seguridad física

Asegúrese de que todos los servidores y dispositivos de red, como enrutadores y conmutadores, se almacenen en una ubicación segura, como una sala de servidores cerrada. También desea asegurarse de controlar y supervisar quién tiene acceso a estos componentes físicos de la red.

No usar concentradores

La mayoría de los entornos actuales utilizan conmutadores en lugar de concentradores, pero si observa un concentrador antiguo conectado a la red, asegúrese de reemplazarlo por un conmutador para que el tráfico se envíe solo al puerto en el que reside el sistema de destino.

Configurar contraseñas

La mayoría de los dispositivos de red, como enrutadores y conmutadores, le permiten configurar contraseñas en el dispositivo, lo que le permite controlar quién está autorizado para administrar el dispositivo. Los routers y switches de Cisco tienen una serie de contraseñas diferentes, como una contraseña de puerto de consola, una contraseña de puerto auxiliar y contraseñas de Telnet. Asegúrese de que cada una de estas contraseñas sea compleja. El código siguiente muestra los comandos para configurar una contraseña de consola:

```
HAL-R1>enable
HAL-R1#config term
HAL-R1(config)#line con 0
HAL-R1(config-line)#password C0nP@$$
HAL-R1(config-line)#login
```

Usar la seguridad portuaria

También debe asegurarse de que los puertos del conmutador que no se estén utilizando estén deshabilitados para ayudar a evitar que personas no autorizadas se conecten a un puerto disponible. En entornos altamente seguros, debe configurar la seguridad de puertos en los puertos, que es un método para especificar qué direcciones MAC pueden conectarse a un puerto en particular.

La seguridad del puerto también es una gran contramedida contra *la inundación de MAC,* que implica que el hacker envíe tramas al conmutador que contienen diferentes direcciones MAC de origen. Esto podría hacer que ocurran dos cosas:

■ El conmutador ve todas las entradas falsas en la tabla de direcciones MAC y ya no confía en la tabla, lo que hace que el conmutador inunde todas las tramas en todos los puertos (lo que se conoce como estado de apertura por error).

■ Las entradas de la tabla de direcciones MAC se sobrescriben para que el conmutador no sepa en qué puerto se encuentran las direcciones MAC válidas. Cuando un conmutador no conoce la ubicación de una dirección MAC en particular, inunda la trama a todos los *puertos* del conmutador, lo que le da al hacker la oportunidad de capturar el tráfico porque el conmutador ya no está filtrando el tráfico.

Para el examen Security+, recuerde que la inundación MAC es cuando el hacker confunde el interruptor con la inundación de todas las tramas a todos los puertos. Esto permite al hacker conectarse a cualquier puerto del switch y poder recibir todo el tráfico de la red.

Otro método que un hacker puede usar para eludir la función de filtrado del interruptor es el *envenenamiento por ARP,* que envenena la caché de ARP en todos los sistemas, obligándolos a enviar datos al sistema del hacker para salir a Internet. ¡El hacker captura el tráfico y luego lo enruta a Internet para el usuario! Aprenderá más sobre el envenenamiento por ARP en el Capítulo 4.

Usar VLAN

Otra característica importante de un switch que se debe usar son las VLAN porque ofrecen una forma de crear diferentes límites de comunicación colocando puertos en ellos. Recuerde que, de forma predeterminada, un sistema que está en una VLAN no puede comunicarse con sistemas en otra VLAN.

Uso de cables y protocolos

Cuando se trata de cableado de red en entornos altamente seguros, debe usar cableado de fibra óptica porque la transmisión se transporta a través de pulsos de luz y no a través de una señal eléctrica. Esto tiene grandes beneficios de seguridad porque los datos transportados a través del cableado de cobre como una señal eléctrica son susceptibles a la interferencia de otros componentes eléctricos, mientras que los datos transmitidos a través de fibra óptica son inmunes a la interferencia eléctrica. También tenga en cuenta que el cableado UTP filtra señales, por lo que teóricamente se podrían escuchar las transmisiones. Debido a que el

cableado de fibra óptica no utiliza una señal eléctrica, la transmisión no se filtra y, por lo tanto, no se puede escuchar.

El cableado de fibra óptica tampoco se presta para *aprovechar* la línea tan fácilmente como la comunicación coaxial o de par trenzado. Es posible que un hacker aproveche la línea de fibra óptica reflejando parte de la luz y luego convirtiendo esa luz en información eléctrica para ser vista por la computadora del hacker. Aunque este ataque es posible, también es fácil detectar la pérdida de luz que es causada por este ataque con el sistema de detección de intrusos adecuado en el cable.

Para el examen Security+, recuerde que el tipo de cable más seguro para usar es el cableado de fibra óptica.

Otra práctica recomendada cuando se trabaja en redes grandes que involucran sistemas seguros y no seguros, o lo que algunas organizaciones llaman sistemas protegidos y desprotegidos, es usar cables de diferentes colores para un sistema protegido en comparación con un sistema no protegido. A continuación, al evaluar la seguridad, puede asegurarse rápidamente de que el sistema protegido está conectado a una red protegida y no a una red desprotegida. Una *red protegida* es una red controlada que no está conectada a Internet, mientras que una red *desprotegida* es aquella que está conectada a Internet. En entornos de alta seguridad, es fundamental que un sistema protegido nunca esté conectado a una red desprotegida porque podría estar expuesto a software malicioso de Internet.

