Packet Tracer - Explorar los Protocolos de Red

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Puerta de enlace predeterminada
R1	G0/0/0	209.165.200.225	255.255.255.248	N/D
	G0/0/1	10.1.1.2	255.255.255.252	
R3	G0/0/0	10.2.2.2	255.255.255.252	N/A
	G0/0/1	172.16.3.1	255.255.255.0	
FIREWALL	VLAN1	192.168.1.1	255.255.255.0	N/A
	VLAN2	209.165.200.226	255.255.255.248	
	VLAN3	192.168.2.1	255.255.255.0	
Servidor DEVASC	NIC	IN: 192.168.2.3	255.255.255.0	192.168.1.1
	VLAN1	OUT: 209.165.200.227	255.255.255.248	209.165.200.225
Ejemplo de Servidor	NIC	64.100.0.10	255.255.255.0	64.100.0.1
PC-A	NIC	DHCP asignado	255.255.255.0	192.168.1.1
PC-B	NIC	172.16.3.2	255.255.255.0	172.16.3.1

Objetivos

Parte 1: Configurar DNS

Parte 2: Configurar DHCP

Parte 3: configurar NTP

Parte 4: Usar SSH para configurar un Switch

Parte 5: Usar SNMP

Parte 6: Configurar HTTPS

Parte 7: Configurar EMAIL

Parte 8: Configurar FTP

Trasfondo/Situación

Muchos servicios se ejecutan en redes detrás de escena para hacer que las cosas sucedan de manera confiable y eficiente. Como desarrollador, debe comprender qué servicios están disponibles y cómo pueden ayudarle. También debe comprender los conceptos básicos de cómo se configuran los servicios más útiles y populares. En Packet Tracer, estos servicios se simulan y la configuración es simple y sencilla. Sin embargo, Packet Tracer hace un muy buen trabajo simulando el tráfico real. A medida que trabaje en este laboratorio y envíe tráfico, le recomendamos que cambie al modo Simulación para explorar el contenido de los distintos tipos de paquetes que la red está generando.

Nota: Packet Tracer no califica todo lo que haces en esta actividad. Sin embargo, debería poder verificar las configuraciones siguiendo los pasos. Al final de la actividad, su porcentaje de finalización debe ser del 100%.

Nota: En esta actividad, los dos servidores web son referidos como **Servidor DEVASC** y **Ejemplo de Servidor** En la topología, son llamados con sus URL: **www.devasc-netacad.pka**y**www.example.com**.

Instrucciones

Parte 1: Configurar DNS

A todos los hosts de una red se les asigna una dirección IP. La dirección IP puede ser una dirección IPv4, una dirección IPv6, o ambas. Esto incluye todos los hosts en Internet también. Pero usted no utiliza su dirección IP para comunicarse con ellos. Utilice nombres comunes como cisco.com. Sistema de nombres de dominio (DNS) es el servicio que traduce automáticamente los nombres comunes y fáciles de recordar en direcciones IP para que la comunicación pueda tener lugar entre dispositivos. En esta actividad de Packet Tracer, los dispositivos utilizan direcciones IPv4.

Paso 1: Configure un servidor DNS local.

a. Haga click en el **Corporate**Server

b. Haga click en **Services**

c. Haga click en **DNS**.

d. Haga clic en el botón **On** para activar el servicio DNS.

Ahora que DNS se ha habilitado, deberá proporcionar la información de todos los hosts de las redes a las que desea traducir su nombre a una dirección IPv4.

e. En el cuadro **Name**, escriba **www.example.com**.

f. La dirección IPv4 del servidor es 64.100.0.10. En el cuadro **Address**, escriba la dirección IPv4.

g. Haga clic en **Add**.

Ahora verá una entrada que muestra el nombre de host y la dirección IPv4 del **servidor de ejemplo**. Aquí es donde DNS buscará el nombre de host y devolverá la dirección IPv4 de ese host a cualquier dispositivo que lo solicite.

Paso 2: Configure y pruebe el uso de un servidor DNS local.

a. Haga click en **PC-A**.

b. Haga click en **Config**.

c. En el cuadro **Servidor DNS**, escriba la dirección IPv4 del servidor DNS **corporativo** : 192.168.1.3.

