



Switching y routing CCNA: Introducción a redes

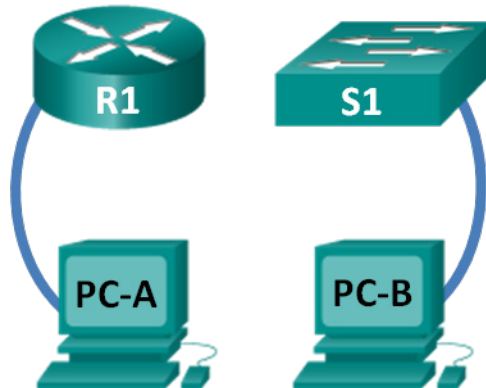
Manual de prácticas de
laboratorio para el instructor

Este documento es propiedad exclusiva de Cisco Systems, Inc. Se otorga permiso a los instructores del curso CCNA Security para uso exclusivo y para imprimir y copiar este documento con el fin de su distribución no comercial como parte de un programa Cisco Networking Academy oficial.

Práctica de laboratorio: Inicialización y recarga de un router y un switch (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Configurar los dispositivos en la red según se muestra en la topología

Parte 2: Inicializar y volver a cargar el router

Parte 3: Inicializar y volver a cargar el switch

Información básica/Situación

Antes de comenzar una práctica de laboratorio de CCNA en la que se utiliza un router o un switch Cisco, asegúrese de que los dispositivos en uso se hayan borrado y no tengan ninguna configuración de inicio. De lo contrario, los resultados de la práctica podrían ser impredecibles. Esta práctica de laboratorio proporciona un procedimiento detallado para inicializar y volver a cargar un router Cisco y un switch Cisco.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio.

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola

Parte 1: Configurar los dispositivos en la red según se muestra en la topología

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Conecte los cables de consola a los dispositivos que se muestran en el diagrama de topología.

Paso 2: Encienda todos los dispositivos de la topología.

Antes de pasar a la parte 2, espere a que todos los dispositivos terminen el proceso de carga de software.

Parte 2: Inicializar el router y volver a cargar

Paso 1: Conéctese al router.

Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando **enable**.

```
Router> enable
Router#
```

Paso 2: Elimine el archivo de configuración de inicio de la NVRAM.

Escriba el comando **erase startup-config** para eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM, non-volatile random-access memory).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Paso 3: Recargue el router.

Emita el comando **reload** para eliminar una antigua configuración de la memoria. Cuando reciba el mensaje Proceed with reload (Continuar con la recarga), presione Entrar para confirmar la recarga. Si se presiona cualquier otra tecla, se anula la recarga.

```
Router# reload
Proceed with reload? [confirm]
```

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 4: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Paso 5: Finalice el programa de instalación automática.

Se le solicitará que finalice el programa de instalación automática. Responda **yes** (sí) y, luego, presione Entrar.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Parte 3: Inicializar el switch y volver a cargar

Paso 1: Conéctese al switch.

Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Paso 2: Determine si se crearon redes de área local virtuales (VLAN, Virtual Local-Area Networks).

Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash
```

```
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

Paso 3: Elimine el archivo VLAN.

- Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Entrar si introdujo el nombre de manera correcta.

- Cuando se le pregunte sobre la eliminación de este archivo, presione Entrar para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Paso 4: Borre el archivo de configuración de inicio.

Utilice el comando **erase startup-config** para borrar el archivo de configuración de inicio de la NVRAM. Cuando se le pregunte sobre la eliminación del archivo de configuración, presione Entrar para confirmar el borrado. (Si se presiona cualquier otra tecla, se anula la operación).

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```



```
[OK]
Erase of nvram: complete
Switch#
```

Paso 5: Recargar el switch.

Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Cuando se le pregunte sobre la recarga del switch, presione Entrar para continuar con la recarga. (Si se presiona cualquier otra tecla, se anula la recarga).

```
Switch# reload
Proceed with reload? [confirm]
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 6: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Escriba **no** en la petición de entrada y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Reflexión

1. ¿Por qué es necesario borrar la configuración de inicio antes de volver a cargar el router?

El archivo de configuración de inicio se carga en la memoria y se convierte en la configuración en ejecución una vez que se vuelve a cargar el router. Al borrar este archivo, el router puede volver a su configuración básica después de una recarga.

2. Después de guardar la configuración en ejecución como la configuración de inicio, encuentra un par de problemas de configuración, por lo que realiza los cambios necesarios para solucionar esos problemas. Si ahora quisiera volver a cargar el dispositivo, ¿qué configuración se restauraría después de la recarga?

Después de una recarga, se restaura la configuración que estaba establecida la última vez que se guardó. Los cambios que se realicen a la configuración en ejecución después de guardar se perderán.

Práctica de laboratorio: Instalación del protocolo IPv6 y asignación de direcciones de host con Windows XP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Instalar el protocolo IPv6 en una PC con Windows XP

- Instalar el protocolo IPv6.
- Examinar la información de dirección IPv6.

Parte 2: Utilizar la utilidad Shell de red (netsh)

- Trabajar en la utilidad **netsh**.
- Configurar una dirección IPv6 estática en la interfaz de la red de área local (LAN).
- Salir de la utilidad **netsh**.
- Mostrar la información de dirección IPv6 mediante **netsh**.
- Emitir instrucciones de **netsh** desde el símbolo del sistema.

Información básica/Situación

El protocolo de Internet versión 6 (IPv6) no está habilitado de manera predeterminada en Windows XP. Windows XP incluye la implementación de IPv6, pero el protocolo IPv6 debe estar instalado. XP no proporciona un método para configurar direcciones IPv6 estáticas desde la interfaz gráfica de usuario (GUI), por lo que todas las asignaciones de direcciones estáticas IPv6 deben realizarse mediante la utilidad Shell de red (**netsh**).

En esta práctica de laboratorio, instalará el protocolo IPv6 en una PC con Windows XP. Luego, asignará una dirección IPv6 estática a la interfaz LAN.

Recursos necesarios

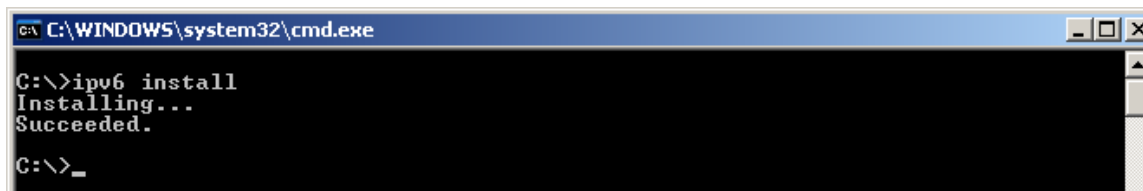
1 PC con Windows XP

Parte 1: Instalar el protocolo IPv6 en una PC con Windows XP

En la parte 1, instalará el protocolo IPv6 en una PC con Windows XP. También utilizará dos comandos para ver las direcciones IPv6 asignadas a la PC.

Paso 1: Instalar el protocolo IPv6.

En la ventana de símbolo del sistema, escriba **ipv6 install** para instalar el protocolo IPv6.



```

C:\WINDOWS\system32\cmd.exe
C:\>ipv6 install
Installing...
Succeeded.
C:\>_
  
```

Paso 2: Examinar la información de dirección IPv6.

Utilice el comando **ipconfig /all** para ver la información de dirección IPv6.

```

C:\WINDOWS\system32\cmd.exe

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-50-56-BE-25-87
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . : Yes
    Autoconfiguration IP Address. . : 169.254.39.128
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : fe80::250:56ff:febe:2587%5
    Default Gateway . . . . . : 
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Teredo Tunneling Pseudo-Interface
    Physical Address. . . . . : FF-FE-FF-FF-FF-FF-FF-FF
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : fe80::ffff:ffff:fffd%4
    Default Gateway . . . . . : 
    NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Automatic Tunneling Pseudo-Interface
    Physical Address. . . . . : A9-FE-27-80
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : fe80::5efe:169.254.39.128%2
    Default Gateway . . . . . : 
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Disabled

C:\>
    
```

Parte 2: Utilizar la utilidad Shell de red (netsh)

Shell de red (**netsh**) es una utilidad de línea de comandos incluida en Windows XP y en sistemas operativos Windows más nuevos, como Vista y Windows 7. Permite configurar información de dirección IPv6 en la LAN. En la parte 2, utilizará la utilidad **netsh** para configurar información de dirección IPv6 estática en una interfaz LAN de una PC con Windows XP. También utilizará la utilidad **netsh** para mostrar la información de dirección IPv6 de la interfaz LAN de la PC.

Paso 1: Trabajar en la utilidad Shell de red

- En la ventana de símbolo del sistema, escriba **netsh** y presione Entrar para iniciar la utilidad **netsh**. El símbolo del sistema cambia de **C:\>** a **netsh>**.

```

C:\WINDOWS\system32\cmd.exe - netsh

C:\>netsh
netsh>
    
```

- En la petición de entrada, introduzca un signo de interrogación (?) y presione Entrar para obtener la lista de parámetros disponibles.

```

netsh>?

The following commands are available:

Commands in this context:
..          - Goes up one context level.
?          - Displays a list of commands.
abort      - Discards changes made while in offline mode.
add        - Adds a configuration entry to a list of entries.
alias      - Adds an alias.
bridge     - Changes to the 'netsh bridge' context.
bye        - Exits the program.
commit     - Commits changes made while in offline mode.
delete     - Deletes a configuration entry from a list of entries.
diag       - Changes to the 'netsh diag' context.
dump       - Displays a configuration script.
exec       - Runs a script file.
exit       - Exits the program.
firewall   - Changes to the 'netsh firewall' context.
help       - Displays a list of commands.
interface  - Changes to the 'netsh interface' context.
lan        - Changes to the 'netsh lan' context.
nap        - Changes to the 'netsh nap' context.
offline    - Sets the current mode to offline.
online     - Sets the current mode to online.
popd       - Pops a context from the stack.
pushd      - Pushes current context on stack.
quit       - Exits the program.
ras        - Changes to the 'netsh ras' context.
routing    - Changes to the 'netsh routing' context.
set        - Updates configuration settings.
show       - Displays information.
unalias    - Deletes an alias.
winsock    - Changes to the 'netsh winsock' context.

The following sub-contexts are available:
bridge diag firewall interface lan nap ras routing winsock

To view help for a command, type the command, followed by a space, and then
type ?.

netsh>

```

- c. Escriba **interface ?** y presione Entrar para obtener la lista de comandos interface.

```

netsh>interface ?

The following commands are available:

Commands in this context:
?          - Displays a list of commands.
add        - Adds a configuration entry to a table.
delete     - Deletes a configuration entry from a table.
dump       - Displays a configuration script.
help       - Displays a list of commands.
ip         - Changes to the 'netsh interface ip' context.
ipv6       - Changes to the 'netsh interface ipv6' context.
portproxy  - Changes to the 'netsh interface portproxy' context.
reset      - Resets information.
set        - Sets configuration information.
show       - Displays information.

The following sub-contexts are available:
ip ipv6 portproxy

To view help for a command, type the command, followed by a space, and then
type ?.

netsh>_

```

Nota: puede utilizar el signo de interrogación (?) en cualquier nivel de la utilidad **netsh** para obtener una lista de las opciones disponibles. Se puede utilizar la flecha hacia arriba para desplazarse por los comandos **netsh** anteriores. La utilidad **netsh** también le permite abreviar comandos, siempre que la abreviatura sea única.

Paso 2: Configurar una dirección IPv6 estática en la interfaz LAN

Para agregar una dirección IPv6 estática a la interfaz LAN, emita el comando **interface ipv6 add address** desde la utilidad **netsh**.

```
netsh>interface ipv6 add address "Local Area Connection" 2001:db8:acad:a::3
Ok.
netsh>
```

Paso 3: Mostrar la Información de dirección IPv6 mediante la utilidad netsh

Para mostrar la información de dirección IPv6, utilice el comando **interface ipv6 show address**.

```
netsh>interface ipv6 show address
Querying active state...

Interface 5: Local Area Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Manual     Preferred  infinite   infinite    2001:db8:acad:a::3
Link       Preferred  infinite   infinite    fe80::250:56ff:febe:2587

Interface 4: Teredo Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::ffff:ffff:ffff:ffff

Interface 2: Automatic Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::5efe:169.254.39.128

Interface 1: Loopback Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Loopback   Preferred  infinite   infinite    ::1
Link       Preferred  infinite   infinite    fe80::1

netsh>
```

Paso 4: Salir de la utilidad netsh.

Para salir de la utilidad **netsh**, utilice el comando **exit**.

```
netsh>exit

C:\>
```

Paso 5: Emitir instrucciones de netsh desde el símbolo del sistema.

Todas las instrucciones de **netsh** se pueden introducir en el símbolo del sistema (fuera de la utilidad **netsh**) si se las precede con el comando **netsh**.

```
C:\>netsh interface ipv6 show address
Querying active state...

Interface 5: Local Area Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Manual     Preferred  infinite   infinite    2001:db8:acad:a::3
Link       Preferred  infinite   infinite    fe80::250:56ff:febe:2587

Interface 4: Teredo Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::ffff:ffff:fffd

Interface 2: Automatic Tunneling Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Link       Preferred  infinite   infinite    fe80::5efe:169.254.39.128

Interface 1: Loopback Pseudo-Interface
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Loopback   Preferred  infinite   infinite    ::1
Link       Preferred  infinite   infinite    fe80::1