En lo que respecta a los protocolos, asegúrese de que está utilizando los protocolos más seguros en todo momento en entornos que requieren la seguridad. Por ejemplo, en lugar de usar Telnet para conectarse de forma remota a sus enrutadores y conmutadores, debe usar SSH. Se deben utilizar los siguientes protocolos seguros en lugar de su equivalente inseguro:

■ Se debe utilizar SSH en lugar de Telnet.

■ Se debe utilizar el comando **scp** (copia segura) en lugar del comando **copy** para copiar información de forma segura entre sistemas.

■ Se debe utilizar FTP seguro (SFTP o FTPS) en lugar de FTP para descargar y cargar archivos.

■ Se debe utilizar HTTPS en lugar de HTTP para cifrar el contenido web entre el cliente y el servidor.

RESUMEN DE LA CERTIFICACIÓN

En este capítulo, revisó los fundamentos de las redes leyendo sobre los tipos de dispositivos y protocolos que existen en la mayoría de los entornos de red en la actualidad. Desde el punto de vista de la seguridad, es fundamental que comprenda los tipos de dispositivos, cables y protocolos que ayudan a crear un entorno seguro. Los siguientes son algunos puntos clave que debe recordar sobre los fundamentos de redes para el examen Security+:

■ Los conmutadores de red se utilizan hoy en día en lugar de los concentradores, de modo que el tráfico se envía solo al puerto que tiene el sistema de destino. Esto ayuda a proteger los datos que se transmiten de ser interceptados.

■ Los routers crean dominios de difusión y son responsables de enrutar (enviar) datos de una red a otra.

■ Las VLAN, una característica importante de un conmutador, crean un límite de comunicación. Cada VLAN en un switch es un dominio de difusión independiente, y se debe usar un enrutador para permitir que un sistema en una VLAN se relacione con otra VLAN.

■ TCP/IP es un conjunto de protocolos; los protocolos más importantes a conocer son TCP, UDP, IP y ARP. (Su examen Security+ definitivamente tendrá varias preguntas sobre algunos de estos miembros del conjunto de protocolos TCP/ IP).

■ El direccionamiento TCP/IP implica la dirección IP, la máscara de subred, las clases de red y las direcciones reservadas especiales. (Memorice cada clase de red para el examen).

Con una sólida comprensión del material presentado en este capítulo, no tendrá problemas con ninguna pregunta relacionada con TCP / IP en el examen Security +. El material presentado aquí no solo es importante para el examen, sino que también será importante después de que asista al examen y continúe con una carrera como profesional de redes.

✓ SIMULACRO DE DOS MINUTOS

Descripción de los dispositivos de red y el cableado

❑Los conmutadores deben utilizarse en lugar de concentradores porque un conmutador filtra el tráfico enviando los datos solo al puerto del conmutador donde reside el sistema de destino, mientras que un concentrador envía los datos a todos los puertos del concentrador, lo que permite que todos los sistemas conectados vean todo el tráfico de red.

❑Los switches tienen excelentes características de seguridad, como poder deshabilitar los puertos no utilizados y configurar la seguridad del puerto, lo que le permite controlar en función de la dirección MAC qué sistemas pueden conectarse a un puerto.

❑Los enrutadores son dispositivos de capa 3 utilizados para enrutar datos de una red a otra. Los enrutadores también se utilizan para dividir una red en múltiples dominios de difusión.

❑Los equilibradores de carga se utilizan para distribuir las solicitudes de los clientes a través de diferentes servidores con el fin de aumentar el rendimiento. Se pueden utilizar varias técnicas para equilibrar la carga: por ejemplo, puede usar round-robin, que rota las solicitudes de manera uniforme a través de los múltiples servidores, o puede usar un algoritmo para decidir qué servidor dentro del equilibrador de carga debe manejar la solicitud.

❑Un servidor proxy se utiliza para enviar solicitudes salientes de Internet en nombre de los clientes y normalmente se utiliza para filtrar los sitios web que un usuario puede visitar y los tipos de aplicaciones que el usuario puede utilizar para la comunicación saliente.

❑El cableado coaxial y de par trenzado utiliza un núcleo de cobre para transportar una señal eléctrica, mientras que el cableado de fibra óptica se utiliza para transportar pulsos de luz. El cableado de fibra óptica es el cableado de elección para entornos altamente seguros.

Descripción de TCP/IP

❑El protocolo IP es responsable del direccionamiento lógico y el enrutamiento.

❑El protocolo TCP se utiliza para una entrega confiable. La comunicación a través de TCP comienza con el apretón de manos de tres vías. TCP garantiza la entrega mediante el uso de números de secuencia y números de confirmación.

❑TCP utiliza indicadores para identificar tipos importantes de paquetes. Los indicadores TCP son SYN, ACK, FIN, RST, URG y PSH.