Ahora, cuando PC-A utiliza nombres de host comunes, enviará una solicitud DNS para la dirección IPv4 del host con ese nombre.

d. Click **Desktop>Simbolo del sistema**

e. Ping **www.example.com**. El ping puede no funcionar la primera vez, o incluso la segunda, a medida que converge la red. Pero por tu tercer intento, debería tener éxito. Observe que la primera línea de la salida muestra que PC-A está utilizando la dirección IPv4 correcta para el **servidor de ejemplo**.

```
Packet Tracer PC Línea de comandos 1.0
C:\> ping www.example.com

Pinging 64.100.0.10 with 32 bytes of data:

Request timed out.
```

```
<output omitted>

C:\> ping www.example.com

Pinging 64.100.0.10 with 32 bytes of data:
Reply from 64.100.0.10: bytes=32 tiempo=3ms TTL=125
<output omitted>

C:\>
```

Nota: Hay un problema conocido con la implementación de Packet Tracer de Firewall. No podrá acceder a los servidores web desde PC-A. Sin embargo, PC-A podrá enviar y recibir correo electrónico a través del servidor de **ejemplo** más adelante en la actividad.

Paso 3: Configure y pruebe el uso de un servidor DNS remoto.

PC-B no tiene un servidor DNS local. Por lo tanto, utilizará el **servidor de ejemplo** como su servidor DNS.

a. Haga click en **PC-B**

b. Haga click en **Config**.

c. En el cuadro **Servidor DNS**, escriba la dirección IPv4 del servidor DNS **corporativo** : 64.100.0.10.

d. Click**Desktop>Simbolo del sistema**

e. Haga ping a **www.example.com**. El ping puede tardar unos segundos, pero debería tener éxito.

f. Haga ping a **www.devasc-netacad.pka**. El ping puede no funcionar la primera vez, o incluso la segunda, a medida que converge la red. Pero por tu tercer intento, debería tener éxito.

g. Cierre la **ventana del símbolo del sistema** y haga click **en Web Browser**.

h. Ingrese **www.example.com** en el campo URL y haga click **Go.** Ahora debería ver la página web Example.com mostrada en el Web Browser.

i. Ingrese **www.devasc-netacad.pka** en el campo URL y haga click en **Go**. Ahora debería ver la página web del servidor DEVASC mostrada en el Navegador Web.

Parte 2: Configure el DHCP

La configuración manual de direcciones IPv4 está bien para redes muy pequeñas, pero en redes más grandes es necesario proporcionar automáticamente direccionamiento IPv4 a los dispositivos cuando se conectan a la red. El Protocolo de configuración dinámica de host (DHCP) proporciona este servicio. También es conveniente cuando los dispositivos se mueven porque si se mueven a una subred diferente, obtendrán una nueva dirección y podrán comunicarse con otros hosts.

Otra gran característica de DHCP es que establece automáticamente no sólo la dirección IPv4 para un host, sino también la subred, la puerta de enlace predeterminada y la dirección del servidor DNS. Esto hace que sea muy fácil configurar varias piezas de información en hosts automáticamente.

Paso 1: Configure DHCP en el servidor corporativo.

Nota: **El** porcentaje de finalización no aumentará hasta que haga clic en Guardar al final de este paso.

a. Haga click en el servidor **corporativo** y luego en **Servicios**, si es necesario.

b. Haga click en **DHCP**.

c. Haga click en el botón **On** para activar el servicio DHCP.

Ahora definirá un grupo de direcciones IPv4 que desea asignar a los hosts. Utilizará direcciones IPv4 en la subred 192.168.1.0. No puede utilizar la dirección 192.168.1.1 porque ya está en uso por la interfaz de

Firewall. Tampoco puede utilizar la dirección del servidor corporativo 192.168.1.3. Además, es una buena práctica dejar algunas direcciones libres para asignar estáticamente a servidores u otros dispositivos donde desea que su dirección siga siendo la misma.

d. El **nombre del grupo** es actualmente **Serverpool**. No lo cambies.

e. Para **la puerta de enlace predeterminada (gateway)**, introduzca la dirección IPv4 de la interfaz INSIDE del **Firewall**: 192.168.1.1.

Esto proporcionará a cada host DHCP una ruta a otras redes.

f. Para **Servidor DNS**, escriba la dirección IPv4 del servidor **corporativo** : 192.168.1.3.

Esto proporcionará a cada host DHCP una dirección para usar para enviar mensajes DNS.

g. Para **Start IP Address**, utilice 192.168.1.10.