C:\>
```

Reflexión

1. ¿Cómo renovaría la información de dirección de la interfaz LAN desde la utilidad **netsh**?

Sugerencia: utilice el signo de interrogación (?) para recibir ayuda sobre cómo obtener la secuencia de parámetros.

Las respuestas pueden variar, pero desde el símbolo del sistema, emitiría el comando **netsh interface ipv6 renew**.

Dibuje su concepto de Internet (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Las redes constan de varios componentes diferentes.

En esta actividad, verá la forma en que se conecta a través de Internet a aquellos lugares, personas o empresas con los cuales interactúa a diario. Después de reflexionar y bosquejar la topología de su hogar o lugar de estudios, puede sacar conclusiones acerca de Internet que tal vez no haya considerado antes de esta actividad.

Información básica/Situación

Dibuje y rotule un mapa de Internet tal como la interpreta en el presente. Incluya la ubicación de su hogar, lugar de estudios o universidad y del cableado, los equipos y los dispositivos correspondientes, entre otros. Es posible que desee incluir algunos de los siguientes elementos:

- Dispositivos o equipos
- Medios (cableado)
- Direcciones o nombres de enlaces
- Orígenes y destinos
- Proveedores de servicios de Internet

Al finalizar, conserve el trabajo en formato impreso, ya que se utilizará para referencia futura al final de este capítulo. Si se trata de un documento electrónico, guárdelo en una ubicación del servidor proporcionada por el instructor. Esté preparado para compartir y explicar su trabajo en clase.

Aquí verá un ejemplo que lo ayudará a comenzar: <http://www.kk.org/internet-mapping>.

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. Su objetivo es ayudar a los estudiantes a reflexionar sobre sus percepciones sobre la manera en que se configura una red para uso personal. Como resultado de esta actividad, el instructor facilitará un debate. La facilitación del debate debe incluir conversaciones entre los estudiantes sobre el trabajo de cada uno.

Recursos necesarios

- Acceso a Internet
- Papel y lápices o bolígrafos (si los estudiantes crean una copia impresa)

Reflexión

1. Después de revisar los dibujos de sus compañeros de clase, ¿había dispositivos informáticos que podría haber incluido en su diagrama? Si la respuesta es afirmativa, indique cuáles y por qué.

Las respuestas varían.

2. Después de revisar los dibujos de sus compañeros de clase, ¿qué similitudes y diferencias encontró en los diseños de algunos modelos? ¿Qué modificaciones le haría a su dibujo después de revisar los otros?

Las respuestas varían.

Dibuje su concepto de Internet

3. ¿De qué manera los íconos en el dibujo de una red podrían organizar el proceso mental y facilitar el aprendizaje? Justifique su respuesta.

Los estudiantes notarán que tener un conjunto de íconos representativos los ayudarán a aprender la forma de dibujar o diseñar la representación de una red. Esto permite consolidar la información y es fácil de entender para aquellos que comprenden lo que representan los íconos. Es una forma de clave para los que se desempeñan en el mismo sector.

Diagramas de red y componentes de red iniciales (varían). A continuación, se incluye una representación de diseño de red muy básica extraída del sitio Web (este diagrama es para referencia del instructor).



Práctica de laboratorio: Investigación de herramientas de colaboración de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Utilizar herramientas de colaboración

- Identificar el nivel de conocimiento actual de herramientas de colaboración.
- Identificar los motivos clave para utilizar herramientas de colaboración.

Parte 2: Compartir documentos mediante Google Drive

Parte 3: Explorar conferencias y reuniones Web

Parte 4: Crear páginas wiki

Información básica/Situación

Las herramientas de colaboración de red les proporcionan a las personas la oportunidad de trabajar juntas de manera eficaz y productiva sin las limitaciones de la ubicación o la zona horaria. Entre los tipos de herramientas de colaboración, se incluyen el uso compartido de documentos, las reuniones Web y las wikis.

En la parte 1, identificará las herramientas de colaboración que utiliza actualmente. También investigará algunas herramientas de colaboración populares que se usan en la actualidad. En la parte 2, trabajará con Google Drive. En la parte 3, investigará las herramientas para conferencias y reuniones Web y, en la parte 4, trabajará con wikis.

Nota para el instructor: esta práctica de laboratorio puede asignarse como tarea para el hogar.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Utilizar herramientas de colaboración

Paso 1: Indique algunas herramientas de colaboración que utiliza actualmente.

Las respuestas varían, pero podrían incluir: Google Drive, Cisco Webex, Citrix Go to Meeting, Confluence Wiki.

Paso 2: Indique algunos motivos para utilizar herramientas de colaboración.

Las respuestas varían, pero podrían incluir: centralización, menos correo electrónico, menos viajes y menor impacto ambiental.

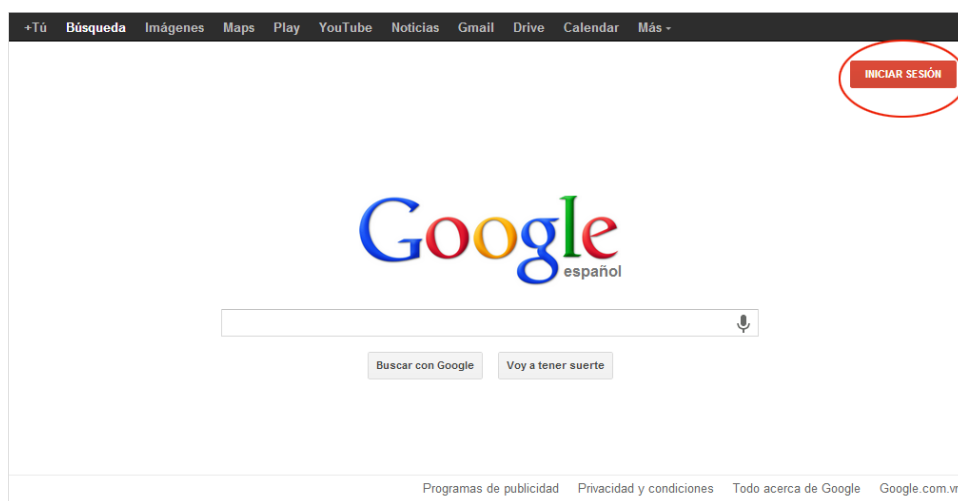
Parte 2: Compartir documentos mediante Google Drive

En la parte 2, explorará las funciones de uso compartido de documentos utilizando Google Drive para configurar dicha característica. Google Drive, anteriormente llamado Google Docs, es un conjunto de aplicaciones de oficina y un servicio de almacenamiento de datos basado en la Web que permite a los usuarios crear y editar documentos en línea mientras colaboran con otros usuarios en tiempo real. Google Drive proporciona 5 GB de almacenamiento con cada cuenta gratuita de Google. Si lo desea, puede adquirir almacenamiento adicional.

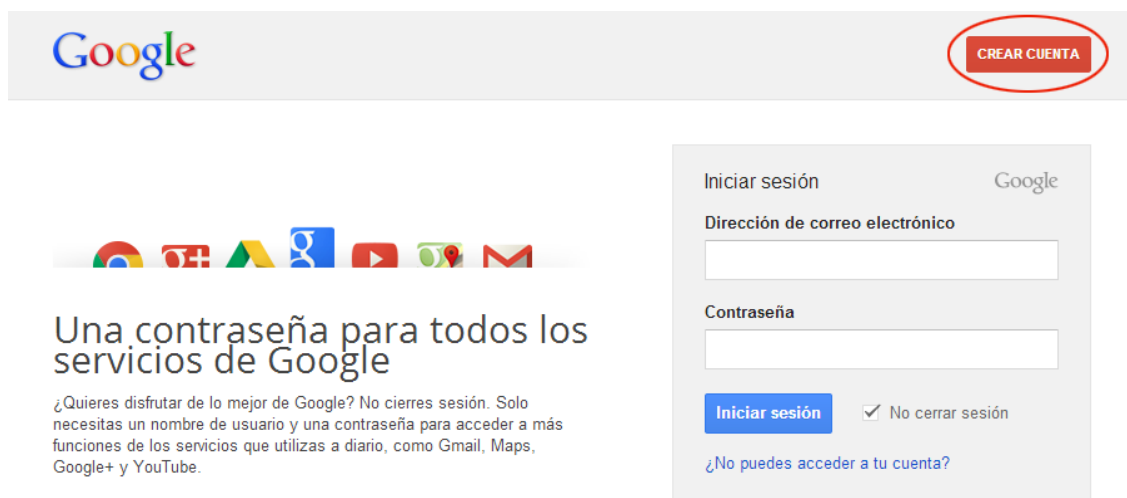
Paso 1: Crear una cuenta de Google

Para utilizar cualquiera de los servicios de Google, primero debe crear una cuenta de Google. Esta cuenta puede usarse con cualquiera de los servicios de Google, incluido Gmail.

- a. Acceda a www.google.com y haga clic en **Iniciar sesión** (en la esquina superior derecha de la página Web).



- b. En la página Web de Cuentas de Google, puede acceder en el momento si ya posee una cuenta de Google, de lo contrario, haga clic en **CREAR CUENTA**.



- c. En la página Web Crea tu cuenta de Google, complete el formulario de la derecha. El nombre que introduzca en el campo **Nombre de usuario** se convierte en el nombre de la cuenta. No es necesario proporcionar el teléfono celular ni la dirección de correo electrónico actual. Debe aceptar las Condiciones del servicio y la Política de privacidad de Google y, luego, hacer clic en **Siguiente paso**.

Inicio sesión

Crea tu cuenta de Google



Con tu cuenta de Google no solo podrás buscar

Habla, chatea, comparte, almacena, organiza, colabora, descubre y crea. Utiliza los productos de Google, desde Gmail hasta Google+ o YouTube, y consulta tu historial de búsqueda con solo introducir tu nombre de usuario y contraseña. Tendrás copias de seguridad de toda tu información disponibles en Google.com.



Tu información siempre disponible

Con una cuenta de Google, puedes acceder a todo tu contenido (a Gmail, a tus fotos, etc.) desde cualquier dispositivo. Puedes hacer búsquedas por voz o utilizando fotos, usar la función gratuita de navegación paso a paso, subir tus fotos automáticamente e incluso comprar desde el móvil con Google Wallet.



Comparte cuanto quieras

Elige el contenido que quieras compartir con tus amigos, con tu familia e incluso con tu jefe en Google+. Inicia una videollamada con amigos, envía un mensaje a varias personas de un grupo a la vez o...

Nombre

No puedes dejar este campo en blanco.

Nombre de usuario

@gmail.com

Prefiero utilizar mi dirección de correo electrónico actual

No puedes dejar este campo en blanco.

Contraseña

Confirma tu contraseña

Fecha de nacimiento

Sexo

Teléfono móvil

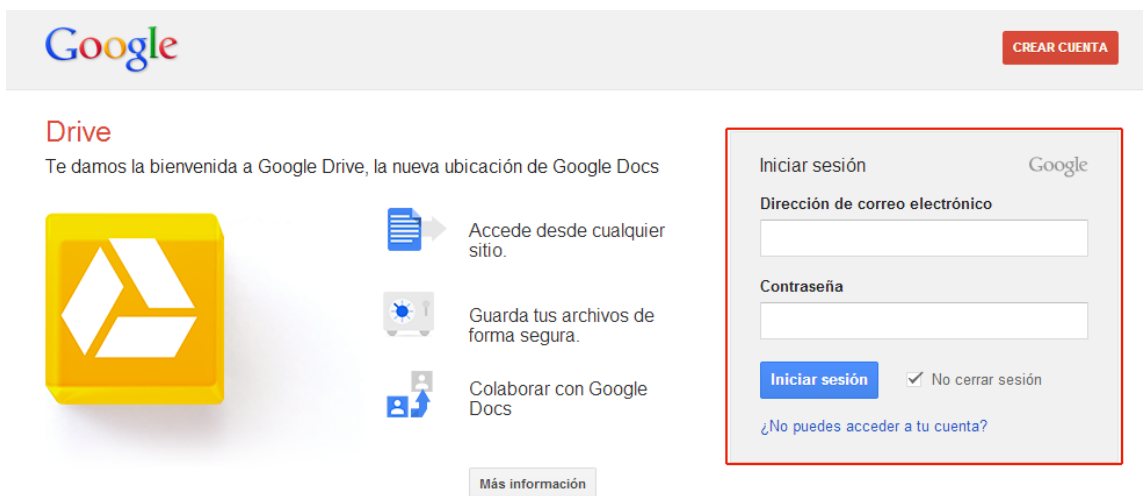
Tu dirección de correo electrónico actual

Demuéstranos que no eres un robot

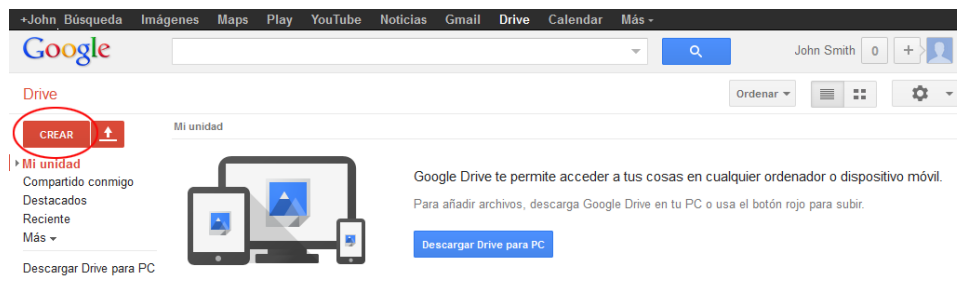
- d. En la página Web siguiente, puede agregar una foto de perfil, si lo desea. Haga clic en **Siguiente paso** para completar el proceso de creación de la cuenta.

Paso 2: Crear un documento nuevo

- Inicio sesión en Google utilizando las credenciales de acceso que creó en el paso 1. Escriba **http://drive.google.com** en su explorador y presione Entrar. Accederá a Google Drive.



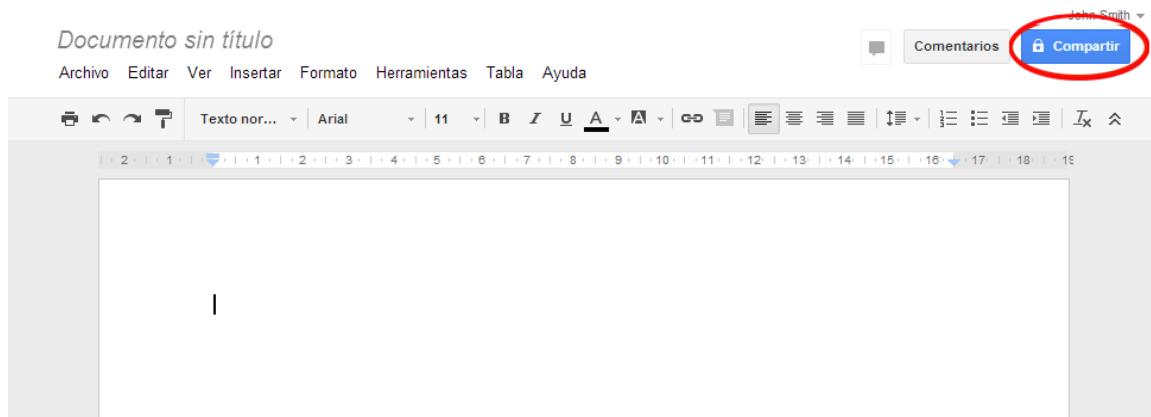
- Haga clic en el botón **CREAR** y aparecerá un menú desplegable para que seleccione el tipo de documento que desea crear. Seleccione **Documento**.



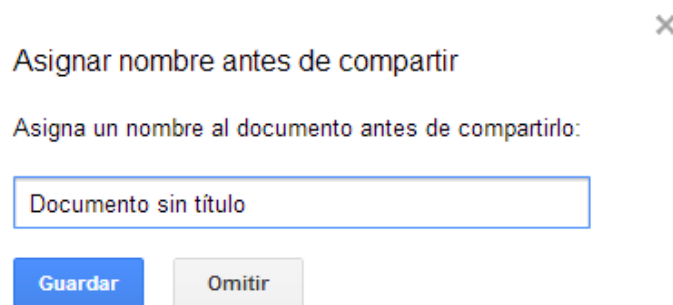
Aparecerá el documento nuevo. Muchas de las funciones del editor de Google funcionan de manera similar a Microsoft Word.

Paso 3: Compartir un documento de Google

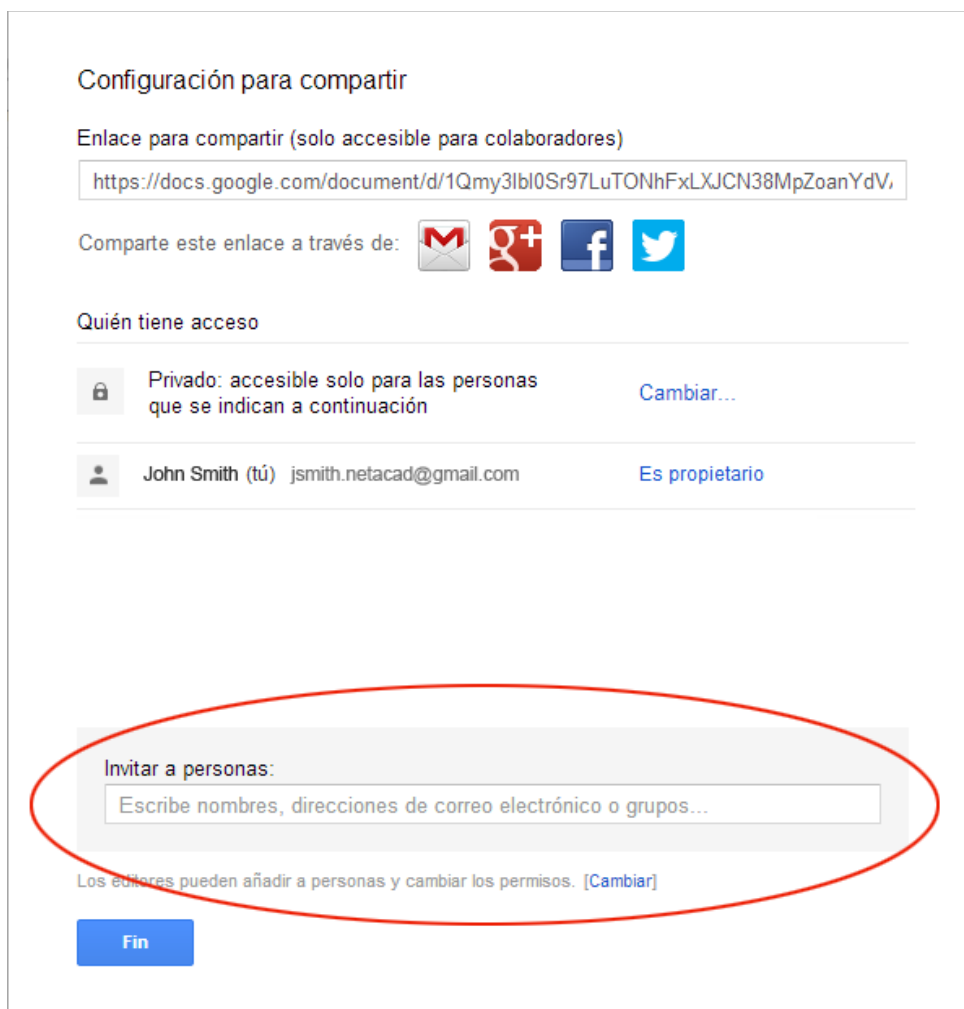
- a. Una vez que el documento en blanco de Google se abre, puede compartirlo con otros usuarios haciendo clic en el botón **Compartir** (en la esquina superior derecha de la página Web).



- b. Nombre el documento nuevo y luego haga clic en el botón **Guardar**.



- c. Aquí, en la página Web Configuración para compartir, en el campo de texto **Invitar a personas** puede introducir nombres de correo electrónico, direcciones de correo electrónico o grupos de Google con quienes compartir este documento.



Configuración para compartir

Enlace para compartir (solo accesible para colaboradores)

<https://docs.google.com/document/d/1Qmy3l0Sr97LuTONhFxLXJCN38MpZoanYdV/>

Comparte este enlace a través de:    

Quién tiene acceso

	Privado: accesible solo para las personas que se indican a continuación	Cambiar...
	John Smith (tú) jsmith.netacad@gmail.com	Es propietario

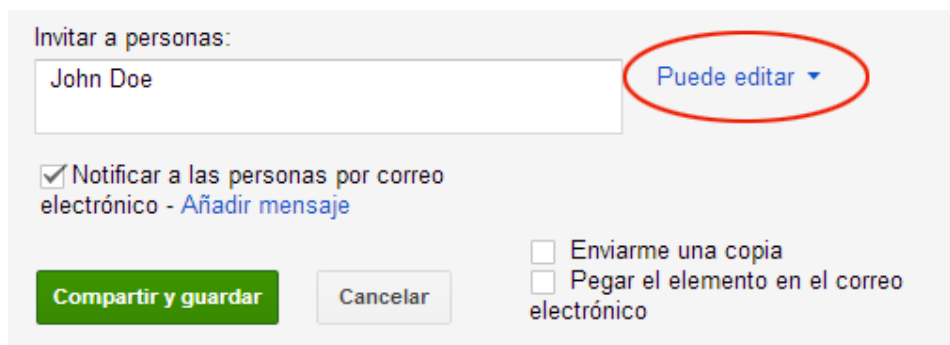
Invitar a personas:

Escribe nombres, direcciones de correo electrónico o grupos...

Los editores pueden añadir a personas y cambiar los permisos. [\[Cambiar\]](#)

[Fin](#)

- d. No bien comience a introducir la información en el cuadro **Invitar a personas**, el cuadro proporcionará más opciones. El menú desplegable **Pueden editar** le permite elegir los privilegios del documento (Puede editar, Puede comentar, Puede ver) para las personas que agregue. También puede especificar cómo notificar a estas personas sobre este documento (**Enviarme una copia** o **Pegar el elemento en el correo electrónico**). Haga clic en **Compartir y guardar**.



Invitar a personas:

John Doe

Puede editar ▼

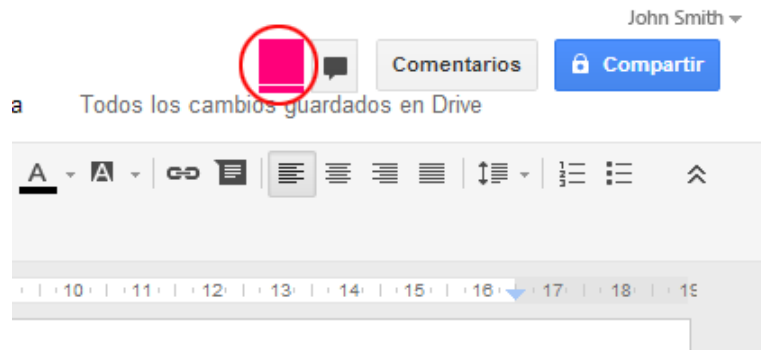
☒ Notificar a las personas por correo electrónico - Añadir mensaje

☐ Enviarme una copia

☐ Pegar el elemento en el correo electrónico

[Compartir y guardar](#) [Cancelar](#)

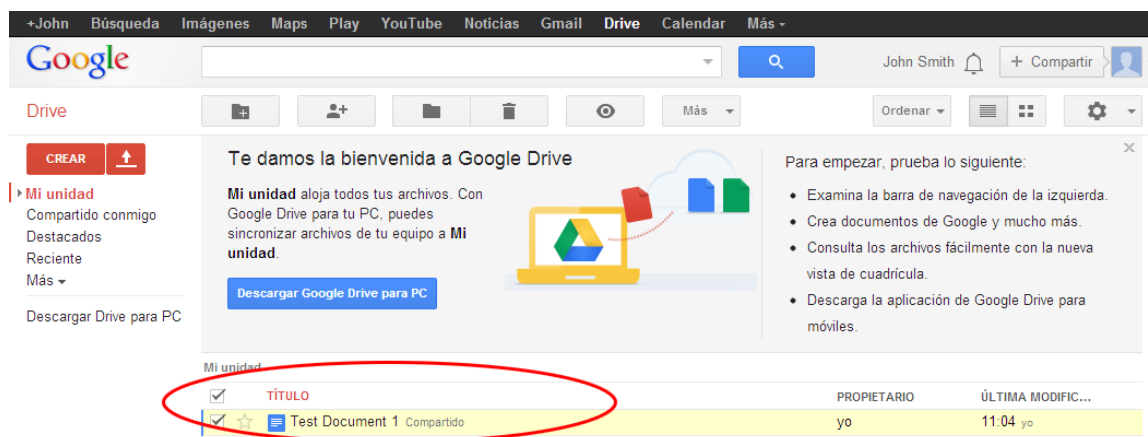
- e. Haga clic en el botón **Fin**. Volverá al documento abierto.
- f. Todos los usuarios con privilegios de uso compartido pueden ver este documento al mismo tiempo. Los usuarios con privilegios de edición pueden editar este documento mientras otros lo ven.
- g. Si alguien está viendo el documento mientras usted lo tiene abierto, podrá ver quiénes son al hacer clic en el menú desplegable **otros lectores** (en la esquina superior derecha del documento).



Paso 4: Cerrar un documento de Google

Para cerrar un documento de Google, mueva el cursor hasta el nombre del documento en la parte superior de la pantalla, y aparecerá una flecha hacia la izquierda a la izquierda del nombre. Haga clic en esa flecha para volver a su página de inicio de Google Drive. El documento se guarda automáticamente.

El documento nuevo aparecerá al comienzo de la lista de documentos, debajo de Mi unidad.



Paso 5: Información adicional

Google desarrolló aplicaciones para PC y smartphones. Para obtener más información acerca de Google Drive, visite <http://drive.google.com>. YouTube también es una fuente posible de tutoriales de Google Drive.

Parte 3: Explorar conferencias y reuniones Web

Las reuniones web combinan el uso compartido de archivos y presentaciones con voz, video y el uso compartido del escritorio. Cisco WebEx Meeting Center es uno de los principales productos de reuniones Web disponibles en la actualidad.

En la parte 3 de esta práctica de laboratorio, verá un video producido por Cisco en el que se repasan las características incluidas en WebEx Meeting Center. El video se encuentra en el siguiente enlace de YouTube: http://www.youtube.com/watch?v=fyaWHEF_aWg

Nota para el instructor: para obtener más herramientas de conferencias de WebEx, puede registrarse para obtener una cuenta gratuita de WebEx Meeting Basics en www.webex.com.

Parte 4: Crear páginas wiki

“Wiki” es una palabra del idioma hawaiano que significa rápido. En términos de redes, una wiki es una herramienta de colaboración basada en la Web que permite que prácticamente todos puedan publicar información, archivos o gráficos en un sitio común para que otros usuarios los lean y modifiquen. Las wikis proporcionan acceso a una página de inicio que tiene una herramienta de búsqueda para ayudarlo a localizar los artículos que le interesan. Las wikis pueden instalarse para la comunidad de Internet o detrás de un firewall corporativo para uso de los empleados. El usuario no solo lee el contenido de la wiki, sino que también participa mediante la creación de contenido en un explorador Web.

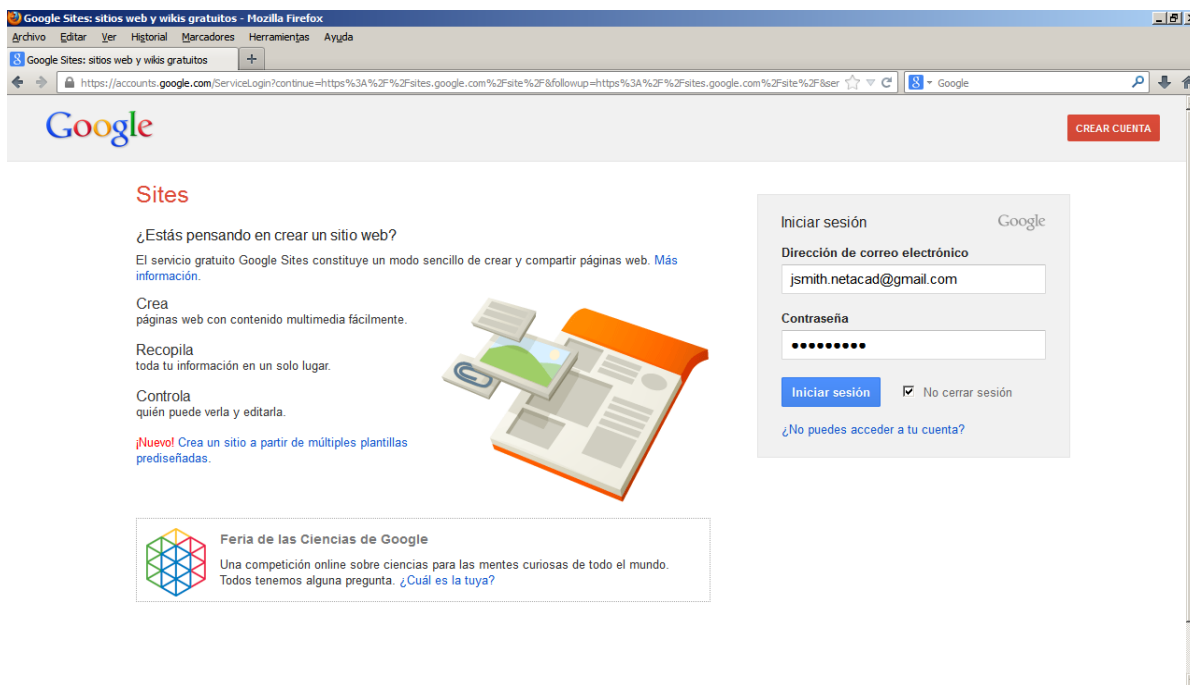
Si bien hay distintos servidores wiki disponibles, todas las wiki incluyen las siguientes características comunes:

- Se puede utilizar cualquier explorador Web para ver o editar páginas, o crear contenido nuevo.
- Los enlaces edit y auto están disponibles para editar una página y automáticamente enlazar páginas. La forma de dar formato al texto es similar a la creación de un correo electrónico.
- Se utiliza un motor de búsqueda para la ubicación rápida de contenidos.
- Se puede configurar el control de acceso mediante el creador de temas que define quién está autorizado a editar el contenido.
- Una wiki es un grupo de páginas Web con diferentes grupos de colaboración.

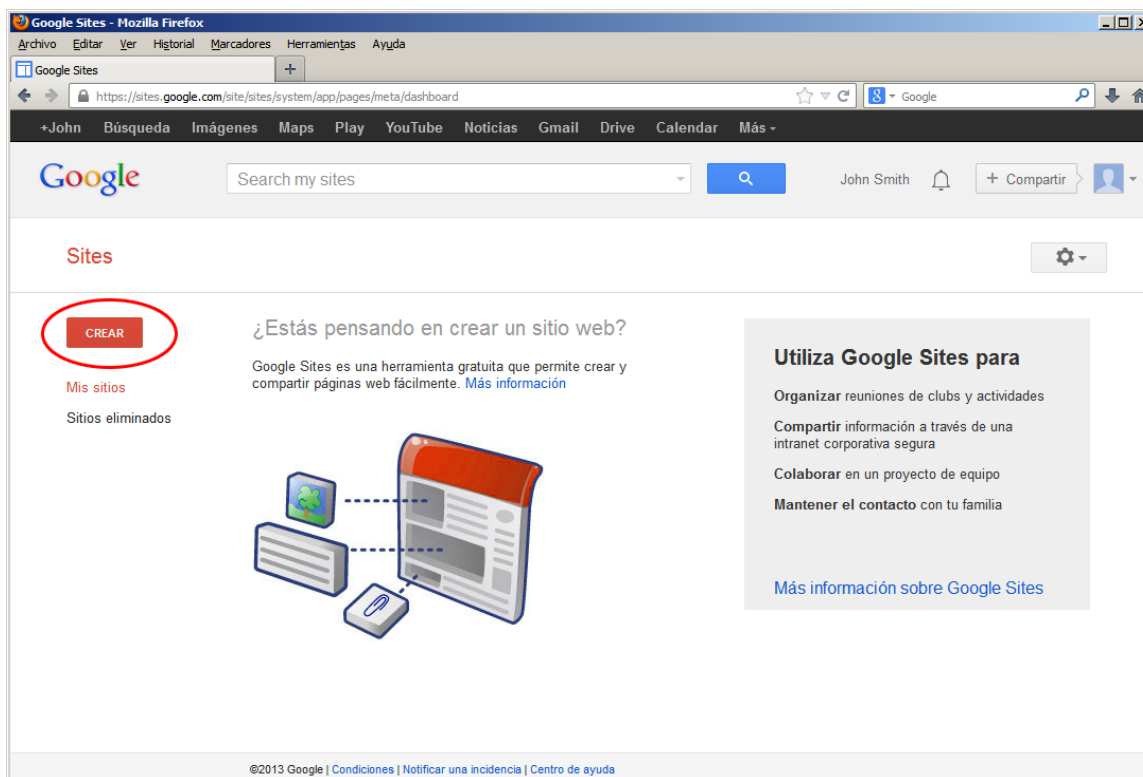