❑UDP se utiliza para la comunicación sin conexión.

❑TCP y UDP utilizan números de puerto para identificar la aplicación de envío y recepción de los datos. Para el examen Security+, conozca los puertos comunes que se describen en este capítulo.

❑ICMP se utiliza para informes de estado y errores. ICMP utiliza tipos y códigos para identificar los diferentes tipos de mensajes. El tipo 8 se utiliza para la solicitud de eco y el tipo 0 se utiliza para la respuesta de eco.

❑ARP es responsable de convertir la dirección lógica (dirección IP) en una dirección física (dirección MAC).

❑Se utilizan varios protocolos de capa de aplicación para proporcionar funcionalidad a los sistemas TCP/IP. Por ejemplo, FTP se utiliza para las descargas de archivos, mientras que SMTP se utiliza para enviar correo electrónico, y POP3 e IMAP se utilizan para leer el correo electrónico.

❑IPv6 es la versión más reciente del protocolo IP y ha cambiado de IPv4. Algunos de los cambios realizados en IPv6 son que el esquema de direcciones se aumentó a 128 bits, los mensajes de difusión se han eliminado y la seguridad IP está integrada en el protocolo.

Prácticas recomendadas de seguridad de red

❑Asegúrese de utilizar cableado de fibra óptica en lugar de par trenzado porque el cableado de fibra óptica es un poco más difícil de aprovechar y es inmune a la interferencia eléctrica.

❑Utilice versiones seguras de protocolos para cifrar la comunicación. Ejemplos de protocolos seguros son SSH, SCP, HTTPS y FTPS.

❑Asegúrese de utilizar las funciones del conmutador, como la seguridad del puerto, para controlar qué sistemas pueden conectarse al conmutador.

❑Deshabilite todos los puertos no utilizados en el conmutador.

Auto Prueba

Las siguientes preguntas le ayudarán a medir su comprensión del material presentado en este capítulo. Como se indicó, algunas preguntas pueden tener más de una respuesta correcta, así que asegúrese de leer todas las opciones de respuesta cuidadosamente.

1. ¿Qué característica de un conmutador de red permite al administrador de red capturar el tráfico de red al supervisar o solucionar problemas de la red?

A. Protección portuaria

B. VLAN

C. Dominio de colisión

D. Duplicación de puertos

2. Su empresa tiene una aplicación web que parece estar funcionando lentamente. ¿Qué se puede hacer para mejorar el rendimiento de la aplicación?

A. Instale un servidor proxy.

B. Instale un equilibrador de carga.

C. Configurar el sitio web en una VLAN.

D. Configurar la seguridad portuaria.

3. ¿Cuál de los siguientes dispositivos podría utilizarse para limitar qué sitios web pueden visitar los usuarios de la red?

A. Enrutador

B. Equilibrador de carga

C. Servidor proxy

D. CAT 5e

4. ¿Qué protocolo TCP/IP se utiliza para convertir la dirección IP en una dirección MAC?

A. ARP

B. TCP

C. ICMP

D. UDP

5. ¿Qué tipo de ICMP se utiliza para identificar los mensajes de solicitud de eco?

A. 0

B. 4

C. 8

D. 9

6. ¿Cuál de las siguientes identifica las etapas del apretón de manos de tres vías?

A. ACK/SYN, ACK, SYN

B. VISIÓN, VISIÓN/ACK, ACK

C. ACK, SYN, ACK/SYN

D. SYN, ACK, ACK/SYN

7. ¿Cuál de los siguientes puertos representa los puertos utilizados por las aplicaciones TCP seguras? (Elija dos.)

A. 23

B. 22

C. 80

D. 143

E. 443

8. Usted es el administrador de red de una pequeña empresa y desea seguir las mejores prácticas de seguridad relacionadas con el conmutador. ¿Cuál de las siguientes acciones debe hacer para reducir el riesgo de un incidente de seguridad que involucre un conmutador de red? (Elija todo lo que corresponda).

A. Deshabilite los puertos no utilizados.

B. Habilite todos los puertos no utilizados.

C. Configurar la seguridad portuaria.

D. Deshabilite la seguridad portuaria.

E. Habilite la contraseña de la consola.

F. Deshabilite la contraseña de la consola.

9. ¿Qué función de conmutador popular le permite crear límites de comunicación entre los sistemas conectados al conmutador?

A. Intoxicación por ARP

B. Duplicación de puertos

C. Protección portuaria

D. Inundación MAC

E. VLAN

10. Su gerente ha estado leyendo sobre hackers que capturan tráfico de red en un entorno de red conmutado y le ha pedido que explique cómo es posible que los hackers puedan hacer esto. ¿Qué técnicas describirás en tu explicación? (Elija dos.)

A. Intoxicación por ARP

B. Duplicación de puertos

Protección portuaria

D. Inundación MAC

E. VLAN

11. Tiene un servidor con una serie de servicios de red instalados. Usando el diagrama, haga coincidir el número de puerto a la derecha con el servicio de la izquierda.