Esto proporciona algunos dispositivos asignados estáticamente en la red en el futuro.

h. Para **Máscara de subred (Subnet Mask)**, use 255.255.255.0.

i. Para Número máximo de usuarios, escriba 245, la cantidad restante después de dejar 10 a un lado.

j. Haga click en **Save** para sobrescribir el nombre predeterminado de **Serverpool**.

Paso 2: Pruebe la configuración de DHCP.

a. Haga click en **PC-A**.

b. Cierre el **símbolo del sistema**, si todavía está abierto.

c. Haga clic en **IP Configuration** (Configuración de IP).

d. Haga click en **DCHP**.

Esto puede llevar un poco de tiempo, pero se le debe proporcionar una dirección IPv4 desde el enrutador fuera de las primeras 10 direcciones. También debería ver automáticamente la máscara de subred, la puerta de enlace predeterminada y el servidor DNS.

Parte 3: Configure NTP

El reloj de un router o switch es importante para administrar, proteger y solucionar problemas de redes. Incluso en redes pequeñas, es importante sincronizar la hora en todos los dispositivos. Tratar de hacer esto manualmente es casi imposible, especialmente para redes grandes. El protocolo de tiempo de red (NTP) se puede utilizar para sincronizar la hora en cada dispositivo al recibirla desde un servidor NTP, asegurando que las horas sean todas iguales.

Paso 1: Active el servicio NTP.

a. Haga click en el **Corporate**Server

b. Haga click en **Services**

c. Haga clic en **NTP**.

d. Haga click en el botón **On** junto a **Service**.

Paso 2: Investigue NTP en S2.

S2 ya se ha configurado para utilizar el servidor corporativo como su servidor NTP.

a. Haga click en **S2**.

b. Haga click en **CLI**.

c. Presione **Enter** para obtener un símbolo del sistema. Ingrese al modo EXEC privilegiado con el **comando enable.** Utilice **cisco** como contraseña.

```
S2> enable
Password: <cisco>
S2#
```

d. Muestre la hora y fecha actuales usando el **comando show clock detail**. Observe que el tiempo está establecido por el hardware y no es preciso.

```
S2# show clock detail
* 0:3:44 .318 UTC Lun 1 Mar 1993
Time source is hardware calendar
S2#
```

e. Puede configurar manualmente la hora con el comando **clock**. Sin embargo, una mejor práctica es utilizar un servidor NTP. Ingrese al modo de configuración global con el **comando configure terminal.**

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#
```

f. Configure S2 para utilizar el servidor corporativo como su servidor NTP. Salga del modo de configuración global y verifique que S2 esté usando NTP. Su hora y fecha deberían ser exactas.

```
S2 (config) # servidor ntp 192.168.1.3
S2(config)# exit
S2# show clock detail
14:1:26 .216 UTC Jue May 21 2020
Time source is NTP
S2#
```

Nota: Puede tardar algún tiempo antes de que la fuente se actualice a NTP. Puede hacer click en Tiempo de avance **rápido** (el botón de flecha doble) para acelerar la simulación.

Parte 4: Usar SSH para acceder de forma segura a un switch.

Secure Shell (SSH) es un protocolo que se utiliza para cifrar la comunicación entre un cliente y un host. SSH es el tipo de conexión preferible porque es seguro en comparación con Telnet. SSH ya se ha configurado en S2.

a. Haga click en PC-A. Cierre **la configuración de IP**, si es necesario.

b. Haga click**Escritorio(Desktop)>Simbolo del sistema**

c. Intente establecer una sesión Telnet insegura en S2.

```
C:\  telnet 192.168.1.4
Trying 192.168.1.4... Open


[Connection to 192.168.1.4 closed by foreign host]
```

d. S2 deniega su solicitud porque está configurada solo para acceso SSH. Introduzca el comando **ssh** y **pulse Intro** para ver cómo utilizar el comando. Tenga en cuenta que la opción es una **L**minúscula, no un número **1**.

```
C:\> ssh
Packet Tracer PC SSH


Usage: SSH -l username target


C:\>
```

e. Intente establecer una conexión SSH con S2. La contraseña es **cisco**.