En esta parte de la práctica de laboratorio, utilizará la cuenta de Google que creó en la parte 2 y creará una página wiki en Google Sites.

Paso 1: Ingresar a Google Sites

Acceda a <http://sites.google.com> e inicie sesión utilizando la cuenta de Google que creó en la parte 2 de esta práctica de laboratorio.



Paso 2: Haga clic en CREAR.



Paso 3: Nombrar el nuevo sitio wiki

En el campo **Nombre del sitio**, escriba un nombre para su nuevo sitio wiki. Debe pensar un nombre único para su sitio que no haya sido utilizado por ningún otro usuario de Google. Google también requiere que ingrese el código (que aparece en la parte inferior de la pantalla) para evitar que scripts automatizados, llamados “robots Web”, creen varios sitios. Después de introducir el nombre del sitio, haga clic en el botón **CREAR**. Si alguien ya usó su nombre del sitio, se le solicitará que introduzca otro nombre.

Práctica de laboratorio: Investigación de herramientas de colaboración de red

+John Búsqueda Imágenes Maps Play YouTube Noticias Gmail Drive Calendar Más -

Google Search my sites John Smith + Compartir

Sites **CREAR** Cancelar

Selecciona una plantilla para usar:

 Plantilla en blanco

 Classroom site

 Navegar por la galería para ver más

Nombre del sitio:
Wiki Example C1LA

Ubicación del sitio: las URL solo pueden contener los caracteres siguientes: A-Z, a-z, 0-9
https://sites.google.com/site/

► Selección de un diseño

► Más opciones

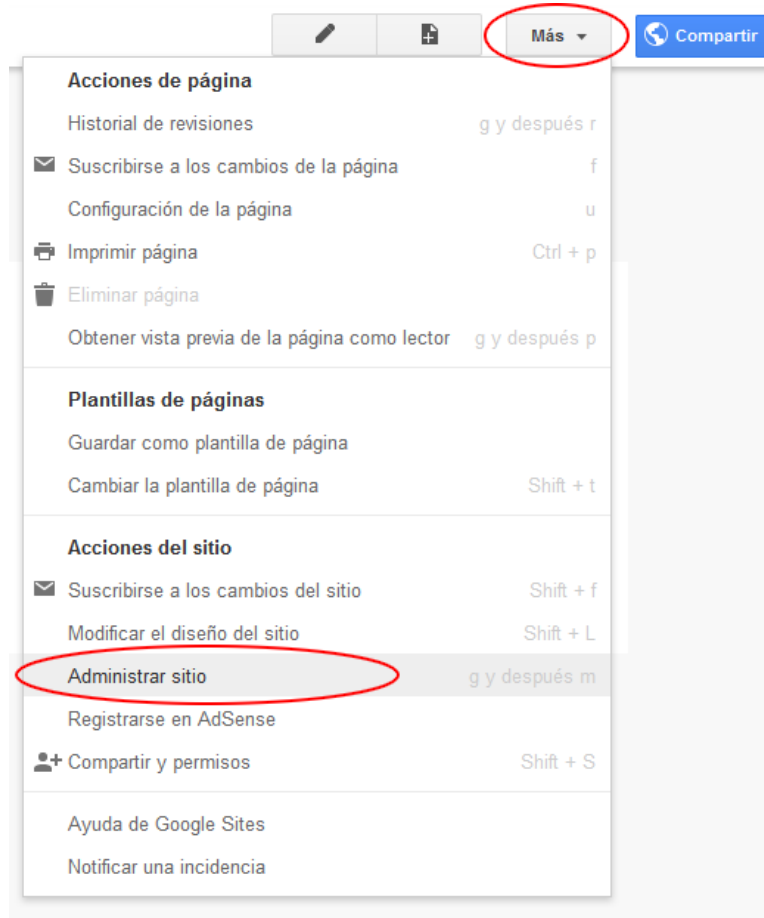
Escribe el código que aparece:

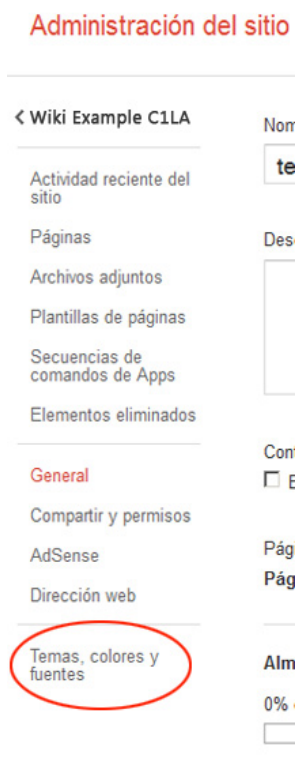
©2013 Google | Condiciones | Notificar una incidencia | Centro de asistencia

Paso 4: Editar el aspecto de su nuevo sitio wiki

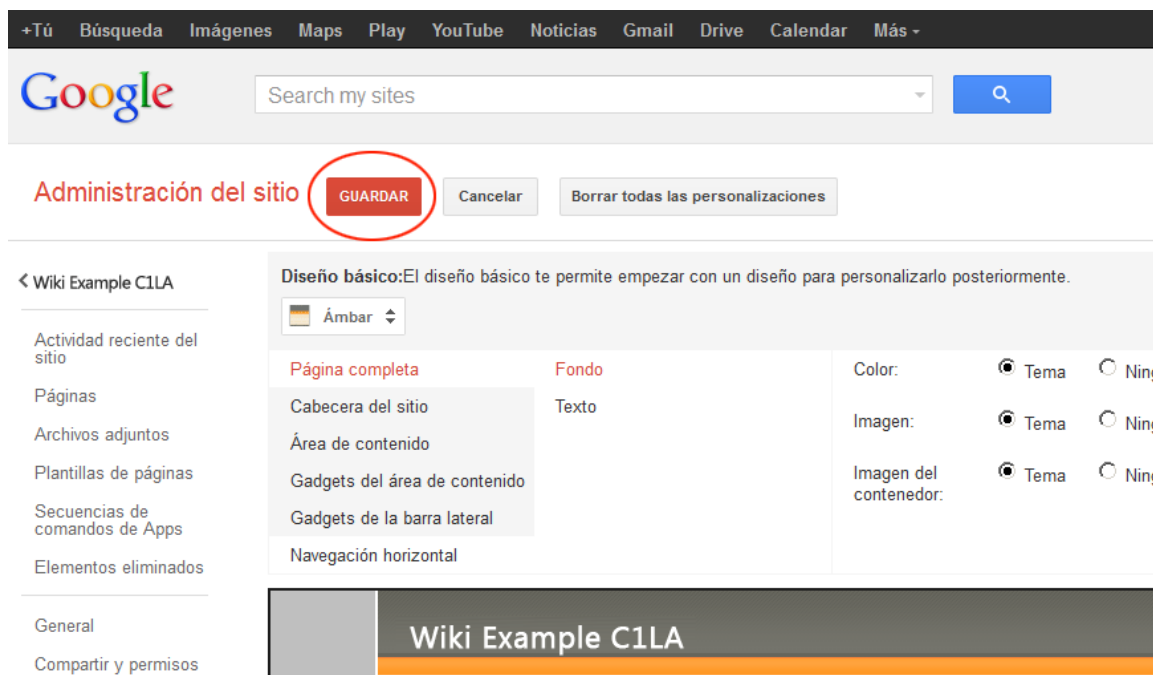
- a. Google proporciona plantillas para que pueda cambiar el aspecto de su nuevo sitio wiki. Haga clic en el menú desplegable **Más** y, a continuación, haga clic en **Administrar sitio**.



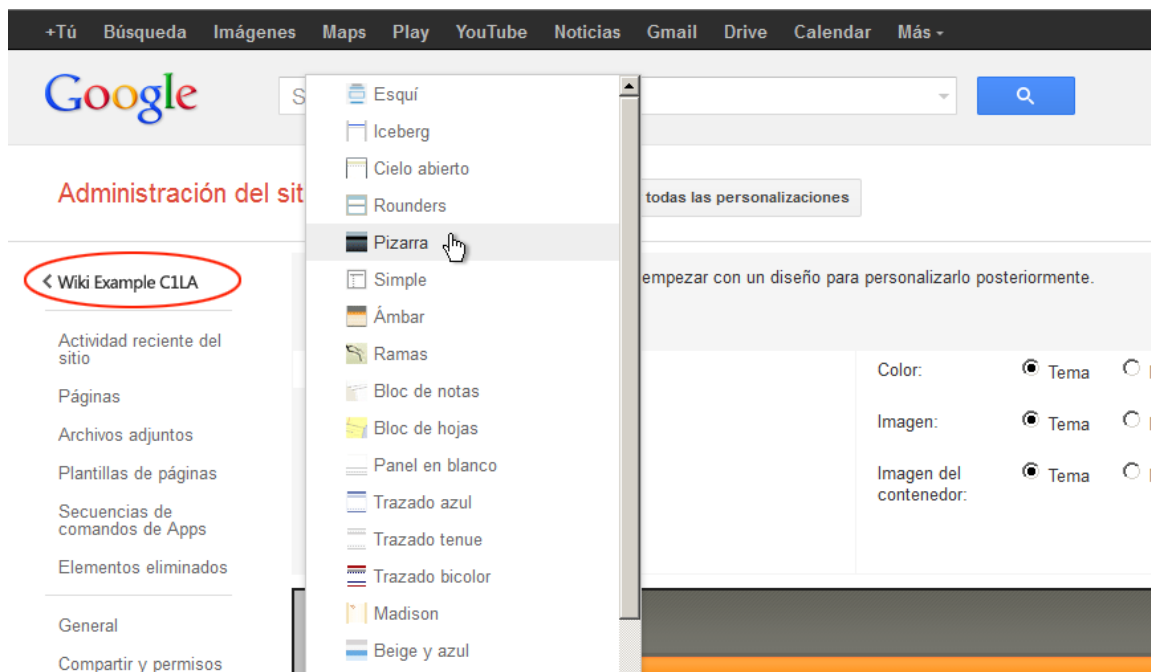
- b. Haga clic en **Temas, colores y fuentes**, en la parte inferior de la barra lateral izquierda.



- c. Seleccione un tema que le guste y haga clic en **GUARDAR**.

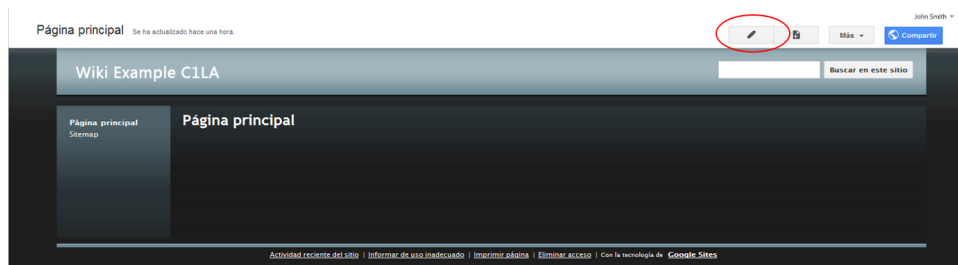


- d. Después de guardar el tema seleccionado, haga clic en el nombre del sitio debajo de **Administración del sitio**.

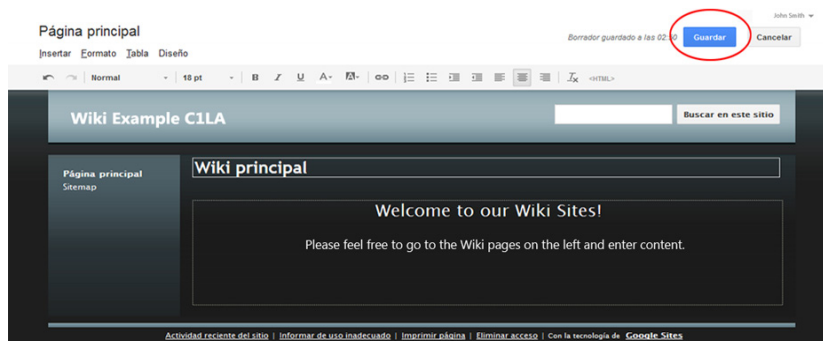


Paso 5: Actualizar la página de inicio

- a. La página de inicio es la primera página que todos verán cuando accedan a su sitio wiki. El contenido de esta página se puede editar haciendo clic en el botón de edición. Desde aquí, podrá agregar texto, imágenes o cualquier otra cosa que desee mostrar en esta página.

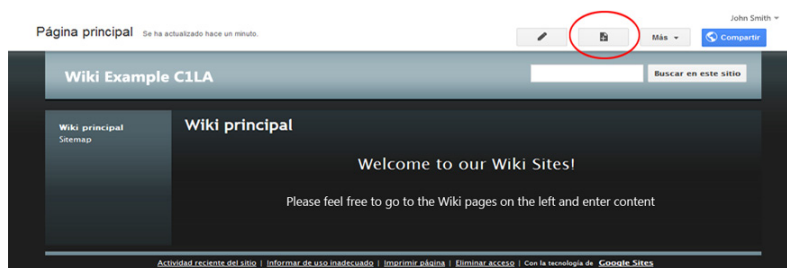


- b. Después de realizar los cambios, haga clic en **Guardar**. De esta manera, saldrá del modo de edición de la página.



Paso 6: Crear una página wiki

- a. Para crear una página nueva que usted y sus visitantes puedan utilizar para hacer publicaciones, haga clic en el ícono de página nueva.



- b. En el campo **Asigna un nombre a tu página**, introduzca un nombre para la página. En el ejemplo que se muestra a continuación, se utiliza el nombre Routers como el tema para esta página.

Sites

Crea una página en el sitio: Wiki Example C1LA

Asigna un nombre a tu página:

URL de tu página: /site/testwidk/routers [Cambiar URL](#)

- c. Haga clic en el menú desplegable **Página web** y seleccione **Anuncios**. Google utiliza este término para indicar una página wiki.

Crea una página en el sitio: Wiki Example C1LA

Asigna un nombre a tu página:

URL de tu página: /site/testwidk/routers [Cambiar URL](#)

Seleccionar una plantilla ([Más información](#))

☐ Página web

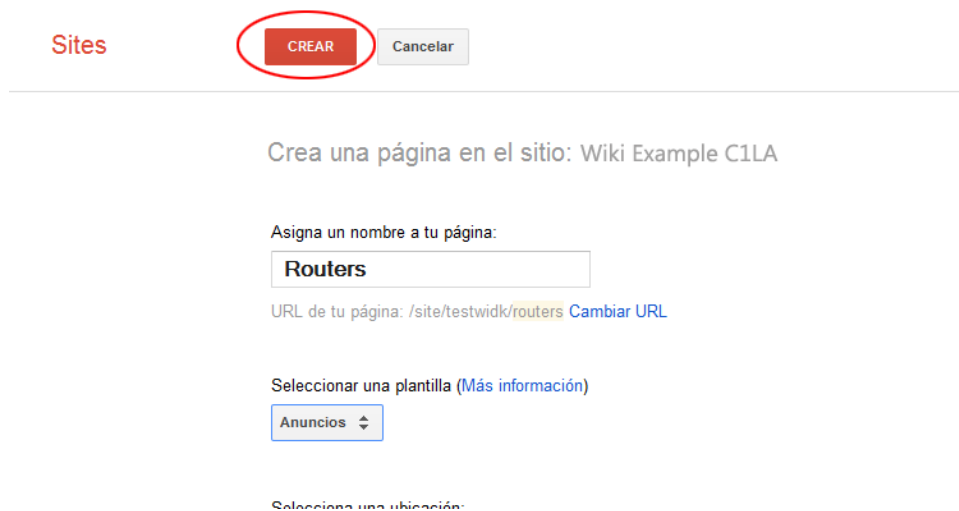
☒ Anuncios

☐ Archivador

☐ Lista

☐ Clasificar la página en Wiki principal

- d. Haga clic en **CREAR** para crear la página wiki nueva.



Sites

CREAR Cancelar

Crea una página en el sitio: Wiki Example C1LA

Asigna un nombre a tu página:

Routers

URL de tu página: /site/testwik/routers [Cambiar URL](#)

Seleccionar una plantilla ([Más información](#))

Anuncios

Selecciona una ubicación:

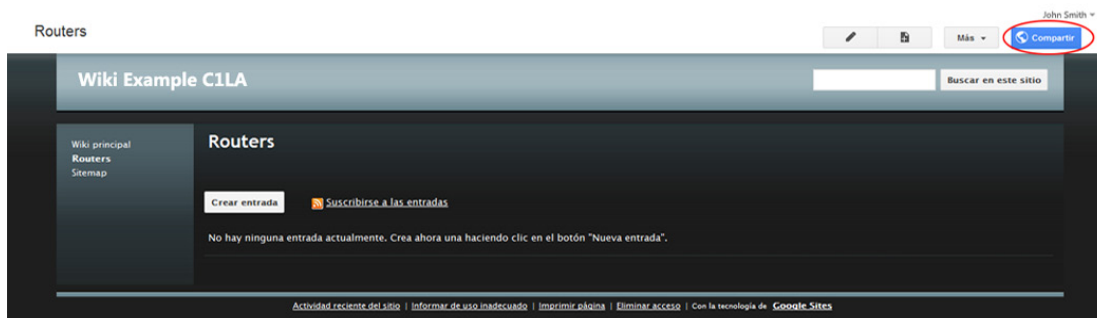
- e. Se muestra la página wiki nueva, llamada Routers, que tiene una opción de menú **Crear entrada** que permite agregar información a la página. (Observe que, en la barra lateral izquierda, hay un enlace nuevo para que los visitantes al sitio puedan acceder a esta página).



Paso 7: Compartir el sitio Web

Un sitio wiki no es realmente un sitio wiki hasta que otras personas puedan contribuir. Hay varias maneras de compartir el sitio nuevo. En este ejemplo, le mostraremos cómo compartir el sitio con personas designadas que tengan cuentas de Gmail.

- a. En el sitio wiki, haga clic en **Compartir**.

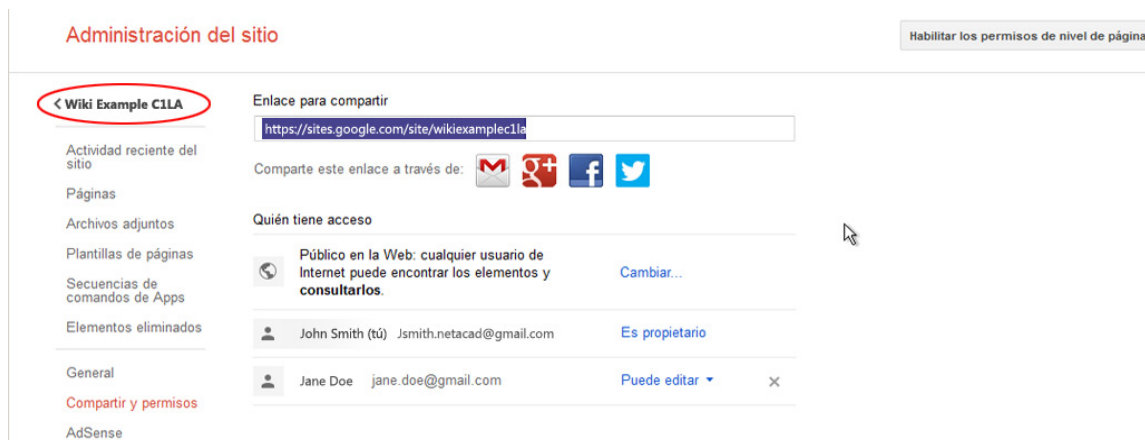


- b. Agregue un nombre, una dirección de correo electrónico o un grupo al que desee otorgarle acceso al sitio.

- c. No bien comience a introducir la información en el cuadro **Invitar a personas**, el cuadro proporcionará más opciones. El menú desplegable **Pueden editar** le permite elegir los privilegios del documento (Puede editar, Puede comentar, Puede ver) para las personas que agregue. También puede especificar cómo notificar a estas personas sobre este documento (**Enviarme una copia** o **Pegar el elemento en el correo electrónico**). Haga clic en **Compartir y guardar**.

- d. Haga clic en **Compartir y guardar** para guardar sus configuraciones de uso compartido.

- e. En la página **Administración del sitio**, aparecerán las personas que tienen acceso al sitio. Haga clic en el nombre del sitio para volver a la página de inicio.



Paso 8: Proporcionar el URL del sitio

Para proporcionar el URL del sitio nuevo, agregue el nombre del sitio al final del URL del sitio de Google, como se muestra aquí: [http://sites.google.com/site/\(nombre de sitio\)](http://sites.google.com/site/(nombre de sitio)).

Paso 9: Buscar información adicional

Para obtener una descripción general rápida de cómo funciona una wiki, visite <http://www.youtube.com/watch?v=-dnL00TdmlY>.

Entre otros ejemplos de wikis y sus sitios Web, se incluyen los siguientes:

- Wikipedia — <http://www.wikipedia.org/>
- Atlassian Confluence (una wiki empresarial popular): <http://www.atlassian.com/software/confluence/>
- Wikispaces (otra wiki gratuita): <http://www.wikispaces.com/>

Reflexión

1. ¿Conoce otras herramientas de colaboración que se utilicen en el mundo empresarial en la actualidad?

Las respuestas varían.

2. ¿Qué herramientas de colaboración considera útiles para un administrador de red?

Las respuestas varían.

Práctica de laboratorio: Investigación de servicios de redes convergentes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Evaluar su conocimiento de la convergencia

Parte 2: Investigar ISP que ofrecen servicios convergentes

Parte 3: Investigar ISP locales que ofrecen servicios convergentes

Parte 4: Seleccionar el mejor servicio convergente de un ISP local

Parte 5: Investigar compañías o instituciones públicas locales que utilicen tecnologías de convergencia

Información básica/Situación

En el contexto de redes, “convergencia” es un término que se utiliza para describir el proceso por el cual se combinan comunicaciones de voz, video y datos en una infraestructura de red común. Las redes convergentes existen hace un tiempo, pero solo fueron viables en grandes organizaciones empresariales debido a los requisitos de infraestructura de red y a la compleja administración requerida para que funcionen sin inconvenientes. Los avances tecnológicos pusieron la convergencia a disposición de las grandes, medianas y pequeñas empresas, así como del consumidor doméstico.

En la parte 1, describirá qué entiende actualmente por convergencia y toda experiencia que haya tenido con este proceso.

En la parte 2, investigará qué proveedores cuentan con este servicio (independientemente de la ubicación geográfica), para lo que utilizará el formulario predefinido que se incluye en la práctica de laboratorio.

En la parte 3, investigará qué ISP locales en su área ofrecen servicios convergentes para consumidores finales, para lo que utilizará el formulario predefinido que se incluye en la práctica de laboratorio.

En la parte 4, seleccionará el ISP que prefiere para uso doméstico e indicará los motivos.

En la parte 5, buscará una compañía o institución pública local que emplee tecnologías de convergencia en sus actividades, para lo que utilizará el formulario predefinido que se incluye en la práctica de laboratorio.

Recursos necesarios

Dispositivo con acceso a Internet

Evaluar su conocimiento de la convergencia

Nota para el instructor: en la parte 1, el instructor quizá desee facilitar un debate con los estudiantes acerca de lo que entienden por convergencia, su definición y las posibles tecnologías utilizadas. Esta práctica de laboratorio puede asignarse como tarea para el hogar.

Paso 1: Describir su comprensión de la convergencia y dar ejemplos de su uso en el hogar

Escriba una definición de convergencia e indique algunos ejemplos.

Convergencia: las redes convergentes son capaces de la entrega de voz, streams de video, texto y gráficos entre diversos tipos de dispositivos en el mismo canal de comunicación y la misma estructura de red. En una red convergente, existen muchos puntos de contacto y numerosos dispositivos especializados, como PC, teléfonos, TV y tablet PC, pero hay una infraestructura de red común. Un ejemplo de red convergente en el hogar es un servicio Triple Play de Charter.com. La voz, el video (TV) y el teléfono se empaquetan y llegan al hogar por un solo cable, comúnmente, una fibra coaxial híbrida.

Investigar ISP que ofrecen servicios convergentes

En la parte 2, investigará y encontrará dos o tres ISP que ofrezcan servicios convergentes para el hogar, independientemente de su ubicación geográfica.

Paso 2: Investigar diversos ISP que ofrezcan servicios convergentes

Enumere algunos de los ISP que encontró en la búsqueda.

Comcast

Charter

AT&T

Paso 3: Complete el siguiente formulario para los ISP seleccionados.

Proveedor de servicios de Internet (Internet Service Provider)	Nombre de producto del servicio convergente
Comcast	Xfinity Triple Play
Time Warner Cable	Televisión, Internet y teléfono
AT&T	AT&T U-verse

Investigar ISP locales que ofrezcan servicios convergentes

En la parte 3, investigará y encontrará dos o tres ISP locales que ofrecen servicios convergentes para el hogar en su área geográfica.

Paso 4: Investigar diversos ISP que ofrezcan servicios convergentes

Enumere algunos de los ISP que encontró en la búsqueda.

Las respuestas varían según la ubicación geográfica.

Paso 5: Complete el siguiente formulario para los ISP seleccionados.

Proveedor de servicios de Internet (Internet Service Provider)	Nombre de producto del servicio convergente	Costo por mes	Velocidad de descarga
Comcast	Xfinity Triple Play	\$89,99	Varía de 10 a 16 Mbps
Time Warner Cable	Televisión, Internet y teléfono	\$99,99	10 Mbps
AT&T	U-Verse	\$59.00	Descarga de 3 Mbps

Seleccionar la mejor oferta de servicio convergente de un ISP local

Elija la mejor opción de la lista de ISP locales seleccionados e indique los motivos por los cuales elige esa opción en particular.

Las respuestas varían y comúnmente se basan en el precio por mes y la prioridad relativa de las velocidades de Internet en comparación con la cantidad de canales de TV que se ofrecen en los paquetes básicos. El estudiante puede seleccionar Comcast debido a las mayores velocidades de descarga para Internet. Remarque a los estudiantes que las prioridades de los usuarios domésticos pueden afectar su elección de servicio. Por ejemplo, los usuarios que realizan exclusivamente streams de películas pueden preferir mayores velocidades de descarga, en comparación con un usuario que más que nada navega por Internet y revisa el correo electrónico de forma ocasional.

Investigar compañías o instituciones públicas locales que utilicen tecnologías de convergencia

En la parte 5, investigará y localizará una compañía en su área que actualmente utilice tecnologías de convergencia en sus negocios.

Paso 6: Investigar y buscar una compañía local que utilice la convergencia

En la tabla siguiente, indique la compañía, el sector y las tecnologías de convergencia utilizadas.

Nombre de la compañía	Sector	Tecnologías de convergencia
Cisco Systems, Inc.	Information Technology, tecnología de la información (TI)	Teléfono, video, datos
Woodward, Inc.	Aeroespacial	Teléfono, video, datos

Reflexión

1. Indique algunas de las ventajas de utilizar tecnologías de convergencia.

Combinar voz, video y señales de datos en una infraestructura de comunicación permite que las compañías administren mejor la tecnología, dado que la red utiliza un conjunto común de reglas y estándares. Ya no es necesario un equipo de distribución separado para ofrecer voz y datos.

2. Indique algunas de las desventajas de utilizar tecnologías de convergencia.

Hasta que las tecnologías alcancen una madurez completa, la configuración y la administración de voz, video y datos que fluyen en un mismo canal pueden presentar un desafío. Dar prioridad a la voz sobre los datos por medio de tecnologías de calidad de servicio (QoS) puede resultar bastante complejo para las compañías que no cuentan con personal capacitado en TI.

Práctica de laboratorio: Realización de un esquema de Internet

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Probar la conectividad de red mediante el comando ping

Parte 2: Rastrear una ruta a un servidor remoto mediante la herramienta tracert de Windows

Parte 3: Rastrear una ruta a un servidor remoto mediante herramientas de software y herramientas basadas en Web

Parte 4: Comparar los resultados de traceroute

Información básica

El software de rastreo de rutas es una utilidad que enumera las redes que atraviesan los datos desde el dispositivo final del usuario que los origina hasta una red de destino remoto.

Esta herramienta de red generalmente se ejecuta en la línea de comandos como:

```
tracert <nombre de la red de destino o dirección del terminal>
```

(sistemas Microsoft Windows)

o

```
traceroute <nombre de la red de destino o dirección del terminal>
```

(Unix y sistemas similares)

Las utilidades de rastreo de rutas permiten a un usuario determinar la trayectoria o las rutas, así como la demora a través de una red IP. Existen varias herramientas para llevar a cabo esta función.

La herramienta **traceroute** (o **tracert**) se usa generalmente para resolver problemas de redes. Al mostrar una lista de los routers atravesados, permite al usuario identificar la ruta tomada para llegar a un destino determinado de la red o a través de internetworks. Cada router representa un punto en el que una red se conecta a otra y a través del cual se envió el paquete de datos. La cantidad de routers se conoce como la cantidad de “saltos” que viajaron los datos desde el origen hasta el destino.

La lista que se muestra puede ayudar a identificar problemas de flujo de datos cuando se intenta acceder a un servicio como, por ejemplo, un sitio Web. También se puede usar para realizar tareas como descarga de datos. Si hay varios sitios Web (espejos) disponibles para el mismo archivo de datos, se puede rastrear cada espejo para darse una buena idea de qué espejo sería el más rápido para usar.

Dos rutas de rastreo entre el mismo origen y destino establecidas en diferentes momentos pueden producir distintos resultados. Esto se debe a la naturaleza “en malla” de las redes interconectadas que componen Internet y a la capacidad de los protocolos de Internet para seleccionar distintas rutas por las cuales enviar paquetes.

Por lo general, el sistema operativo del dispositivo final tiene herramientas de rastreo de rutas basadas en la línea de comandos integradas.

Otras herramientas, como VisualRoute™, son programas patentados que proporcionan información adicional. VisualRoute utiliza la información disponible en línea para mostrar la ruta gráficamente.

Esta práctica de laboratorio supone la instalación de VisualRoute. Si la computadora que utiliza no tiene VisualRoute instalado, puede descargar el programa desde el siguiente enlace:

<http://www.visualroute.com/download.html>

Si tiene problemas para descargar o instalar VisualRoute, solicite ayuda al instructor. Asegúrese de descargar la edición Lite.

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Download
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Download

Situación

Con una conexión a Internet, usará tres utilidades de rastreo de rutas para examinar la ruta de Internet hacia las redes de destino. Esta actividad debe realizarse en una PC que tenga acceso a Internet y acceso a una línea de comandos. Primero, usará la utilidad tracert integrada en Windows. En segundo lugar, utilizará una herramienta traceroute basada en la Web (<http://www.subnetonline.com/pages/network-tools/online-traceroute.php>). Finalmente, utilizará el programa traceroute de VisualRoute.

Nota para el instructor: muchos lugares de estudio no tienen acceso al símbolo del sistema. En el apéndice A, se incluyen traceroutes para utilizar. Según la situación, esta práctica de laboratorio se puede asignar para realizarse en clase o como tarea para el hogar, o bien el instructor puede realizarla como demostración explicativa.

Los programas de software gratuitos, como VisualRoute, pueden volverse obsoletos rápidamente. Si VisualRoute Lite Edition ya no está disponible cuando realiza esta práctica de laboratorio, escriba en su motor de búsqueda preferido “descargar herramienta traceroute visual”.

Algunas instituciones deshabilitan las respuestas de eco ICMP que utilizan tanto las utilidades ping como traceroute. Antes de que los estudiantes comiencen esta actividad, asegúrese de que no haya restricciones locales sobre datagramas ICMP. En esta actividad se da por sentado que los datagramas ICMP no están restringidos por ninguna política de seguridad local.

Recursos necesarios

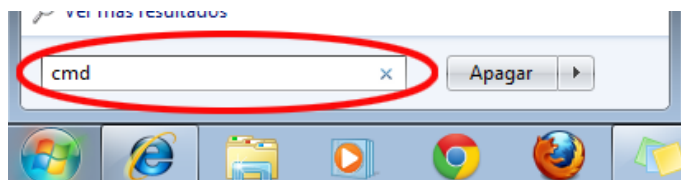
1 PC (Windows 7, Vista o XP, con acceso a Internet)

Parte 1: Probar la conectividad de red mediante el comando ping

Paso 1: Determinar si hay posibilidad de conexión al servidor remoto

Para rastrear la ruta hacia una red distante, la PC que se utiliza debe tener una conexión a Internet en funcionamiento.

- La primera herramienta que utilizaremos es ping. Ping es una herramienta que se utiliza para probar si hay posibilidad de conexión a un host. Se envían paquetes de información al host remoto con instrucciones de que responda. La PC local mide si se recibe una respuesta para cada paquete y cuánto tiempo tardan esos paquetes en atravesar la red. El nombre “ping” proviene de la tecnología de sonar activo en la cual un pulso de sonido se envía por debajo del agua y rebota en tierra o en otras embarcaciones.
- En la PC, haga clic en el ícono **Inicio de Windows**, escriba **cmd** en el cuadro de diálogo **Buscar programas y archivos** y, a continuación, presione Entrar.



- c. En el símbolo del sistema, escriba **ping www.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

- d. En la primera línea de resultados, aparece el nombre de dominio completamente calificado (FQDN) e144.dscb.akamaiedge.net. A continuación, aparece la dirección IP 23.1.48.170. Cisco aloja el mismo contenido Web en diferentes servidores en todo el mundo (conocidos como espejos). Por lo tanto, según dónde se encuentre geográficamente, el FQDN y la dirección IP serán diferentes.
- e. En cuanto a esta porción del resultado:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Se enviaron cuatro pings y se recibió una respuesta de cada ping. Como se respondió cada ping, hubo una pérdida de paquetes del 0%. En promedio, los paquetes tardaron 54 ms (milisegundos) en cruzar la red. Un milisegundo es 1/1000.^a de un segundo.

Nota para el instructor: si el primer paquete ICMP excede el tiempo de espera, eso podría deberse a que la PC intenta resolver la dirección de destino. Esto no debería ocurrir si se repite el ping, dado que ahora la dirección se encuentra en la memoria caché.

El streaming video y los juegos en línea son dos aplicaciones que se ven afectadas cuando hay pérdida de paquetes o una conexión de red lenta. Es posible determinar la velocidad de una conexión a Internet de manera más precisa al enviar 100 pings, en lugar de los cuatro predeterminados. Para ello, se debe hacer lo siguiente:

```
C:\>ping -n 100 www.cisco.com
```

Así se ve el resultado:

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

- f. Ahora, haga ping a los sitios Web de registros regionales de Internet (RIR) en distintas partes del mundo:

Para África:

```
C:\> ping www.afrinic.net
```

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Para Australia:

```
C:\> ping www.apnic.net
```

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Para Europa:

```
C:\> ping www.ripe.net
```

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Para América del Sur:

```
C:\> ping lacnic.net
```

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Todos estos pings se ejecutaron desde una PC ubicada en los EE. UU. ¿Qué sucede con el tiempo promedio de ping en milisegundos cuando los datos viajan dentro del mismo continente (América del Norte) en comparación con datos que viajan desde América del Norte hacia distintos continentes?

La respuesta varía según la ubicación. En los datos arriba mencionados, el tiempo promedio de ping en milisegundos aumenta notablemente.

¿Qué se puede destacar de los pings que se enviaron al sitio Web europeo?

En el momento en que se enviaron estos pings, el sitio estaba inaccesible.

Parte 2: Rastrear una ruta a un servidor remoto mediante la herramienta Tracert

Paso 1: Determinar qué ruta a través del tráfico de Internet llega al servidor remoto

Ahora que se verificó la posibilidad de conexión básica utilizando la herramienta ping, resulta útil observar con mayor detalle cada segmento de red que se atraviesa. Para ello, se utilizará la herramienta **tracert**.

- a. En el símbolo del sistema, escriba **tracert www.cisco.com**.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms     38 ms     37 ms     10.18.20.1
  3  37 ms     37 ms     37 ms     G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4  43 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5  43 ms     43 ms     65 ms     0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6  45 ms     45 ms     45 ms     0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7  46 ms     48 ms     46 ms     TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]
  8  45 ms     45 ms     45 ms     a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

- b. Guarde el resultado de **tracert** en un archivo de texto de la siguiente manera:
 - 1) Haga clic con el botón secundario en la barra de título de la ventana del símbolo del sistema y seleccione **Editar > Seleccionar todo**.
 - 2) Vuelva a hacer clic con el botón secundario en la barra de título del símbolo del sistema y seleccione **Editar > Copiar**.
 - 3) Abra el programa **Bloc de notas** de **Windows**: ícono **Inicio de Windows > Todos los programas > Accesorios > Bloc de notas**.
 - 4) Para pegar el resultado en el bloc de notas, seleccione **Editar > Pegar**.
 - 5) Seleccione **Archivo > Guardar como** y guarde el archivo del bloc de notas en el escritorio con el nombre **tracert1.txt**.

- c. Ejecute **tracert** para cada sitio Web de destino y guarde el resultado en archivos numerados secuencialmente.

```
C:\> tracert www.afrinic.net
```

```
C:\> tracert www.lacnic.net
```

- d. Interpretación de los resultados de **tracert**.

Las rutas rastreadas pueden atravesar muchos saltos y distintos proveedores de servicios de Internet (ISP), según el tamaño del ISP y la ubicación de los hosts de origen y destino. Cada “salto” representa un router. Un router es un tipo especializado de computadora que se utiliza para dirigir el tráfico a través de Internet. Imagine que realiza un viaje en automóvil por varios países atravesando muchas carreteras. En distintos puntos del viaje, se encuentra con una bifurcación en el camino, donde debe optar entre varias carreteras diferentes. Ahora, imagine además que hay un dispositivo en cada bifurcación del camino que lo orienta para tomar la carretera correcta hacia el destino final. Esto es lo que hace el router con los paquetes en una red.

Dado que las PC se comunican mediante números, en lugar de palabras, los routers se identifican de manera mediante direcciones IP (números con el formato x.x.x.x) exclusivas. La herramienta **tracert** muestra qué ruta toma un paquete de información a través de la red para llegar a su destino final. La herramienta **tracert** también le da una idea de la velocidad con la que avanza el tráfico en cada segmento de la red. Se envían tres paquetes a cada router en el trayecto, y el tiempo de retorno se mide en milisegundos. Ahora utilice esta información para analizar los resultados de **tracert** para www.cisco.com. El traceroute completo es el siguiente:

```
C:\>tracert www.cisco.com

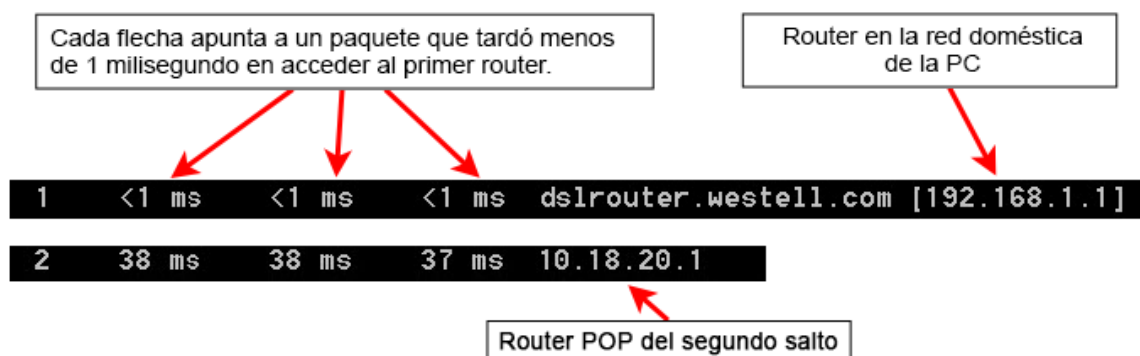
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms     38 ms     37 ms     10.18.20.1
  3  37 ms     37 ms     37 ms     G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4  43 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5  43 ms     43 ms     65 ms     0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6  45 ms     45 ms     45 ms     0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7  46 ms     48 ms     46 ms     TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8  45 ms     45 ms     45 ms     a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

A continuación, se muestra el desglose:



En el resultado de ejemplo que se muestra arriba, los paquetes de traceroute viajan desde la PC de origen hasta el gateway predeterminado del router local (salto 1: 192.168.1.1) y, desde allí, hasta el router de punto de presencia (POP) de ISP (salto 2: 10.18.20.1). Cada ISP tiene numerosos routers POP. Estos routers POP se encuentran en el extremo de la red del ISP y son los medios por los cuales los clientes se conectan a Internet. Los paquetes viajan por la red de Verizon a través de dos saltos y, luego, saltan a un router que pertenece a alter.net. Esto podría significar que los paquetes viajaron a otro ISP. Esto es importante porque a veces se produce una pérdida de paquetes en la transición entre ISP, o a veces un ISP es más lento que otro. ¿Cómo podríamos determinar si alter.net es otro ISP o el mismo?

- e. Existe una herramienta de Internet que se conoce como "whois". La herramienta whois nos permite determinar a quién pertenece un nombre de dominio. En <http://whois.domaintools.com/>, encontrará una herramienta whois basada en la Web. Según la herramienta whois basada en la Web, este dominio también pertenece a Verizon.

```
Registrant:
Verizon Business Global LLC
Verizon Business Global LLC
One Verizon Way
Basking Ridge NJ 07920
US
domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

Domain Name: alter.net
```

En resumen, el tráfico de Internet comienza en una PC doméstica y atraviesa el router doméstico (salto 1). Luego, se conecta al ISP y atraviesa la red (saltos de 2 a 7) hasta que llega al servidor remoto (salto 8). Este es un ejemplo relativamente inusual en el que solo participa un ISP desde el inicio hasta el final. Es común que haya dos o más ISP participantes, como se muestra en los ejemplos siguientes.

- f. Ahora, examine un ejemplo en el que se incluye tráfico de Internet que pasa por varios ISP. A continuación, se muestra el comando `tracert` para www.afrinic.net.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1      1 ms      <1 ms      <1 ms      dslrouter.westell.com [192.168.1.1]
  2     39 ms     38 ms     37 ms     10.18.20.1
  3     40 ms     38 ms     39 ms     G4-0-0-2204.ALBVNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4     44 ms     43 ms     43 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5     43 ms     43 ms     42 ms     0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6     43 ms     71 ms     43 ms     0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7     47 ms     47 ms     47 ms     te-7-3-0.edge2.NewYork2.Level3.net [4.68.111.137
]
  8     43 ms     55 ms     43 ms     vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9     52 ms     51 ms     51 ms     ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10    130 ms    132 ms    132 ms     ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11    139 ms    145 ms    140 ms     ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12    148 ms    140 ms    152 ms     ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13    144 ms    144 ms    146 ms     ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14    151 ms    150 ms    150 ms     ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
 15    150 ms    150 ms    150 ms     ae-58-223.csw2.London1.Level3.net [4.69.153.138]
 16    156 ms    156 ms    156 ms     ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17    157 ms    159 ms    160 ms     195.50.124.34
 18   353 ms    340 ms    341 ms     168.209.201.74
 19   333 ms    333 ms    332 ms     csw4-pk1-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms    331 ms    331 ms     196.37.155.180
 21   318 ms    316 ms    318 ms     fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms    334 ms    332 ms     196.216.2.136

Trace complete.
```

¿Qué sucede en el salto 7? ¿level3.net es el mismo ISP que el de los saltos del 2 al 6 o es un ISP diferente? Utilice la herramienta `whois` para responder esta pregunta.

El tráfico de Internet pasa de estar en alter.net a estar en level3.net. La herramienta `whois` revela que se trata de compañía o ISP diferente.

¿Qué sucede en el salto 10 con la cantidad de tiempo que le toma a un paquete viajar entre Washington D. C. y París, en comparación con los saltos anteriores (del 1 al 9)?

En los saltos del 1 al 9, la mayoría de los paquetes atraviesan su enlace en 50 ms o menos. En el enlace de Washington D. C. a París, el tiempo aumenta a 132 ms.

¿Qué sucede en el salto 18? Realice una búsqueda de `whois` para 168.209.201.74 utilizando la herramienta `whois`. ¿A quién pertenece esta red?

El tiempo para atravesar un enlace en la red aumenta de 159 a 340 ms. Debido al aumento de tiempo, probablemente el tráfico pasa a una red diferente desde la red backbone de nivel 3. Si utilizamos la herramienta whois, la dirección IP (168.209.201.74) pertenece a African Network Information Center.

- g. Escriba **tracert www.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2   38 ms   38 ms   37 ms    10.18.20.1
  3   38 ms   38 ms   39 ms    G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.81.196.190]
  4   42 ms   43 ms   42 ms    so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  5   82 ms   47 ms   47 ms    0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6   46 ms   47 ms   56 ms    204.255.168.194
  7  157 ms   158 ms   157 ms    ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8  156 ms   157 ms   157 ms    xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9  161 ms   161 ms   161 ms    xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10  158 ms   157 ms   157 ms    ae0-0.ar3.nu.registro.br [200.160.0.249]
 11  176 ms   176 ms   170 ms    gw02.lacnic.registro.br [200.160.0.213]
 12  158 ms   158 ms   158 ms    200.3.12.36
 13  157 ms   158 ms   157 ms    200.3.14.147

Trace complete.
```

¿Qué sucede en el salto 7?

El tiempo que le toma a un paquete atravesar la red aumenta notablemente, más de cuatro veces, de ~40 a ~180 ms. ¿Los estudiantes realizaron una búsqueda de whois de registro.br con la herramienta whois basada en la Web: <http://whois.domaintools.com/>? Si lo hicieron, la información que recibieron no fue tan útil. ¿Los estudiantes accedieron a <http://translate.google.com/> para obtener una traducción de Núcleo de Informação e Coordenação do Ponto? Hubiera sido más útil realizar una solicitud de “top domain.br” en un motor de búsqueda, lo que habría revelado que estábamos en una red brasileña. El trabajo detectivesco por Internet puede ser divertido.

Parte 3: Rastrear una ruta a un servidor remoto mediante herramientas de software y herramientas basadas en Web

Paso 1: Utilizar una herramienta traceroute basada en la Web

- a. Utilice <http://www.subnetonline.com/pages/network-tools/online-tracepath.php> para rastrear la ruta a los siguientes sitios Web:

www.cisco.com

www.afrinic.net

Capture y guarde el resultado en el bloc de notas.

www.cisco.com:

TracePath Output:

1:	pera.subnetonline.com (141.138.203.105)	0.157ms	pmtu 1500
1:	gw-v130.xl-is.net (141.138.203.1)	1.168ms	
2:	rt-eu01-v2.xl-is.net (79.170.92.19)	0.566ms	
3:	akamai.telecity4.nl-ix.net (193.239.116.226)	1.196ms	

www.afrinic.com:

TracePath Output:

1:	pera.subnetonline.com (141.138.203.105)	0.175ms	pmtu 1500
1:	gw-v130.xl-is.net (141.138.203.1)	0.920ms	
2:	rt-eu01-v2.xl-is.net (79.170.92.19)	0.556ms	
3:	xl-internetservices.nikhef.openpeering.nl (217.170.0.225)	10.679ms	
4:	r22.amstnl02.nl.bb.gin.ntt.net (195.69.144.36)	asymm 5	4.412ms
5:	ae-5.r23.londen03.uk.bb.gin.ntt.net (129.250.5.197)	49.349ms	
6:	ae-2.r02.londen03.uk.bb.gin.ntt.net (129.250.5.41)	asymm 7	8.842ms
7:	dimensiondata-0.r02.londen03.uk.bb.gin.ntt.net (83.231.235.222)	18.080ms	
8:	168.209.201.74 (168.209.201.74)	196.375ms	
9:	csw4-pkl-gil-1.ip.isnet.net (196.26.0.101)	asymm 10	186.855ms
10:	196.37.155.180 (196.37.155.180)	185.661ms	
11:	fa1-0-1.ar02.jnb.afrinic.net (196.216.3.132)	197.912ms	

¿En qué se diferencia el comando traceroute cuando se accede a www.cisco.com desde el símbolo del sistema (consulte la parte 1) en lugar de hacerlo desde el sitio Web en línea? (Los resultados pueden variar dependiendo de dónde se encuentre geográficamente y de qué ISP proporcione conectividad al lugar de estudios).

El comando tracert ejecutado desde el símbolo del sistema en la parte 1 terminó en un servidor en Cambridge, Massachusetts. El comando traceroute ejecutado desde el sitio Web en los Países Bajos llegó a un servidor reflejado en los Países Bajos. El dominio cisco.com se aloja en numerosos sitios Web o sitios reflejados por todo el mundo. Esto se hace para que el tiempo de acceso al sitio sea rápido desde cualquier lugar del mundo.

Compare el comando tracert de la parte 1 que va a África con el comando tracert que va a África desde la interfaz Web. ¿Qué diferencia advierte?

La ruta a través de Europa pasa por otro ISP. Plantee a los estudiantes que no existe un solo backbone para Internet, sino que son muchos. Todos se conectan a los puntos de interconexión. El rendimiento en la red en un ISP podría ser muy diferente al rendimiento en la red con otro ISP.

Algunos de los traceroutes contienen la abreviatura asymm. ¿Tiene alguna idea de a qué se refiere? ¿Qué significa?

Es una abreviatura de “asymmetric” (asimétrico). Significa que el paquete de prueba tomó una ruta para llegar al destino y una ruta diferente para volver. Imagine a una persona que conduce desde su casa hacia la ciudad de Nueva York. En el camino a esa ciudad, nota que la carretera está congestionada y que el tráfico avanza lento. Podría decidir volver a casa por una ruta diferente (o asimétrica).

Paso 2: Usar VisualRoute Lite Edition

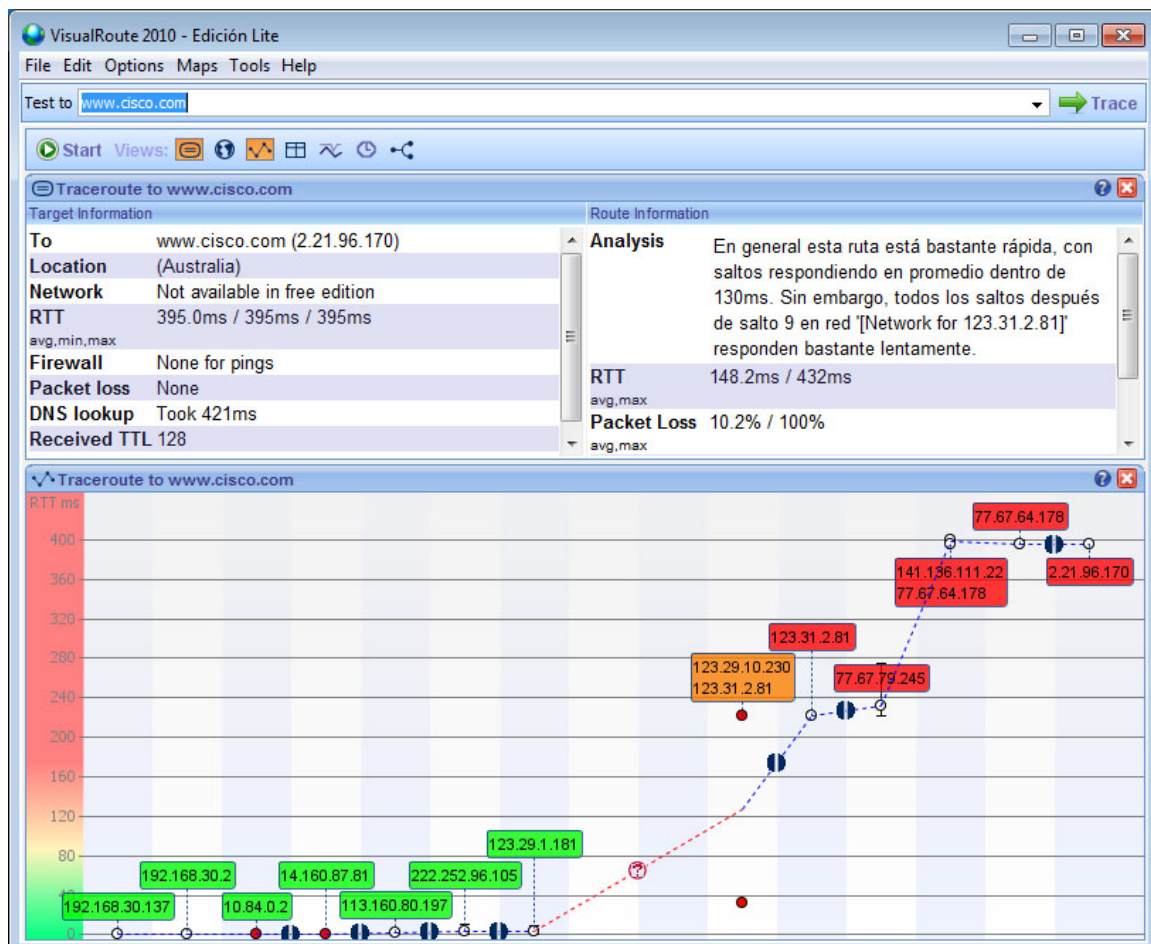
VisualRoute es un programa traceroute patentado que puede mostrar gráficamente los resultados de la ruta de rastreo.

- a. Si VisualRoute Lite Edition no está instalado, descárguelo del enlace siguiente:

<http://www.visualroute.com/download.html>

Si tiene problemas para descargar o instalar VisualRoute, solicite ayuda al instructor. Asegúrese de descargar la edición Lite.

- b. Rastree las rutas a www.cisco.com utilizando VisualRoute 2010 Lite Edition.
c. Registre las direcciones IP del trayecto en el bloc de notas.



Parte 4: Comparar los resultados de traceroute

Compare los resultados de traceroute para www.cisco.com de las partes 2 y 3.

Paso 1: Indique la ruta a www.cisco.com que se obtiene al utilizar el comando `tracert`.

```
192.168.1.1 > 10.18.20.1 > 130.81.196.190 > 130.81.22.46 > 152.63.1.57 > 152.63.17.109 > 152.63.21.14 > 23.1.144.170
```

Paso 2: Indique la ruta a www.cisco.com que se obtiene al utilizar la herramienta basada en la Web que se encuentra en subnetonline.com.

```
141.138.203.105 > 141.138.203.1 > 79.170.92.19 > 19.239.116.226
```

Paso 3: Indique la ruta a www.cisco.com que se obtiene al utilizar VisualRoute Lite Edition.

```
192.168.1.17 > 192.168.1.1 > 10.18.20.1 130.81.196.188 > 130.81.151.1 130.81.22.46 > 152.63.9.249 > 152.63.17.109 > 152.63.21.14 > 231.144.170
```

¿Todas las utilidades de traceroute usaron las mismas rutas para llegar a www.cisco.com? ¿Por qué o por qué no?

Las rutas de rastreo entre el mismo origen y destino establecidas en diferentes momentos pueden producir distintos resultados. Esto se debe a la naturaleza “en malla” de las redes interconectadas que componen Internet y a la capacidad de los protocolos de Internet para seleccionar distintas rutas por las cuales enviar paquetes.

Reflexión

Ahora que se analizó traceroute mediante tres herramientas diferentes (tracert, interfaz Web y VisualRoute), ¿VisualRoute proporciona algún detalle que las otras dos herramientas no ofrezcan?

Las respuestas varían. Un detalle posible es que VisualRoute resalta gráficamente la cantidad de tiempo que toma viajar entre los saltos en Internet. Al resaltar en amarillo y en rojo los tiempos más lentos, se ve más claramente que hay problemas de red a lo largo de estos enlaces.

Apéndice A

```
C:\> tracert www.cisco.com
```

```
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	38 ms	38 ms	37 ms	10.18.20.1
3	37 ms	37 ms	37 ms	G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.196.190]
4	43 ms	43 ms	42 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	43 ms	43 ms	65 ms	0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
6	45 ms	45 ms	45 ms	0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
7	46 ms	48 ms	46 ms	TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]
8	45 ms	45 ms	45 ms	a23-1-144-170.deploy.akamaitechnologies.com [23.1.144.170]

```
Trace complete.
```

```
C:\> tracert www.afrinic.net
```

```
Tracing route to www.afrinic.net [196.216.2.136]  
over a maximum of 30 hops:
```

1	1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	39 ms	38 ms	37 ms	10.18.20.1
3	40 ms	38 ms	39 ms	G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.197.182]
4	44 ms	43 ms	43 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	43 ms	43 ms	42 ms	0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
6	43 ms	71 ms	43 ms	0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
7	47 ms	47 ms	47 ms	te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137]
8	43 ms	55 ms	43 ms	vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
9	52 ms	51 ms	51 ms	ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]
10	130 ms	132 ms	132 ms	ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
11	139 ms	145 ms	140 ms	ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.137]
12	148 ms	140 ms	152 ms	ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14]
13	144 ms	144 ms	146 ms	ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29]
14	151 ms	150 ms	150 ms	ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
15	150 ms	150 ms	150 ms	ae-58-223.csw2.London1.Level3.net [4.69.153.138]
16	156 ms	156 ms	156 ms	ae-227-3603.edge3.London1.Level3.net [4.69.166.154]
17	157 ms	159 ms	160 ms	195.50.124.34
18	353 ms	340 ms	341 ms	168.209.201.74
19	333 ms	333 ms	332 ms	csw4-pkl-gil-1.ip.isnet.net [196.26.0.101]
20	331 ms	331 ms	331 ms	196.37.155.180
21	318 ms	316 ms	318 ms	fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
22	332 ms	334 ms	332 ms	196.216.2.136

```
Trace complete.
```

```
C:\> tracert www.lacnic.net
```

```
Tracing route to lacnic.net [200.3.14.10]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	38 ms	37 ms	37 ms	10.18.20.1
3	37 ms	38 ms	40 ms	G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.196.190]
4	43 ms	42 ms	43 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	46 ms	75 ms	46 ms	0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
6	43 ms	43 ms	43 ms	204.255.168.194
7	178 ms	182 ms	178 ms	ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
8	172 ms	180 ms	182 ms	xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

Práctica de laboratorio: Realización de un esquema de Internet

```
9    177 ms    172 ms    181 ms    xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]
```

```
10   173 ms    180 ms    176 ms    ae0-0.ar3.nu.registro.br [200.160.0.249]
```

```
11   184 ms    183 ms    180 ms    gw02.lacnic.registro.br [200.160.0.213]
```

```
12   180 ms    179 ms    180 ms    200.3.12.36
```

```
13   182 ms    180 ms    180 ms    www.lacnic.net [200.3.14.10]
```

```
Trace complete.
```

Práctica de laboratorio: Investigación de oportunidades laborales de TI y redes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Investigar oportunidades laborales

- Identificar las oportunidades de laborales de redes actuales que tienen demanda.
- Explicar el valor de las certificaciones de Cisco en el mercado laboral.

Parte 2: Reflexionar sobre la investigación

- Identificar las tendencias de contratación actuales en TI y redes.
- Identificar las certificaciones y aptitudes profesionales futuras sobre redes.
- Identificar trayectorias profesionales adicionales sobre redes.

Información básica/Situación

Los empleos en el área de tecnología de la información (TI) y redes de computadoras continúan creciendo. La mayoría de los empleadores requieren cierta forma de certificación estándar del sector, título u otras calificaciones de sus posibles empleados, en particular de aquellos que cuentan con limitada experiencia. La certificación Cisco CCNA es una certificación de nivel inicial conocida y establecida sobre redes, respetada en el sector. Existen más niveles y tipos de certificaciones de Cisco que se pueden obtener, y cada una de ellas puede mejorar las oportunidades laborales, así como la escala salarial.

En esta práctica de laboratorio, realizará cierta búsqueda laboral orientada en la Web, para descubrir qué tipos de empleos relacionados con TI y redes de computadoras se encuentran disponibles, qué tipo de aptitudes y certificaciones necesitará y las escalas salariales asociadas con los diversos puestos.

Recursos necesarios

- Dispositivo con acceso a Internet

Parte 1: Buscar oportunidades laborales

En la parte 1, utilizará un explorador Web para visitar los sitios Web conocidos de bolsas de trabajo monster.com y salary.com.

Paso 1: Abrir un explorador Web y acceder a un sitio Web de bolsa de trabajo

En la barra de direcciones URL, escriba <http://monster.com> y presione Entrar.

Nota: para acceder a bolsas de trabajo fuera de los EE. UU., utilice el siguiente enlace para hacer búsquedas en su país:

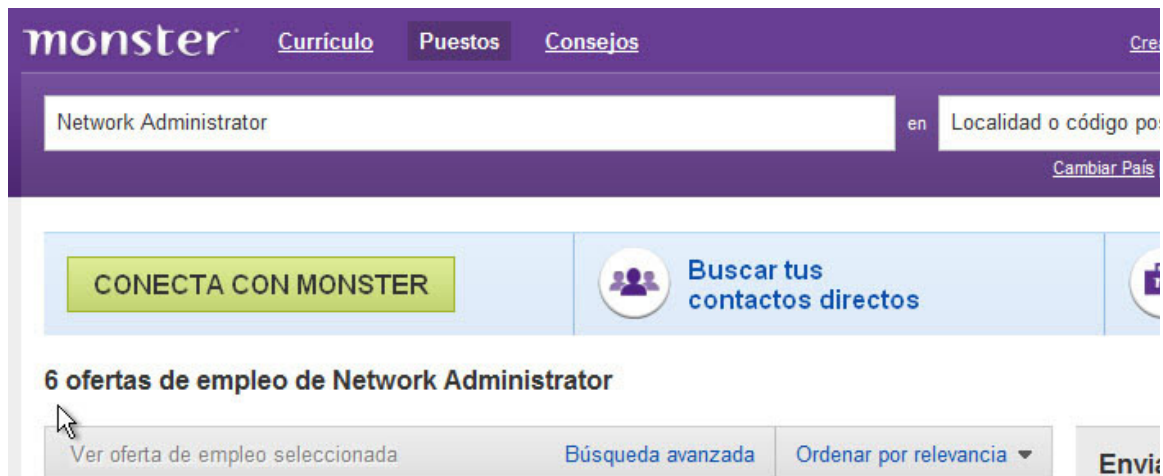
<http://www.monster.com/geo/siteselection/>

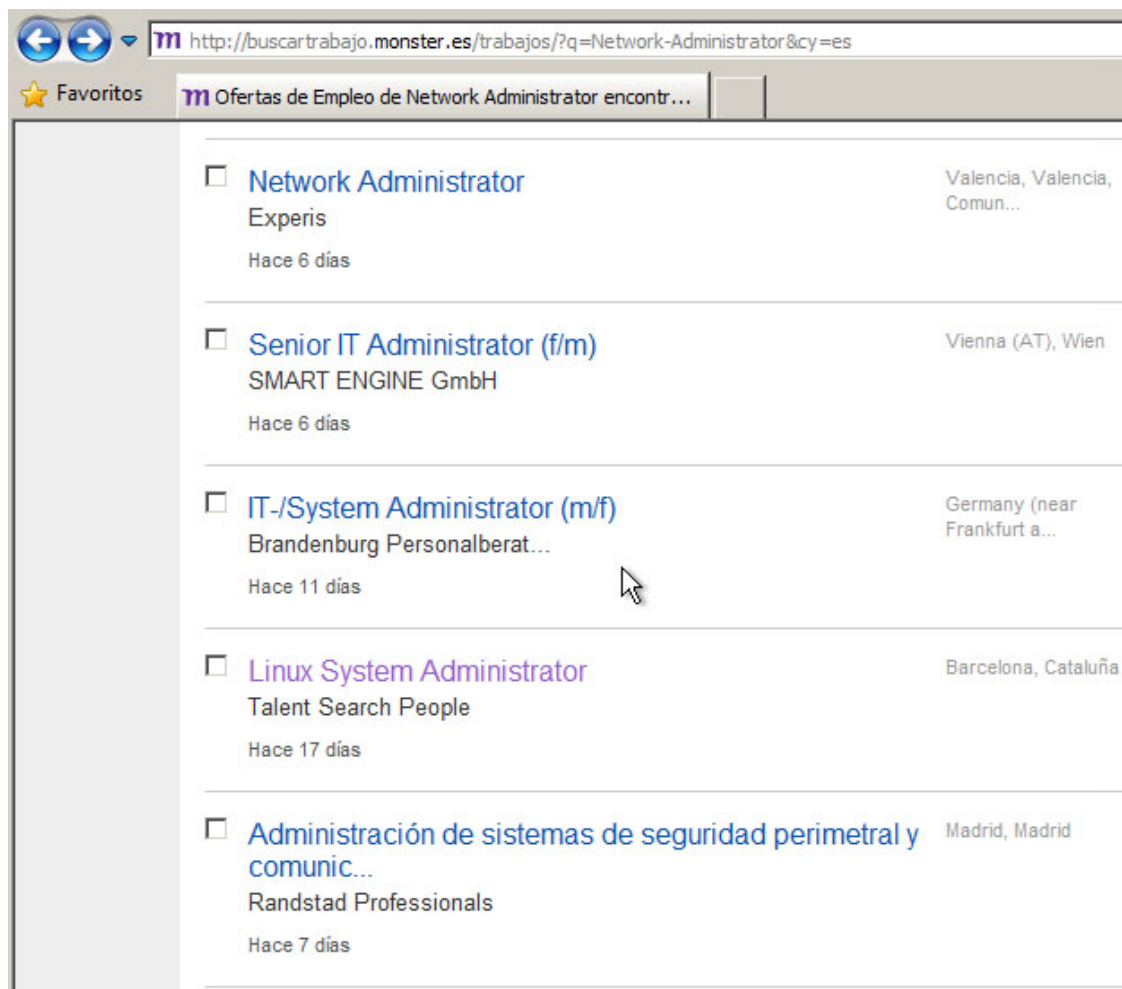
Paso 2: Buscar trabajos relacionados con redes

- a. Escriba la palabra *Network* en el cuadro Puesto. Observe que el sitio Web ofrece sugerencias sensibles al contexto en función de las palabras clave proporcionadas. Haga clic o termine de escribir las palabras *Network Administrator* (Administrador de red) y haga clic en el botón **BUSCAR** (consulte la imagen siguiente).



- b. Observe los resultados de la búsqueda:





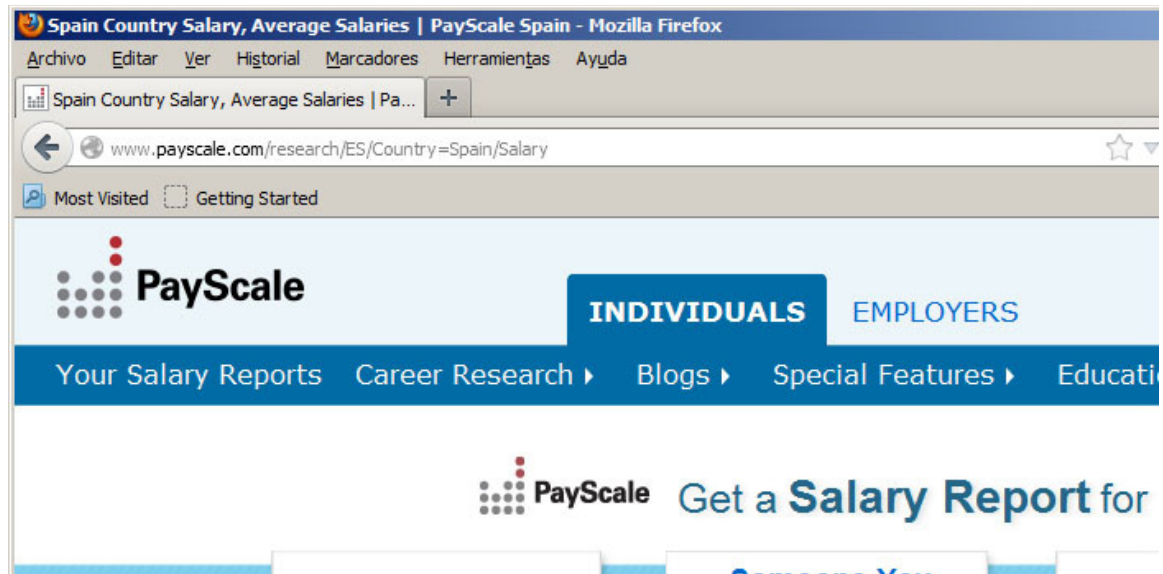
- c. Ahora enfoque la búsqueda agregando términos en el cuadro del campo de palabras clave. Pruebe con términos como Cisco CCNA, CCNP, CCNA Security, CCNA Voice, etc.
- d. Ahora intente refinar la búsqueda agregando ubicaciones geográficas diferentes. ¿Encontró empleos en las ubicaciones que introdujo?

Las respuestas varían.

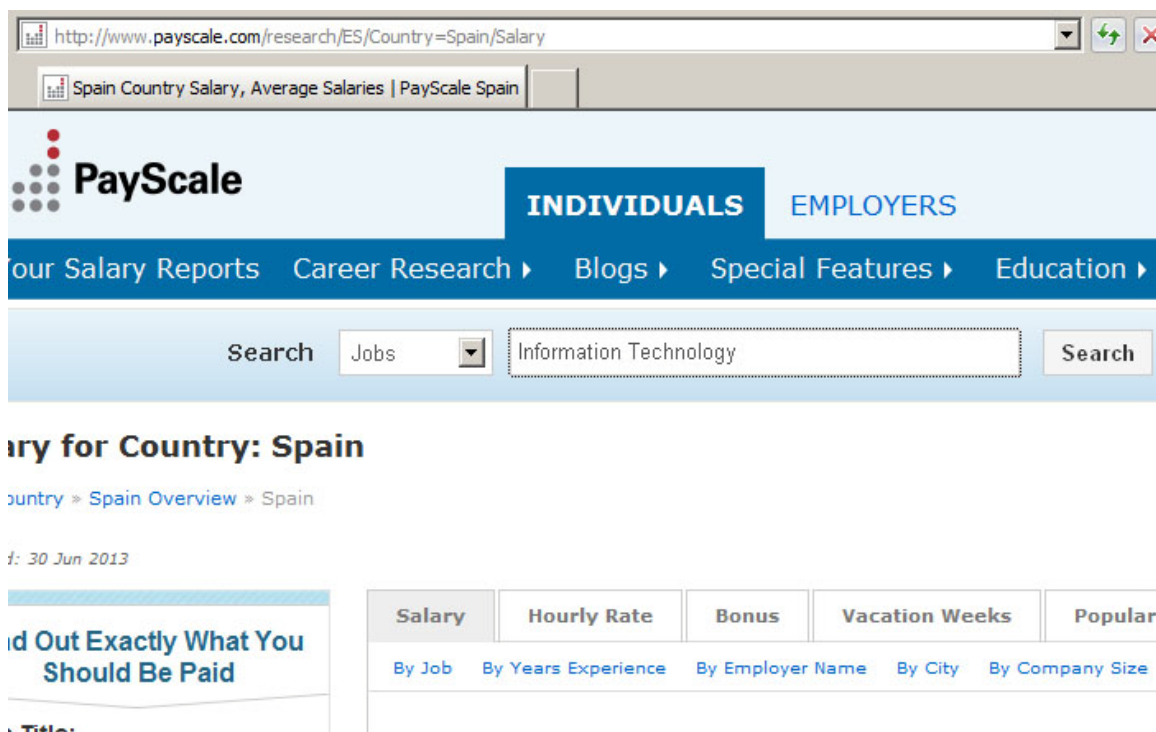
- e. Intente buscar en un sitio Web diferente. Acceda a <http://salary.com> y haga clic en el botón de la barra de menús **Job Search** (Búsqueda laboral).

Nota: para obtener escalas salariales fuera de los EE. UU., utilice el siguiente enlace para hacer búsquedas en su país:

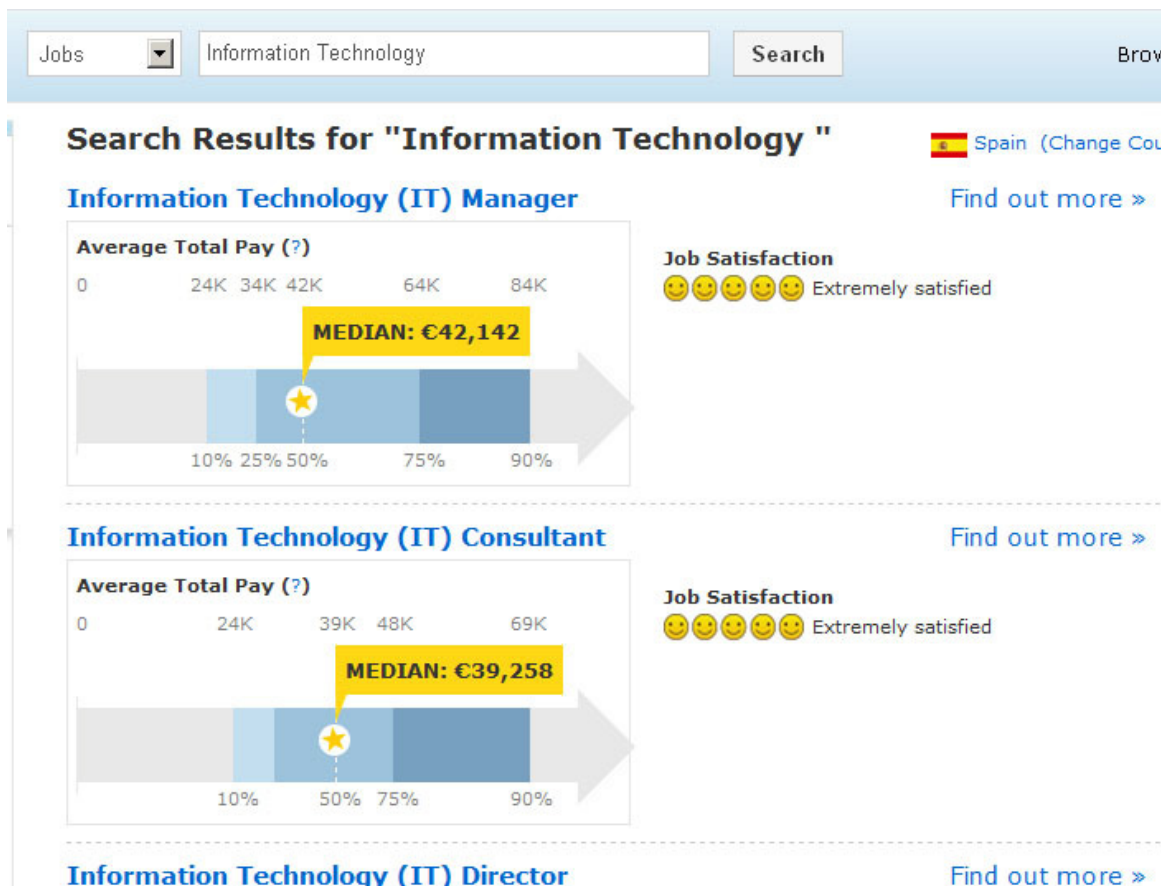
<http://www.payscale.com/rccountries.aspx>



- f. Ahora, agregue un término de búsqueda como *Information Technology* (Tecnología de la información) en el cuadro del campo Job Title (Puesto) y haga clic en **Submit** (Enviar).