```
C:\  ssh -l administrador 192.168.1.4

Password:



S2>
```

Ahora puede configurar S2 de forma segura.

f. Ahora está accediendo a la línea de comandos de S2 a través de una conexión segura. Introduzca el modo de configuración global con el comando **enable** para verificar que puede configurar el conmutador de forma remota. Utilice **cisco** como contraseña. A continuación, ingrese **exit** para finalizar la sesión SSH.

```
S2> enable
Password:
S2# exit

[Connection to 192.168.1.4 closed by foreign host]
C:\>
```

Parte 5: Investigar ID de objeto MIB SNMP

El Protocolo simple de administración de redes (SNMP) se puede utilizar para obtener y establecer variables relacionadas con el estado y la configuración de los hosts de la red, como los routers y switch, así como las computadoras cliente de la red. El administrador de SNMP puede sondear a los agentes SNMP para obtener datos, o los datos se pueden enviar automáticamente al administrador de SNMP mediante la configuración de traps en los agentes SNMP. En esta parte, recuperará los códigos de Id. de objeto de la Base de información de administración (MIB) para conocer los detalles de los mensajes mediante el explorador MIB.

Los dispositivos Cisco utilizan cadenas de comunidad para autenticar el acceso a la base de información de administración (MIB). Aquí es donde toda la información sobre el dispositivo es guardada. Una cadena de comunidad es simplemente una contraseña de texto sin formato. Las cadenas de comunidad pueden ser de solo lectura (ro) o de lectura y escritura (rw). Estas cadenas de comunidad se han creado para usted en R3 para que pueda investigar la MIB.

Nota: Aunque se puede acceder a SNMP mediante programación para gestionar la red, ahora hay herramientas más sofisticadas disponibles, como verá en el resto de este curso. Sin embargo, SNMP tiene una gran base de instalación en las redes hoy en día y seguirá siendo una valiosa herramienta de gestión para el futuro previsible.

Siga estos pasos para investigar la simulación de SNMP en Packet Tracer.

a. Haga click en **PC-B** Cierre el **Web Browser**, si es necesario.

b. Haga click en **MIB Browser**.

c. Introduzca la dirección de **R3** en el campo **Address** : 172.16.3.1.

d. Haga click en **Advanced**.

e. Introduzca **read** en el campo **Read Community**.

f. Escriba **write** en el campo **Write Community**.

g. Cambie la **versión SNMP** a **v3**.

h. Haga clic en OK.

i. Haga click en la flecha situada junto a **MIB Tree** para expandir el árbol.

j. Haga click en la flecha situada junto a las **MIB router_std**.

k. Continúe expandiendo el árbol hasta que llegue a **.mgmt**.

l. Expanda **.mgmt**.

m. Continúe expandiendo el árbol hasta que llegue a **.system**.

n. Expanda **.system**. Es posible que necesite ampliar la ventana en el punto. También puede agarrar la barra central entre el **MIB Tree** a la izquierda y la **tabla de resultados** a la derecha.

o. Haga click en **.sysName**.

p. Haga click en el botón **GO**

Ahora verá que el valor del objeto es **R3**. Puede ver otros objetos en la MIB, como las interfaces en el router.

q. Expanda el árbol **.interfaces > .IFTable > .IFEntry > .iFoperStatus** y haga click en **Go**.

Verá que dos de tres interfaces están activadas. Ahora puede consultar fácilmente cualquier cosa sobre el router.

Parte 6: Configurar HTTPS

Cuando se conecta a un servidor mediante HTTP, se conecta y asume que es el servidor correcto. Los datos transferidos entre usted y el servidor se envían en texto sin formato, por lo que si alguien capturó esos datos, podría leerlos y manipularlos. Normalmente, esto no es un problema si simplemente estás navegando por Internet. Pero si está creando una cuenta, accediendo a una cuenta o proporcionando cualquier información personal, puede ser capturada y utilizada por otra persona. Secure HTTP (HTTPS) agrega una capa de seguridad mediante el cifrado de la conexión entre usted y el servidor. Un sitio debe poseer un certificado de seguridad de un origen de confianza para comprobar que el sitio es legítimo. El explorador comprueba que el certificado es válido y procedente de una fuente de confianza antes de conectarlo al sitio.

Paso 1: Abre tu página web desde un PC.

a. Haga click en **PC-B**

b. Haga click en **Desktop(Escritorio)**

c. Haga clic en **Web Browser**.

d. Ingrese a **www.devasc-netacad.pka** en el cuadro de la **URL** y haga click en **Go**. Verificaste el acceso antes. Sin embargo, después de hacer click en **Go**, observe que el protocolo es HTTP (http://).

Paso 2: Examine el FIREWALL.

a. Haga click en **FIREWALL**.

b. Haga click en **CLI**.

c. Presione **Enter**.

d. Ingrese **enable** y presione **Enter**.

No hay contraseña, así que presione **Enter**.

e. Ingrese **show run** y presione **Enter**.

f. Utilice la barra espaciadora para desplazarse por la configuración del firewall.

Observe las dos configuraciones siguientes en la lista de acceso OUTSIDE-DMZ:

```
<output omitted>
Access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3
Access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq www
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq 443
<output omitted>
```

La línea con **www** permite el puerto 80, que es tráfico HTTP no seguro. La línea con el puerto **443** permite el puerto 443, que está protegido el tráfico HTTP (HTTPS).

g. Quite la instrucción **de lista de acceso** que permite el tráfico HTTP no seguro en el puerto 80. Introduzca la instrucción **no** versión de la lista de acceso como se muestra a continuación. El comando se ajustará a la siguiente línea, pero no presione **Enter** hasta que haya completado el comando completo.

```
FIREWALL# configure terminal
Firewall (config) # no access-list  OUTSIDE-DMZ extended permit tcp any host
192.168.2.3 eq www
Firewall (config) #
```

Paso 3: Configurar HTTPS.

a. Haga click en el **DEVASC Server**.

b. Haga click en **Services > HTTP**. Observe que HTTP está configurado **en Activado**, pero HTTPS está **Desactivado**.

c. Desactive HTTP y active HTTPS. Aunque el cortafuegos ya no permitirá el acceso HTTP, es recomendable configurar también el servidor para que solo permita HTTPS.

d. Haga click en el botón de opción para que HTTPS lo **active**.

Paso 4: Verfifique la configuración de HTTPS

a. Haga click en **PC-B**

b. Cierre el **Navegador(Browser) MIB**, si es necesario. Haga click en el **Web Browser** para volver a abrirlo.

c. Verifique que **PC-B** ya no pueda acceder a **www.devasc-netacad.pka** mediante HTTP. Después de unos segundos, debería recibir un mensaje de tiempo de **espera de solicitud**. Haga click en **Fast Forward Time** para acelerar esto.

d. Cambie **http** a **https** y haga click en **Go**. Ahora debería ver la página web.

https: //www.devasc-netacad.pka

Parte 7: Configure el EMAIL

Los clientes de correo electrónico utilizan el Protocolo simple de transferencia de correo (SMTP), puerto 25, para enviar correo electrónico a un servidor. SMTP también se utiliza para enviar correo electrónico entre servidores. El cliente de correo electrónico utiliza el protocolo de oficina de correos 3 (POP3), puerto 110, para recuperar correo del servidor.

Paso 1: Configure el servidor EMAIL.

a. Haga click en el **servidor de ejemplo**.

b. Haga click en **Services**.

c. Haga click en **EMAIL**.

d. Active los servicios **SMTP** y **POP3**.

e. Escriba **www.example.com** en el cuadro **Domain Name**.

f. Haga click en **Set**.

Paso 2: Cree usuarios

a. En el cuadro **User**, escriba **student1**.

b. Introduzca **clase** para la contraseña.

c. Haga click **en el cuadro más (+)** para agregar el usuario.

d. Repita este paso para agregar un usuario llamado **student2** con la misma contraseña.

Paso 3: Configure los clientes.

a. Haga click en **PC-A**.

b. Haga click en **Desktop(Escritorio)**

c. Haga click en **EMAIL**.

d. Ingrese la siguiente información:

Your name: **student1**

Email Address: **Student1@www.example.com**

Incoming Mail Server: **64.100.0.10**

Outgoing Mail Server: **64.100.0.10**

User Name: **student1**

Password: **clase**

e. Haga click en **Save**.

f. Repita esta configuración en **PC-B** reemplazando **Student1** por **Student2**.

Paso 4: Enviar y recibir correo electrónico

a. En **PC-B**, abra **Correo electrónico** si no está abierto.

b. Haga click en **Redactar Compose**.

c. Complete la siguiente información:

A: student1@www.example.com

Asunto: Email

En el cuadro de mensaje, escriba un mensaje para Estudiante1 como «¿Cómo estás?«

d. Haga click en **Enviar(Send)**.

e. En **PC-A**, abra **Correo electrónico** si no está abierto.

f. Haga click en**Recibir(Receive)**. Esto puede tomar un poco de tiempo y algunos intentos de completar.

g. Haga doble click en el mensaje cuando llegue para leerlo.

h. Haga click en **Responder(reply)**.

i. Introduce una respuesta al correo electrónico y haz click en **Enviar(Send)**.

j. Haga click en **Enviar(Send)** .

k. Vuelva a **PC**-B, haga click en **Recibir(Receive)** para leer la respuesta.

Parte 8: Configurar FTP

El Protocolo de transferencia de archivos (FTP) es una aplicación comúnmente utilizada para transferir archivos entre clientes y servidores en la red. El servidor está configurado para ejecutar el servicio donde los clientes se conectan, inician sesión y transfieren archivos. FTP utiliza el puerto 21 como puerto de comando del servidor para crear la conexión. A continuación, FTP utiliza el puerto 20 para la transferencia de datos.

Paso 1: Configure el servidor.

a. Haga click en el**Corporate**Server

b. Haga click en **Services**

c. Haga click en **FTP**.

d. Haga click el botón **On** para activar el servicio FTP.

e. En el cuadro **Username**, escriba **student**.

f. En el cuadro **Password**, escriba **class**.

g. Marque todas las casillas debajo de estos campos para establecer el permiso de usuario para permitir escritura, lectura, eliminación, cambio de nombre y lista.

h. Haga click en **Add**.

Nota: En este punto, su porcentaje de finalización debe ser del 100%. De lo contrario, haga click **en Verificar resultados** para ver qué componentes requeridos aún no se completaron. El resto de esta actividad no se clasifica.

Paso 2: Utilice el servicio FTP

a. Haga click en **PC-A**.

b. Haga click en **Desktop(Escritorio)**

c. Haga click en **Símbolo del sistema**.

d. Introduzca **dir** para ver los archivos en el PC.