- g. En la imagen siguiente, observe la gran cantidad de resultados coincidentes de la búsqueda. También existen herramientas fáciles de usar para refinar la búsqueda, en la columna de la izquierda.



- h. Dedique cierto tiempo a buscar empleos y observar los resultados de las búsquedas. Tome nota de las aptitudes requeridas para los distintos puestos y de la escala salarial inicial.

Parte 2: Reflexionar sobre la investigación

En la parte 2, responderá preguntas sobre la base de las conclusiones de la investigación realizada.

- a. ¿Qué puestos buscó?

- b. ¿Qué aptitudes o certificaciones se requerían?

- c. ¿Encontró empleos que anteriormente no sabía que existían? Si la respuesta es afirmativa, ¿cuáles fueron?

- d. ¿Encontró empleos que le interesan? Si la respuesta es afirmativa, ¿cuáles son y qué aptitudes o certificaciones requieren?

Dibuje su concepto actual de Internet (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Identificar los componentes comunes de una red.

- Los estudiantes ilustrarán la forma en que se aplican los conceptos del capítulo 1 para mostrar cómo se conectan los dispositivos de red a Internet y a través de Internet. Después de reflexionar sobre la topología para el hogar o para pequeñas empresas, los estudiantes se familiarizarán con el uso de los íconos de los dispositivos y con el conocimiento necesario para visualizar la conectividad de red mediante los cursos de red restantes.

Información básica/Situación

En esta actividad, utilizará el conocimiento que adquirió en el capítulo 1 y el documento de la actividad de creación de modelos que preparó al comienzo de este capítulo. También puede consultar las otras actividades realizadas en este capítulo, incluidas las actividades de Packet Tracer.

Dibuje un esquema de Internet como la ve ahora. Utilice los íconos presentados en el capítulo de medios, dispositivos finales y dispositivos intermediarios.

En el dibujo revisado, tal vez desee incluir alguno de los siguientes elementos:

- WAN
- LAN
- Computación en la nube
- Proveedores de servicios de Internet (niveles)

Conserve el dibujo en formato impreso. Si se trata de un documento electrónico, guárdelo en una ubicación del servidor proporcionada por el instructor. Esté preparado para compartir y explicar su trabajo revisado en clase.

Nota para el instructor: esta actividad de creación de modelos puede utilizarse como asignación con calificación, ya que su propósito es validar el conocimiento adquirido en el capítulo 1 sobre lo siguiente:

- WAN
- LAN
- Computación en la nube
- Proveedores de servicios de Internet (niveles)

Recursos necesarios

- Dibujo de la actividad de creación de modelos del comienzo del capítulo
- Packet Tracer (puede ser optativo si los estudiantes bosquejan su propio dibujo)
- Papel y lápices o lapiceras

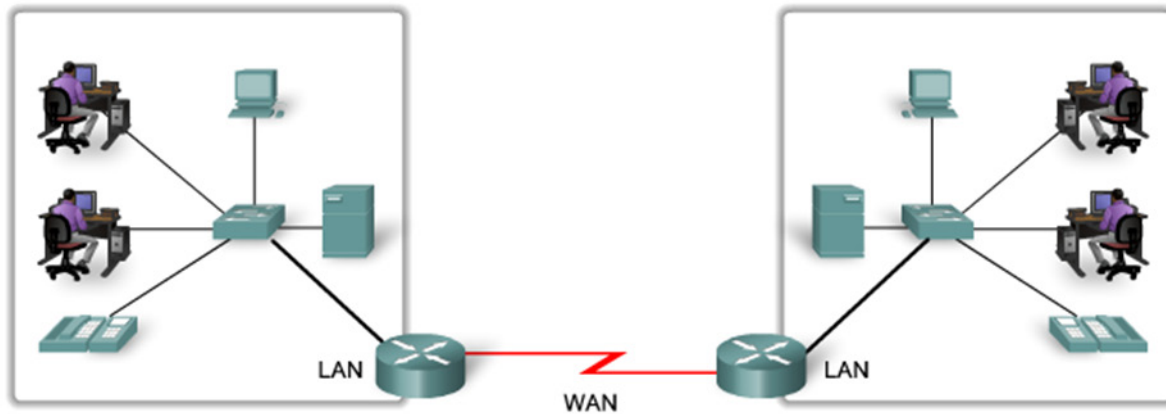
Reflexión

1. Después de completar el capítulo 1, ¿tiene más conocimiento de los dispositivos, el cableado y los componentes físicos de una red pequeña o mediana? Justifique su respuesta.

Dibuje su concepto actual de Internet

(Las respuestas varían por alumno, pero esta pregunta de reflexión generará cierto debate favorable en la clase y promoverá la comunidad entre los estudiantes y el instructor).

Representación gráfica de la actividad de creación de modelos (los diseños varían)



Nota para el instructor: este es un modelo representativo que podría “crearse” como resultado de esta actividad.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Dispositivos/equipo
- Medios (cableado)
- Enlaces de medios sociales
- Orígenes y destinos
- Redes de área local
- Redes de área amplia

Es solo un sistema operativo

(Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Describir la estructura de comandos del software Cisco IOS.

- Los estudiantes reconocerán que los comandos de texto que se utilizan en las interfaces de línea de comandos se eligen intencionalmente del idioma hablado. A menudo, los comandos de texto se abrevian, o su sintaxis se simplifica de alguna manera, con el fin de mantener el conjunto de comandos resultante conciso. Además, los comandos se pueden agrupar en modos de contexto que simplifican su uso. Configurar un dispositivo mediante comandos escritos es similar a impartir órdenes breves en forma oral. El sistema operativo ejecuta los comandos, y el dispositivo lleva a cabo el proceso propiamente dicho.

Información básica/Situación

Imagine que ingresa como ingeniero a una compañía que fabrica automóviles. Actualmente, la compañía trabaja en un nuevo modelo de automóvil. Este modelo tendrá ciertas funciones que el conductor podrá controlar mediante comandos de voz específicos.

Debe diseñar el conjunto de comandos que utiliza ese sistema de control activado por voz.

Las funciones del automóvil que se pueden controlar mediante comandos de voz son las siguientes:

- Luces
- Limpiaparabrisas
- Radio
- Equipo de teléfono
- Aire acondicionado
- Encendido

Su tarea consiste en idear un conjunto simple de comandos orales que se usarán para controlar estos sistemas e identificar cómo deben ejecutarse.

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. Su objetivo es ayudar a los estudiantes a reflexionar sobre sus percepciones sobre la manera en que se configura una red por medio del uso de comandos de voz (similar a la estructura de comandos del IOS). La facilitación del debate debe incluir conversaciones entre los estudiantes sobre el trabajo de cada uno.

Recursos necesarios

- Papel y lápices o bolígrafos, o PC

Reflexión

1. ¿De qué manera puede ayudar a operar un vehículo la creación de conjunto de comandos de voz? ¿Cómo podrían usarse esos mismos comandos en una PC o en un sistema operativo de red?

Algunas respuestas sugeridas para el debate incluyen:

- Mencione que las opciones utilizadas para formar un conjunto de palabras habladas constituirá el conjunto de comandos. Una opción obvia es utilizar palabras simples en español como el conjunto de comandos. Otras opciones incluyen palabras en distintos idiomas, utilizar números de comando o atajos. Sin embargo, debe tenerse en cuenta que esto haría que los conjuntos de comandos fueran significativamente menos intuitivos.
- Hable acerca de las opciones de los estudiantes para crear un conjunto de comandos directo, sin jerarquía, o de agrupar los comandos según su función. Resalte el hecho de que, por ejemplo, un comando de ayuda sin más contexto no sería útil, porque no indica para qué necesita ayuda exactamente el usuario. Hay dos maneras de proporcionar contexto a un comando:
- Pregunte a los estudiantes si expresaron el contexto en forma explícita con cada comando (por ejemplo, subir el volumen de la radio/bajar el volumen de la radio; subir el volumen del teléfono/bajar el volumen del teléfono), que constituye el enfoque llano directo, o pregunte si introdujeron modos (agrupaciones de comandos que se refieren a un contexto determinado y que, una vez colocados en ese contexto, no tuvieron que volver a remarcarse). Por ejemplo, después de enmarcar la instrucción en el modo de radio, los comandos subir volumen y bajar volumen no son ambiguos.
- Analice las ventajas de ambos enfoques. Para un pequeño grupo de comandos, el enfoque directo es más conveniente. Para un conjunto de comandos más grande, que posiblemente pueda ampliarse a frases largas y con muchas palabras, es preferible utilizar modos, dado que contribuye a mantener el conjunto de comandos organizado y limita la longitud de los comandos individuales.
- ¿Cómo decidieron los estudiantes la forma en que se iniciaría el reconocimiento de comandos de voz a fin de que el automóvil no interpretara erróneamente una conversación ocasional de los pasajeros como comandos? Las posibilidades incluyen decir una palabra específica, por lo demás no utilizada, o presionar un botón en el volante. Además, analice la forma en que los estudiantes manejaron un sistema que debería solicitar al usuario que introduzca comandos de voz y cómo se informaría al usuario que el comando hablado no se entendió correctamente o no es válido.
- ¿Cómo manejaron los estudiantes el acceso a comandos más importantes desde el punto de vista de la seguridad, como luces y encendido? ¿Cómo se protegieron o aislaron esos comandos para evitar que se produjera una manipulación inadvertida? Las posibilidades incluyen decir una palabra específica, por lo demás no utilizada, o presionar un botón en el volante.
- Solicite a los estudiantes que discutan acerca de qué parte del software de la computadora incorporada del automóvil procesaría los comandos de voz y qué software específico ejecutaría los comandos. El software que realiza el reconocimiento de voz y traduce los comandos de voz en una forma que la computadora puede entender es la interfaz de comandos que se utiliza para interactuar con el vehículo. Sin embargo, los comandos deben ser procesados por el software operativo central del automóvil, que controla todas sus funciones y organiza todos sus sistemas. Como ejemplo, decir “encender motor” incluye el procesamiento del comando de voz en la interfaz de comandos; luego, el sistema operativo procesa ese comando por medio de la activación del motor de arranque durante un lapso determinado, la habilitación del flujo de combustible, la coordinación de varios sistemas del automóvil vehículo para hacer que funcione, etcétera.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Los distintos sistemas del automóvil que pueden controlarse mediante comandos de voz se relacionan con diferentes componentes de los routers y switches que pueden configurarse.
- Los comandos de voz se relacionan con los comandos del IOS.
- La elección de palabras o frases cortas en español como conjunto de comandos se relaciona con el estilo general de la CLI del IOS.
- La organización del conjunto de comandos de voz en modos se relaciona con la CLI del IOS, organizada en modos.

- Iniciar el proceso de reconocimiento de voz se relaciona con iniciar una sesión de la CLI en modo EXEC presionando la tecla Entrar. Además, las peticiones de voz del automóvil se relacionan con las peticiones de la línea de comandos.
- Los comandos potencialmente perjudiciales, como apagar luces o encender motor, se relacionan con los comandos potencialmente perjudiciales del IOS (reload [recargar], erase flash: [borrar memoria flash] o delete startup-config [eliminar configuración de arranque]).
- La interfaz de voz y el sistema operativo del automóvil se relacionan con el modo EXEC del IOS (el intérprete de comandos) y el IOS propiamente dicho.

Práctica de laboratorio: Establecimiento de una sesión de consola con Tera Term (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Acceder a un switch Cisco a través del puerto serie de consola

- Conectarse a un switch Cisco mediante un cable serial de consola.
- Establecer una sesión de consola utilizando un emulador de terminal, como Tera Term.

Parte 2: Mostrar y configurar parámetros básicos de los dispositivos

- Utilizar los comandos **show** para mostrar la configuración del dispositivo.
- Configurar el reloj del switch

Parte 3: Acceder a un router Cisco mediante un cable de consola mini-USB (optativo)

Nota: los usuarios en Netlab o en otro equipo de acceso remoto deben completar solo la parte 2.

Nota para el instructor: los cables de consola y los cables de consola mini-USB ya no se envían de forma predeterminada con los nuevos routers ISR G2, como Cisco 1941, Cisco 2901 o Cisco 2911. Estos cables de consola pueden adquirirse a través de Cisco Systems, Inc. o de otros proveedores externos.

Información básica/Situación

Se utiliza una variedad de modelos de switches y routers Cisco en redes de todo tipo. Estos dispositivos se administran mediante una conexión de consola local o una conexión remota. Casi todos los dispositivos Cisco tienen un puerto serie de consola al que el usuario puede conectarse. Algunos modelos más nuevos, como el router de servicios integrados (ISR) 1941 G2, que se utiliza en esta práctica de laboratorio, también tienen un puerto de consola USB.

En esta práctica de laboratorio, aprenderá cómo acceder a un dispositivo Cisco a través de una conexión local directa al puerto de consola mediante un programa de emulación de terminal (Tera Term). También aprenderá a configurar los parámetros del puerto serie para la conexión de consola de Tera Term. Después de establecer una conexión de la consola con el dispositivo Cisco, puede ver o modificar la configuración del dispositivo. En esta práctica de laboratorio, solo mostrará los parámetros y configurará el reloj.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son ISR Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el switch y el router se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cable de consola (DB-9 a RJ-45) para configurar el switch o el router a través del puerto de consola RJ-45
- Cable mini-USB para configurar el router a través del puerto de consola USB

Nota para el instructor: si no está instalado en la PC, Tera Term se puede descargar del siguiente enlace seleccionando **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

Nota para el instructor: en PC con Microsoft Windows conectadas a un dispositivo Cisco IOS con un cable USB, se debe instalar un controlador USB antes de su uso. El controlador se puede encontrar en www.cisco.com con el dispositivo Cisco IOS relacionado. El controlador USB se puede descargar en el siguiente enlace:

<http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

Nota para el instructor: para descargar el archivo del controlador USB, debe tener una cuenta válida de Cisco Connection Online (CCO).

Parte 1: Acceder a un switch Cisco a través del puerto serie de consola

Conectará una PC a un switch Cisco mediante un cable de consola. Esta conexión le permitirá acceder a la interfaz de línea de comandos (CLI) y mostrar los parámetros o configurar el switch.

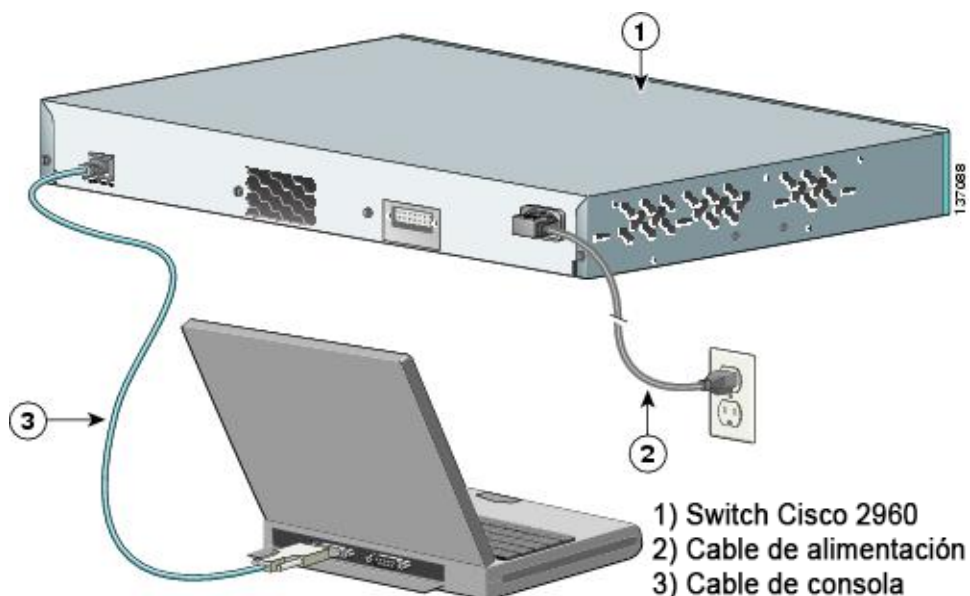
Paso 1: Conectar un switch Cisco y una PC mediante un cable de consola

- a. Conecte el cable de consola al puerto de consola RJ-45 del switch.
- b. Conecte el otro extremo del cable al puerto serie COM de la PC.

Nota: la mayoría de las PC actuales no tienen puertos serie COM. Se puede utilizar un adaptador de USB a DB9 con el cable de consola para realizar la conexión de consola entre la PC y un dispositivo Cisco. Estos adaptadores de USB a DB9 pueden adquirirse en cualquier tienda de electrónica informática.

Nota: si utiliza un adaptador de USB a DB9 para conectar el puerto COM, puede ser necesario instalar un controlador para el adaptador proporcionado por el fabricante de la PC. Para determinar el puerto COM que utiliza el adaptador, consulte el paso 4 de la parte 3. Se requiere el número de puerto COM correcto para conectar el dispositivo Cisco IOS por medio de un emulador de terminal en el paso 2.

- c. Si aún no están encendidos, encienda el switch Cisco y la PC.



Paso 2: Configurar Tera Term para establecer una sesión de consola con el switch

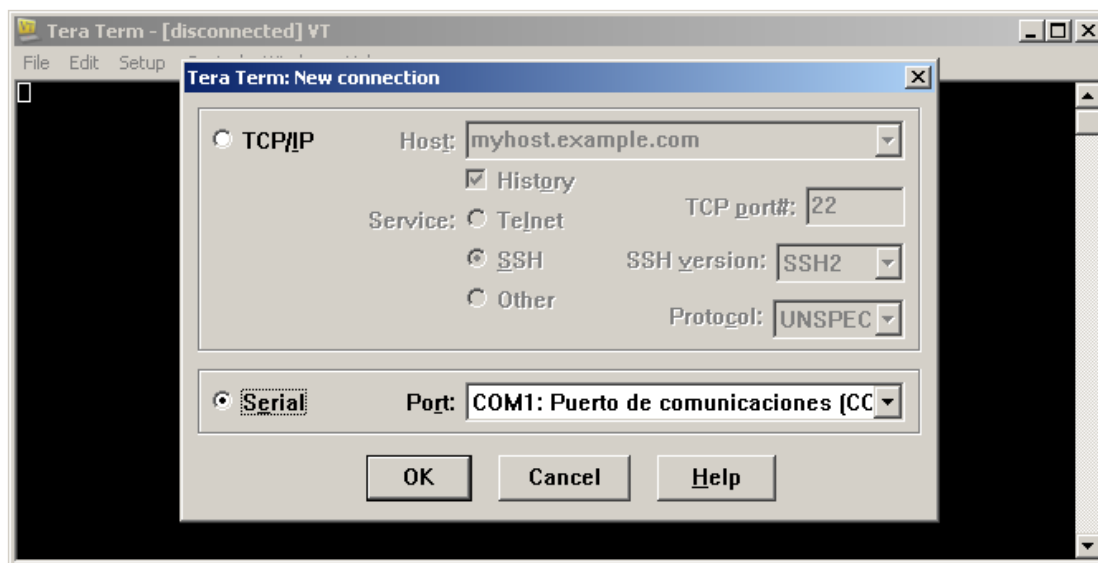
Tera Term es un programa de emulación de terminal. Este programa le permite acceder al resultado para la terminal del switch y también le permite configurar el switch.

- a. Inicie Tera Term haciendo clic en el botón **Inicio de Windows**, situado en la barra de tareas. Localice **Tera Term** en **Todos los programas**.

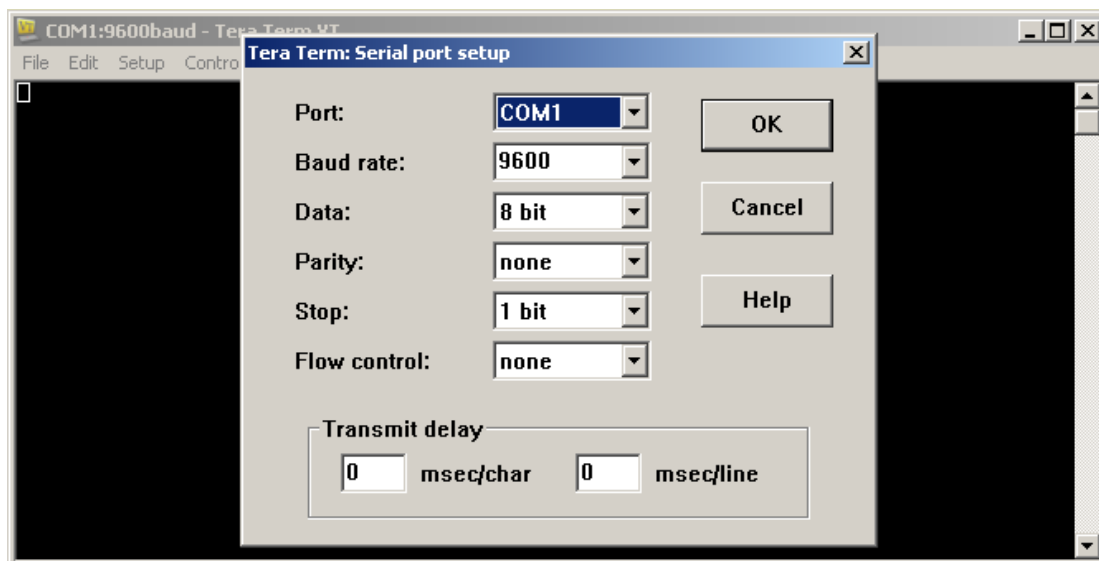
Nota: si no está instalado en el sistema, Tera Term se puede descargar del siguiente enlace seleccionando **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

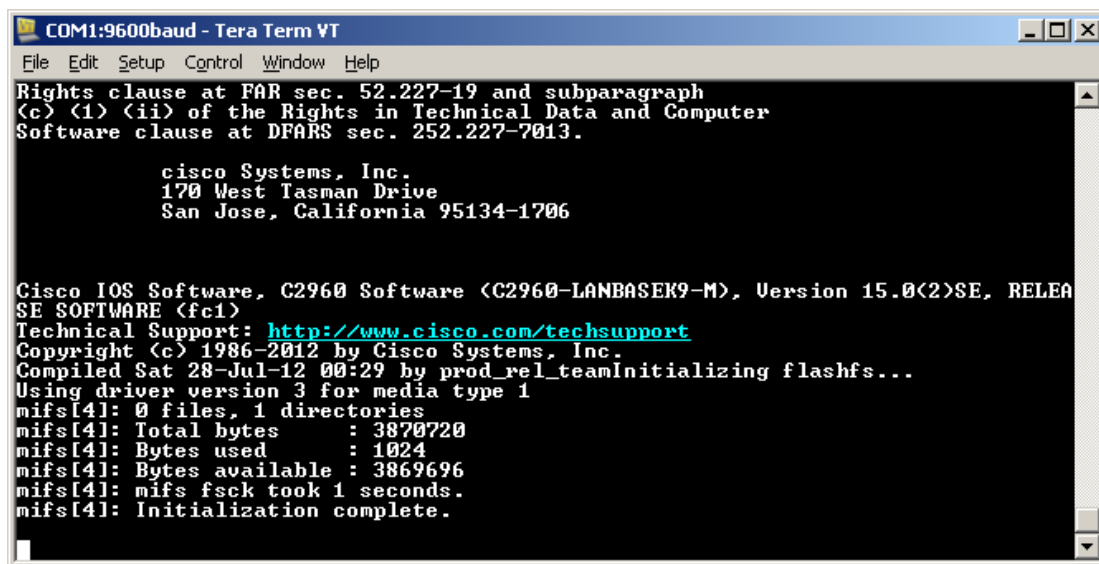
- b. En el cuadro de diálogo New Connection (Conexión nueva), haga clic en el botón de opción **Serial**. Verifique que esté seleccionado el puerto COM correcto y haga clic en **OK** (Aceptar) para continuar.



- c. En el menú **Setup** (Configuración) de Tera Term, seleccione **Serial port...** (Puerto serie) para verificar los parámetros de serie. Los parámetros predeterminados para el puerto de consola son 9600 baudios, 8 bits de datos, ninguna paridad, 1 bit de parada y ningún control del flujo. Los parámetros predeterminados de Tera Term coinciden con los parámetros del puerto de consola para las comunicaciones con el switch Cisco IOS.



- d. Cuando pueda ver el resultado de terminal, estará listo para configurar un switch Cisco. El siguiente ejemplo de la consola muestra el resultado para la terminal del switch durante la carga.



Parte 2: Mostrar y configurar parámetros básicos de los dispositivos

En esta sección, se le presentan los modos de ejecución privilegiado y de usuario. Debe determinar la versión del Sistema operativo Internetwork (IOS), mostrar los parámetros del reloj y configurar el reloj en el switch.

Paso 1: Mostrar la versión de la imagen del IOS del switch

- Una vez que el switch completa el proceso de inicio, se muestra el siguiente mensaje (introduzca **n** para continuar).

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Nota: si no ve el mensaje que se muestra arriba, consulte con el instructor para restablecer el switch a la configuración inicial.

- En el modo EXEC del usuario, muestre la versión del IOS para el switch.

```
Switch> show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
```

```
ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
```

```
Switch uptime is 2 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"
```

```
<resultado omitido>
```

¿Qué versión de la imagen del IOS utiliza actualmente el switch?

c2960-lanbasek9-mz.150-2.SE.bin. Las respuestas varían según el switch.

Paso 2: Configurar el reloj.

A medida que aprenda más sobre redes, verá que configurar la hora correcta en un switch Cisco puede resultar útil cuando trabaja en la resolución de problemas. Mediante los siguientes pasos, se configura manualmente el reloj interno del switch.

- Muestre la configuración actual del reloj.

```
Switch> show clock
```

```
*00:30:05.261 UTC Mon Mar 1 1993
```

- La configuración del reloj se cambia en el modo EXEC privilegiado. Para acceder al modo EXEC privilegiado, escriba **enable** en la petición de entrada del modo EXEC del usuario.

```
Switch> enable
```

- Configure los parámetros del reloj. El signo de interrogación (?) proporciona ayuda y le permite determinar la información de entrada esperada para configurar la hora, la fecha y el año actuales. Presione Entrar para completar la configuración del reloj.

```
Switch# clock set ?
```

```
hh:mm:ss Current Time
```

```
Switch# clock set 15:08:00 ?
```

```
<1-31> Day of the month
```

```
MONTH Month of the year
```

```
Switch# clock set 15:08:00 Oct 26 ?
```

```
<1993-2035> Year
```

```
Switch# clock set 15:08:00 Oct 26 2012
```

```
Switch#
```

```
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43 UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by console.
```

- d. Introduzca el comando **show clock** para verificar que los parámetros del reloj se hayan actualizado.

```
Switch# show clock
```

```
15:08:07.205 UTC Fri Oct 26 2012
```

Parte 3: Acceder a un router Cisco mediante un cable de consola mini-USB (optativo)

Si utiliza un router Cisco 1941 u otros dispositivos Cisco IOS con un puerto de consola mini-USB, puede acceder al puerto de consola del dispositivo mediante un cable mini-USB conectado al puerto USB en su PC.

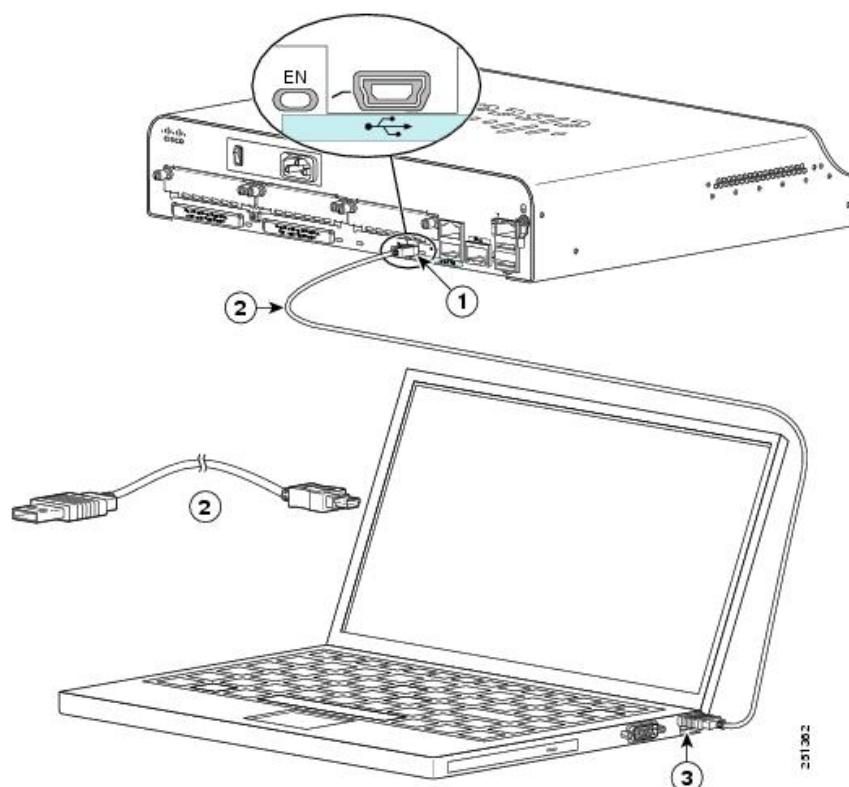
Nota: el cable de consola mini-USB es el mismo tipo de cable mini-USB que se utiliza con otros dispositivos electrónicos, como discos duros USB, impresoras USB o hubs USB. Estos cables mini-USB pueden adquirirse a través de Cisco Systems, Inc. o de otros proveedores externos. Asegúrese de utilizar un cable mini-USB (y no un cable micro-USB) para conectarse al puerto de consola mini-SUB en un dispositivo Cisco IOS.



Nota: debe utilizar el puerto USB o el puerto RJ-45; no se deben usar ambos de manera simultánea. Cuando se utiliza el puerto USB, tiene prioridad sobre el puerto de consola RJ-45 usado en la parte 1.

Paso 1: Configurar la conexión física con un cable mini-USB

- a. Conecte el cable mini-USB al puerto de consola mini-USB del router.
- b. Conecte el otro extremo del cable a un puerto USB de la PC.
- c. Si aún no están encendidos, encienda el router Cisco y la PC.



- 1) Puerto de consola USB tipo B mini de 5 pines
- 2) Cable de consola USB tipo B mini de 5 pines a USB tipo A
- 3) Conector USB tipo A

Paso 2: Verificar que la consola USB está lista

Si utiliza una PC con Microsoft Windows y el indicador LED del puerto de consola USB (con el rótulo EN) no se vuelve de color verde, instale el controlador de consola USB de Cisco.

En PC con Microsoft Windows conectadas a un dispositivo Cisco IOS con un cable USB, se debe instalar un controlador USB antes de su uso. El controlador se puede encontrar en www.cisco.com con el dispositivo Cisco IOS relacionado. El controlador USB se puede descargar en el siguiente enlace:

<http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

Nota: para descargar este archivo, debe tener una cuenta válida de Cisco Connection Online (CCO).

Nota: este enlace está relacionado con el router Cisco 1941; sin embargo, el controlador de consola USB no es específico del modelo de dispositivo Cisco IOS. Este controlador de consola USB funciona solamente con switches y routers Cisco. Para finalizar la instalación del controlador USB, se debe reiniciar la PC.

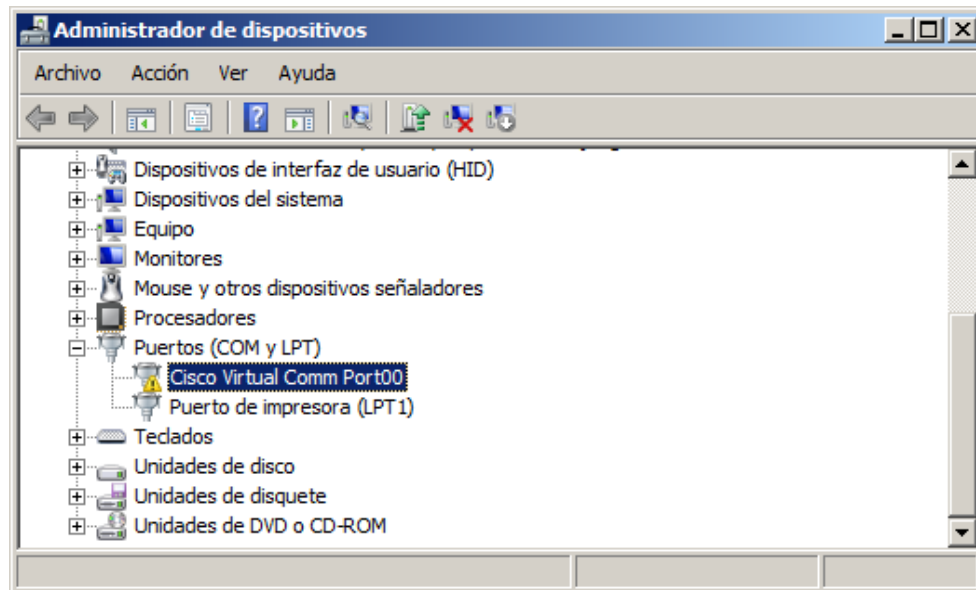
Nota: una vez extraídos los archivos, la carpeta contiene instrucciones de instalación y remoción, y los controladores necesarios para los distintos sistemas operativos y arquitecturas. Seleccione la versión adecuada para su sistema.

Cuando el indicador LED del puerto de consola USB se vuelve de color verde, el puerto está listo para el acceso.

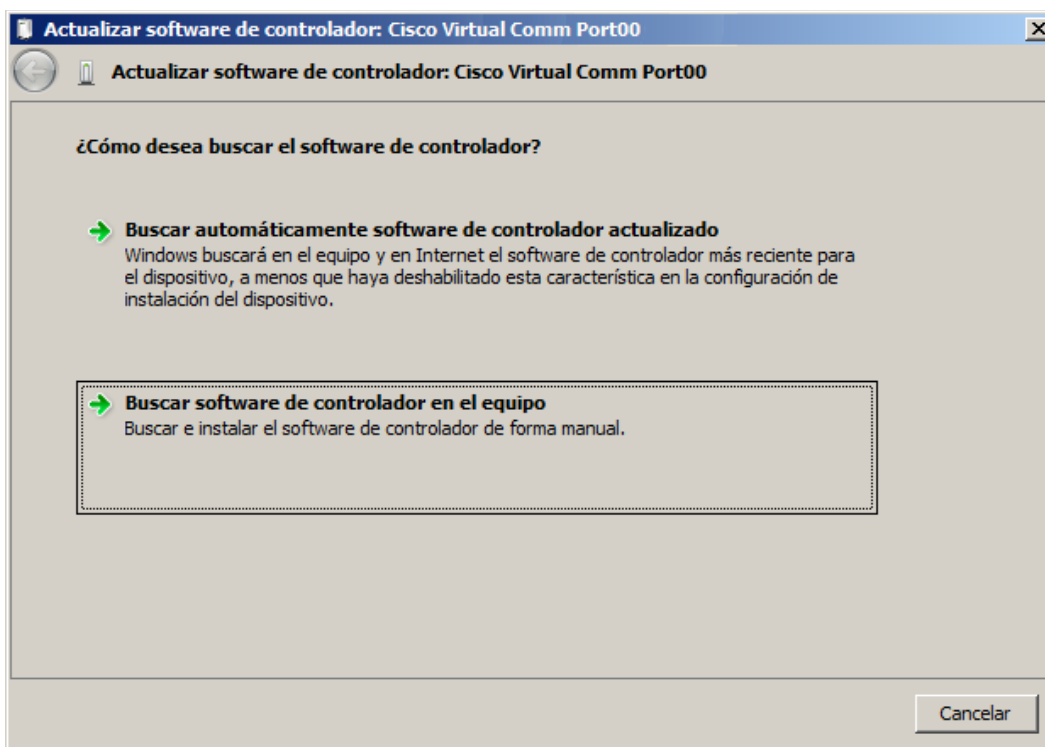
Paso 3: Habilitar el puerto COM para la PC con Windows 7 (optativo)

Si utiliza una PC con Microsoft Windows 7, tal vez necesita realizar los siguientes pasos para habilitar el puerto COM:

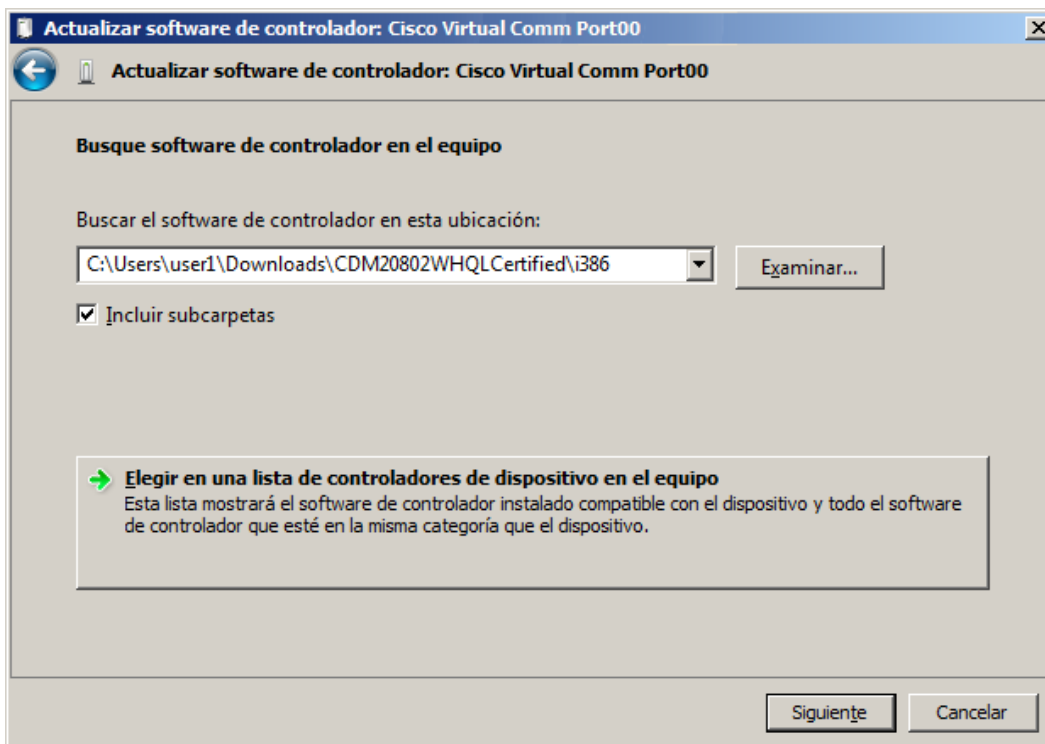
- Haga clic en el ícono de **Inicio de Microsoft** para acceder al **Panel de control**.
- Abra el **Administrador de dispositivos**.
- Haga clic en el enlace de árbol **Puertos (COM y LPT)** para expandirlo. Aparecerá el ícono de **Cisco Virtual Comm Port00** con un signo de exclamación amarillo.



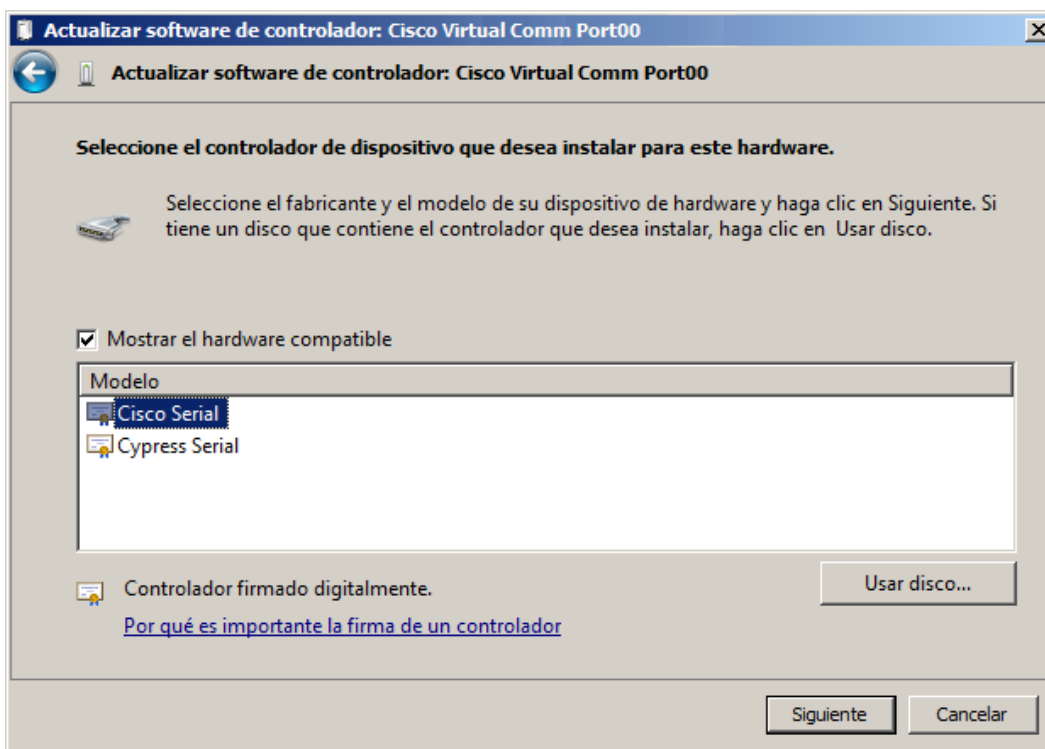
- d. Para resolver el problema, haga clic con el botón secundario en el ícono **Cisco Virtual Comm Port00** y seleccione **Actualizar software de controlador**.
- e. Seleccione **Buscar software de controlador en el equipo**.



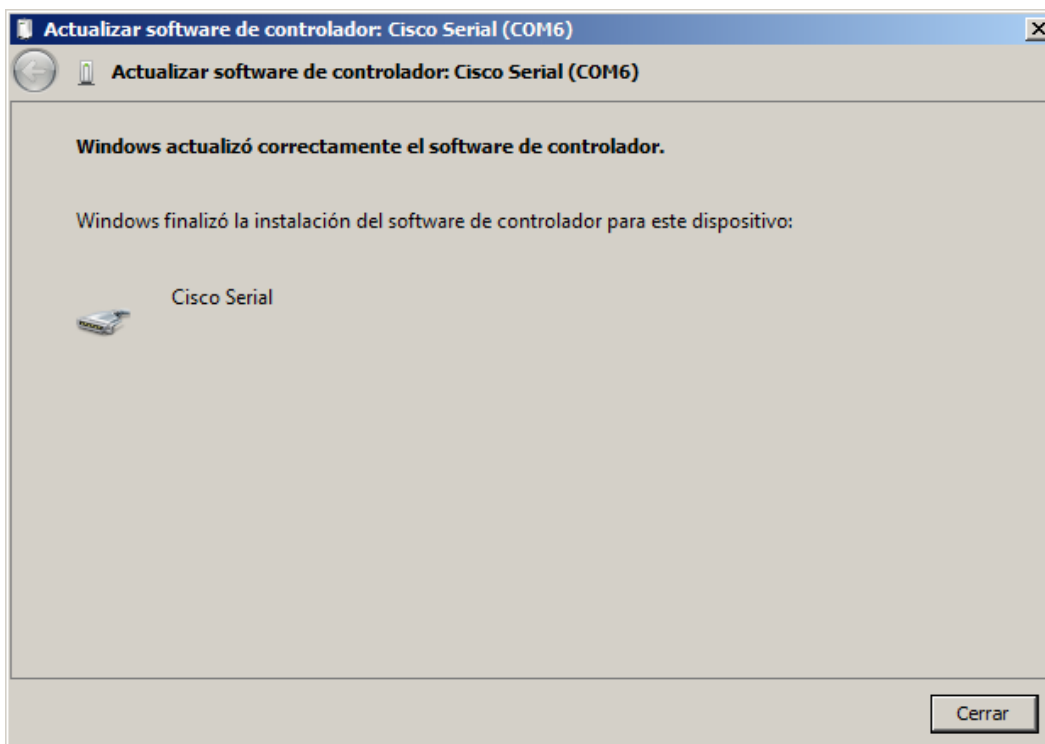
- f. Seleccione **Elegir en una lista de controladores de dispositivo en el equipo** y haga clic en **Siguiente**.



- g. Seleccione el controlador **Cisco Serial** y haga clic en **Siguiente**.

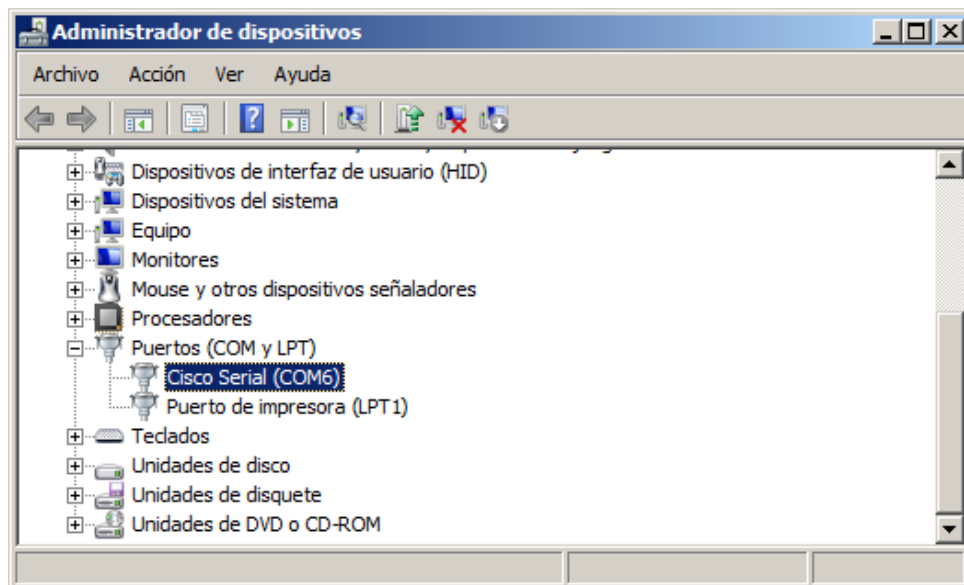


- h. El controlador de dispositivo se instaló correctamente. Tome nota del número de puerto asignado en la parte superior de la ventana. En este ejemplo, se utiliza COM 6 para la comunicación con el router. Haga clic en **Cerrar**.

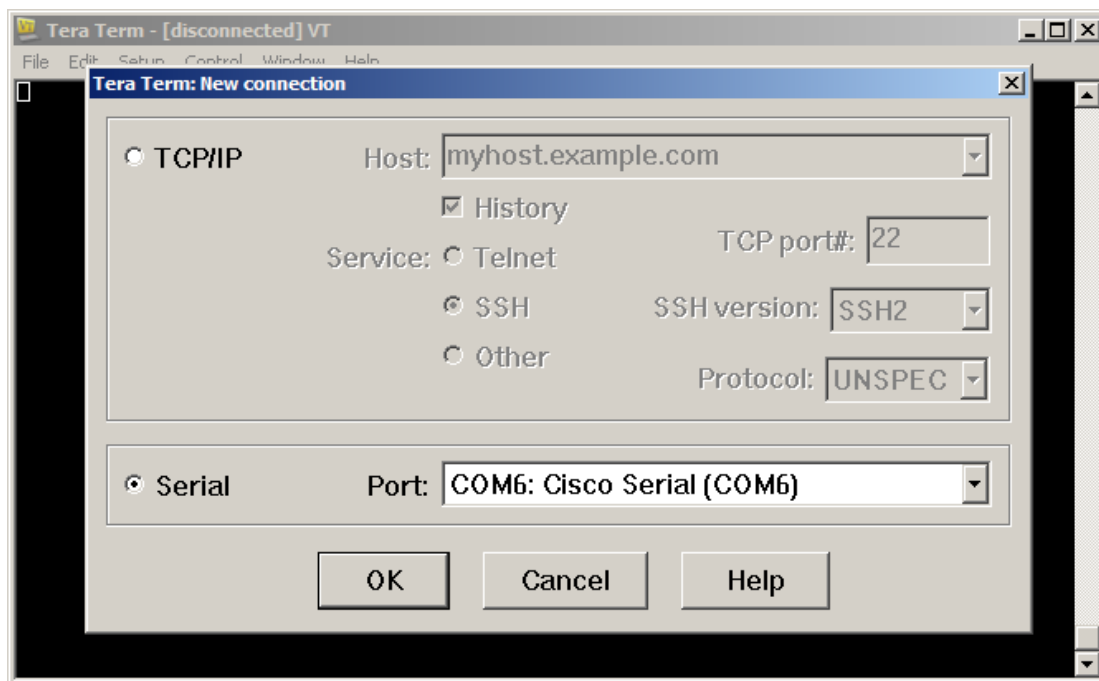


Paso 4: Determinar el número de puerto COM (optativo)

- a. Si necesita determinar el número de puerto COM, abra el **Panel de control** y seleccione **Administrador de dispositivos**. Busque el encabezado **Puertos (COM y LPT)**, expándalo y determine el número de puerto COM que está en uso. En este ejemplo, se seleccionó **Cisco Serial (COM 6)** para la conexión al router, dado que hay un controlador de consola USB de Cisco en uso. Si utiliza un cable de consola o un adaptador de otro fabricante, esa información se refleja en la convención de nomenclatura.