```
C:\  dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3

Directory of C:\

6/2/2106 23:28 PM 26 sampleFile.txt
26 bytes 1 File (s)
C:\>
```

e. FTP a la dirección IPv4 del servidor corporativo.

```
C:\  ftp 192.168.1.3
Tratando de conectar(Trying to connect)... 192.168.1.3
Connected to 192.168.1.3
220- Welcome to PT Ftp Server
Username:
```

f. Introduzca el nombre de usuario y la contraseña que configuró anteriormente para obtener acceso.

g. **¿ Entrar?** y **pulse enter** para ver los comandos disponibles en el cliente ftp.

```
ftp> ?
         ?
         cd
         delete
         dir
         get
```

```
          help
          passive
          put
          pwd
          quit
          rename
ftp>
```

h. Introduzca **dir** para ver los archivos disponibles en el servidor.

```
ftp dir

Listing /ftp directory from 192.168.1.3:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
<output omitted>
```

i. Introduzca **put sampleFile.txt** para enviar el archivo al servidor.

```
ftp put sampleFile.txt

Writing file sampleFile.txt en 192.168.1.3:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.08 secs (325 bytes/sec)
ftp>
```

j. Utilice el comando **dir** de nuevo para enumerar el contenido del servidor FTP de nuevo para ver el archivo.

k. Introduzca **get asa842-k8.bin** para recuperar el archivo del servidor. Esto puede tardar 30 segundos o más en completarse ya que el archivo es grande.El **tiempo de avance rápido** no ayuda.

```
ftp get asa842-k8.bin

Readind file asa842-k8.bin from 192.168.1.3:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in  46.893 secs (42706 bytes/seg)
ftp>
```

l. Escriba **delete sampleFile.txt** para eliminar el archivo del servidor.

```
ftp delete sampleFile.txt

Deleting file sampleFile.txt from 192.168.1.3: ftp>
[Deleted file sampleFile.txt successfully ]
ftp>
```

m. Introduzca **quit** para salir del cliente FTP.

n. Mostrar de nuevo el contenido del directorio en el PC para ver el archivo de imagen desde el servidor FTP.

En la ventana Instrucciones para esta actividad, su porcentaje de finalización debe ser del 100%. De lo contrario, haga click en **Check Results** para saber cuáles son los componentes requeridos que aún no se completaron.