- b. Abra Tera Term. Haga clic en el botón de opción **Serial** y seleccione **Port COM6: Cisco Serial (COM 6)** (Puerto COM6: Cisco Serial [COM 6]). Este puerto ahora debe estar disponible para la comunicación con el router. Haga clic en **OK** (Aceptar).



Reflexión

1. ¿Cómo evita que personal no autorizado acceda a su dispositivo Cisco a través del puerto de consola?

Aportando seguridad física al dispositivo y utilizando protección con contraseña

2. ¿Cuáles son las ventajas y desventajas de usar la conexión serial de consola en comparación con la conexión USB de consola a un switch o un router Cisco?

Depende de la disponibilidad de puertos en la PC y el router o switch. Si la PC tiene un puerto serie y se dispone de un cable DB9 a RJ45, generalmente es más fácil conectarse al router o al switch utilizando el puerto serie de consola. Si la PC no tiene un puerto serie, se puede usar un adaptador de USB a serie de un proveedor externo. Los switches Cisco no tienen puertos de consola mini-USB, por lo que la conexión por USB no es una opción. Si se conecta con frecuencia a un router Cisco que tiene un puerto de consola mini-USB, este puede ser el método más eficaz una vez que los controladores Cisco están instalados, porque prácticamente todas las PC más recientes tienen puertos USB.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Práctica de laboratorio: Creación de una red simple (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

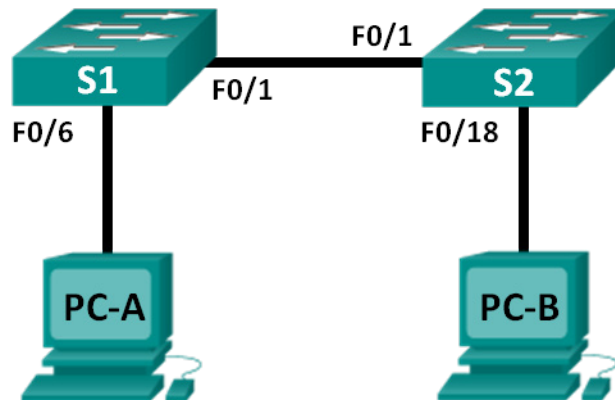


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	No aplicable	No aplicable	No aplicable
S2	VLAN 1	No aplicable	No aplicable	No aplicable
PC-A	NIC	192.168.1.10	255.255.255.0	No aplicable
PC-B	NIC	192.168.1.11	255.255.255.0	No aplicable

Objetivos

Parte 1: Configurar la topología de la red (Ethernet únicamente)

- Identificar los cables y puertos para usar en la red.
- Realizar el cableado de una topología física de laboratorio.

Parte 2: Configurar hosts en las PC

- Introducir la información de dirección IP estática en la interfaz LAN de los hosts.
- Verificar que las PC puedan comunicarse por medio de la utilidad **ping**.

Parte 3: Configurar y verificar los parámetros básicos del switch

- Configurar cada switch con nombre de host, contraseñas locales y mensaje de inicio de sesión.
- Guardar las configuraciones en ejecución.
- Mostrar la configuración en ejecución del switch.
- Mostrar la versión del IOS para el switch en uso.
- Mostrar el estado de las interfaces.

Información básica/Situación

Las redes están formadas por tres componentes principales: hosts, switches y routers. En esta práctica de laboratorio, armará una red simple con dos hosts y dos switches. También configurará parámetros básicos, incluidos nombres de host, contraseñas locales y mensaje de inicio de sesión. Utilice los comandos **show** para mostrar la configuración en ejecución, la versión del IOS y el estado de la interfaz. Utilice el comando **copy** para guardar las configuraciones de los dispositivos.

En esta práctica de laboratorio, aplicará direccionamiento IP a las PC para habilitar la comunicación entre estos dos dispositivos. Use la utilidad **ping** para verificar la conectividad.

Nota: los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: asegúrese de que los switches se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice A para conocer el procedimiento de inicialización y recarga de un switch.

Recursos necesarios

- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota para el instructor: los puertos Ethernet de los switches 2960 cuentan con detección automática, y se puede utilizar un cable de conexión directa o un cable cruzado para todas las conexiones. Si los switches que se utilizan en la topología no son del modelo 2960, es probable que se necesite un cable cruzado para conectar los dos switches.

Parte 1: Configurar la topología de la red (Ethernet únicamente).

En la parte 1, realizará el cableado para conectar los dispositivos según la topología de la red.

Paso 1: Encender los dispositivos

Encienda todos los dispositivos de la topología. Los switches no tienen un interruptor de corriente; se encienden en cuanto enchufa el cable de alimentación.

Paso 2: Conectar los dos switches

Conecte un extremo de un cable Ethernet a F0/1 en el S1 y el otro extremo del cable a F0/1 en el S2. Las luces de F0/1 en los dos switches deberían tornarse ámbar y, luego, verde. Esto indica que los switches se conectaron correctamente.

Paso 3: Conectar las PC a sus respectivos switches

- Conecte un extremo del segundo cable Ethernet al puerto NIC en la PC-A. Conecte el otro extremo del cable a F0/6 en el S1. Después de conectar la PC al switch, la luz de F0/6 debería tornarse ámbar y luego verde, lo que indica que la PC-A se conectó correctamente.
- Conecte un extremo del último cable Ethernet al puerto NIC en la PC-B. Conecte el otro extremo del cable a F0/18 en el S2. Después de conectar la PC al switch, la luz de F0/18 debería tornarse ámbar y luego verde, lo que indica que la PC-B se conectó correctamente.

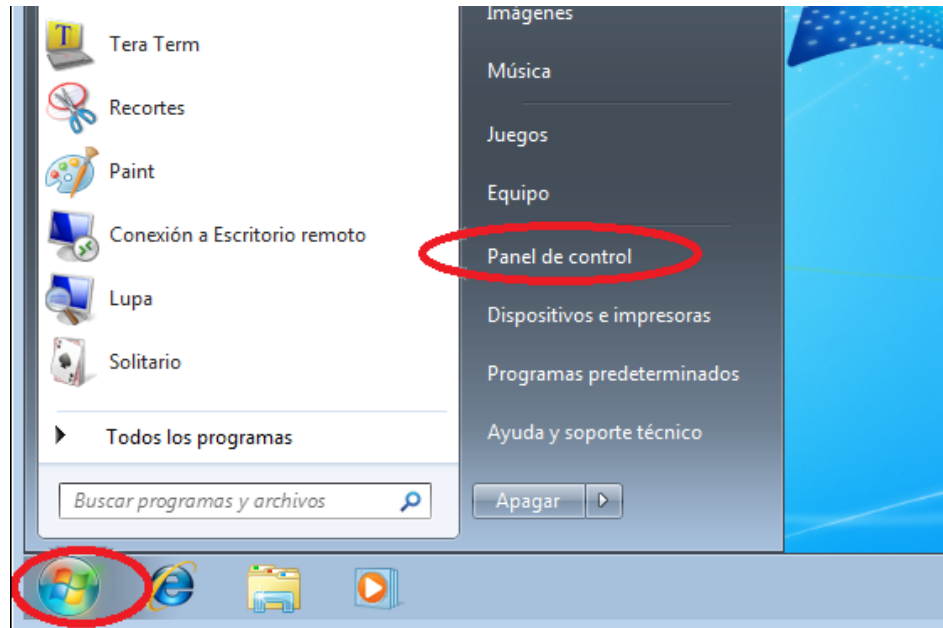
Paso 4: Inspeccionar visualmente las conexiones de la red

Después de realizar el cableado de los dispositivos de red, tómese un momento para verificar cuidadosamente las conexiones con el fin de minimizar el tiempo necesario para resolver problemas de conectividad de red más adelante.

Parte 2: Configurar hosts en las PC

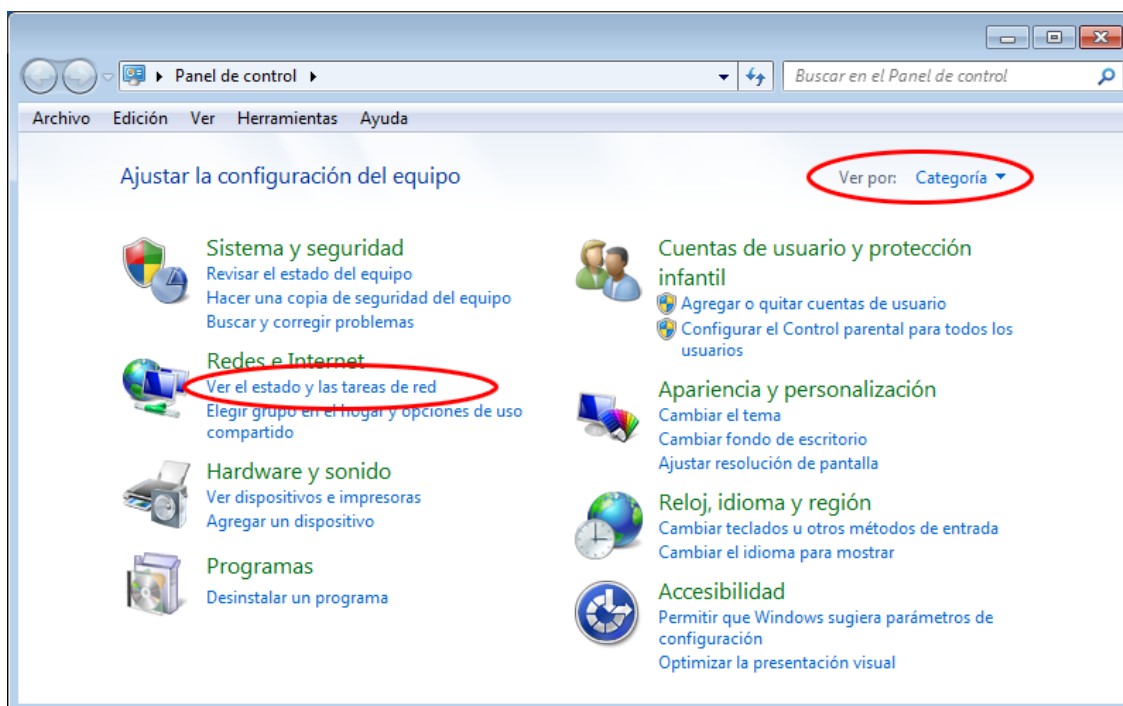
Paso 1: Configurar la información de dirección IP estática en las PC

- a. Haga clic en el ícono **Inicio de Windows** y, a continuación, seleccione **Panel de control**.

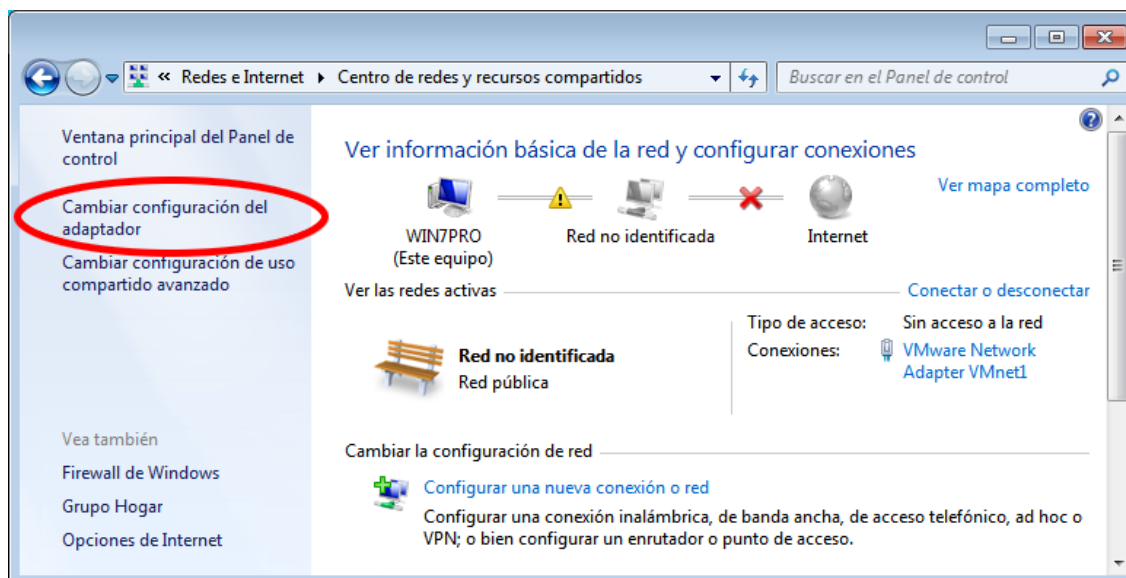


- b. En la sección Redes e Internet, haga clic en el enlace **Ver el estado y las tareas de red**.

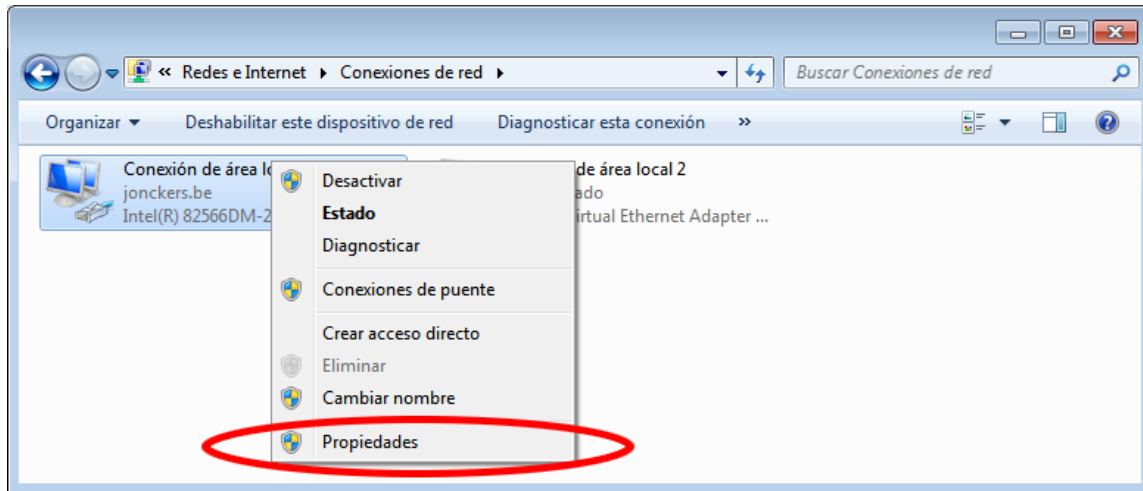
Nota: si en el panel de control se muestra una lista de íconos, haga clic en la opción desplegable que está junto a **Ver por:** y cambie la opción para que se muestre por **Categoría**.



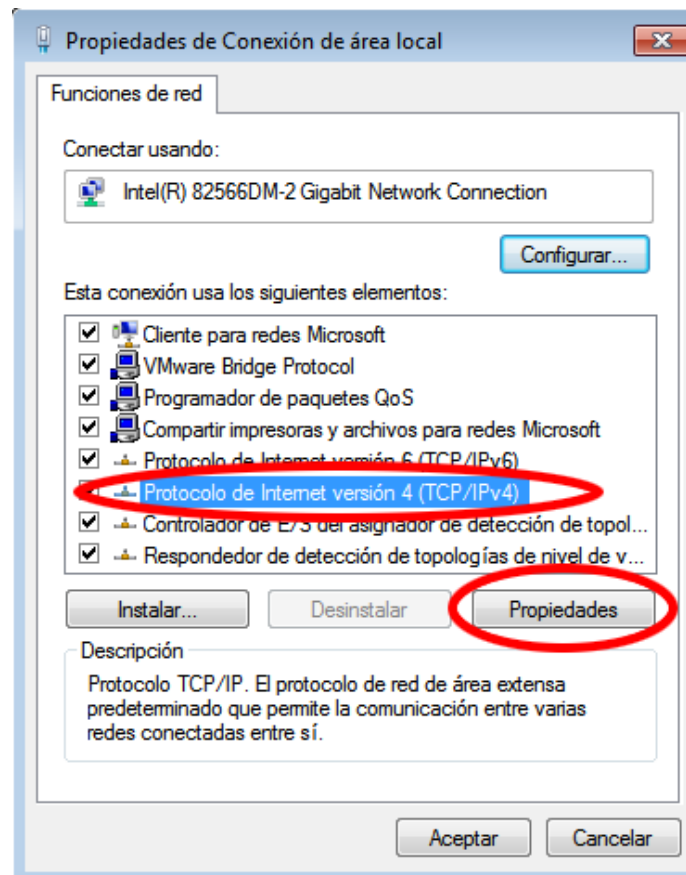
- c. En el panel izquierdo de la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**.



- d. En la ventana Conexiones de red, se muestran las interfaces disponibles en la PC. Haga clic con el botón secundario en la interfaz **Conexión de área local** y seleccione **Propiedades**.

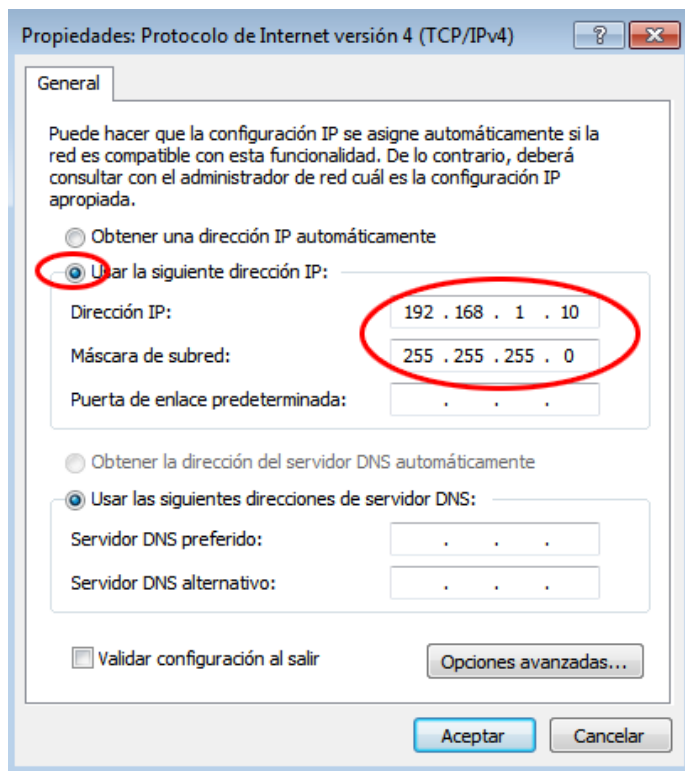


- e. Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades**.



Nota: también puede hacer doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)** para que se muestre la ventana Propiedades.

- f. Haga clic en el botón de opción **Usar la siguiente dirección IP** para introducir manualmente una dirección IP, la máscara de subred y el gateway predeterminado.



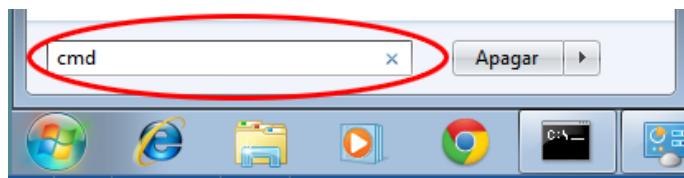
Nota: en el ejemplo mencionado arriba, se introdujeron la dirección IP y la máscara de subred para la PC-A. El gateway predeterminado no se introdujo porque no hay un router conectado a la red. Consulte la tabla de direccionamiento de la página 1 para obtener información de dirección IP para la PC- B.

- g. Después de introducir toda la información IP, haga clic en **Aceptar**. Haga clic en **Aceptar** en la ventana Propiedades de Conexión de área local para asignar la dirección IP al adaptador LAN.
- h. Repita los pasos anteriores para introducir la información de dirección IP para la PC-B.

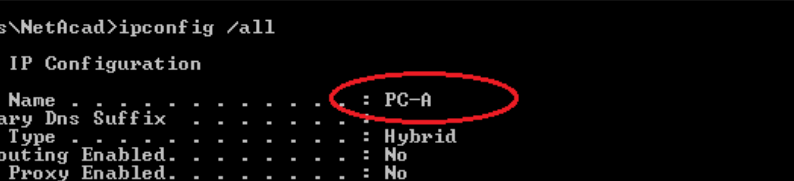
Paso 2: Verificar la configuración y la conectividad de la PC

Utilice la ventana del símbolo del sistema (**cmd.exe**) para verificar la configuración y la conectividad de la PC.

- a. En la PC-A, haga clic en el ícono **Inicio de Windows**, escriba **cmd** en el cuadro de diálogo **Buscar programas y archivos** y, a continuación, presione Entrar.



- b. En la ventana cmd.exe, puede introducir comandos directamente en la PC y ver los resultados de esos comandos. Verifique la configuración de la PC mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4.



C:\Windows\system32\cmd.exe

```
C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-A
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No


Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-BE-6C-89
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:b05a%11(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- c. Escriba **ping 192.168.1.11** y presione Entrar.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

¿Fueron correctos los resultados del ping? _____ Sí

Si no lo fueron, resuelva los problemas que haya presentes.

Nota: si no obtuvo una respuesta de PC-B, intente hacer ping a PC-B nuevamente. Si aún no recibe una respuesta de PC-B, intente hacer ping a PC-A desde PC-B. Si no puede obtener una respuesta de la PC remota, solicite ayuda al instructor para resolver el problema.

Nota para el instructor: si el primer paquete ICMP excede el tiempo de espera, eso podría deberse a que la PC intenta resolver la dirección de destino. Esto no debería ocurrir si se repite el ping, dado que ahora la dirección se encuentra en la memoria caché.

Parte 3: Configurar y verificar los parámetros básicos del switch

Paso 1: Acceda al switch mediante el puerto de consola.

Utilice Tera Term para establecer una conexión de consola al switch desde la PC-A.

Paso 2: Ingrese al modo EXEC privilegiado.

Puede acceder a todos los comandos del switch en el modo EXEC privilegiado. El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes. Entre al modo EXEC privilegiado introduciendo el comando **enable**.

```
Switch> enable
Switch#
```

La petición de entrada cambió de **Switch>** a **Switch#**, lo que indica que está en el modo EXEC privilegiado.

Paso 3: Entre al modo de configuración.

Utilice el comando **configuration terminal** para ingresar al modo de configuración.

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

La petición de entrada cambió para reflejar el modo de configuración global.

Paso 4: Asignar un nombre al switch

Utilice el comando **hostname** para cambiar el nombre del switch a **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Paso 5: Evitar búsquedas de DNS no deseadas

Para evitar que el switch intente traducir comandos introducidos de manera incorrecta como si fueran nombres de host, desactive la búsqueda del Sistema de nombres de dominios (DNS).

```
S1(config)# no ip domain-lookup
S1(config)#
```

Paso 6: Introducir contraseñas locales

Para impedir el acceso no autorizado al switch, se deben configurar contraseñas.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Paso 7: Introducir un mensaje MOTD de inicio de sesión

Se debe configurar un mensaje de inicio de sesión, conocido como “mensaje del día” (MOTD), para advertir a cualquier persona que acceda al switch que no se tolerará el acceso no autorizado.

El comando **banner motd** requiere el uso de delimitadores para identificar el contenido del mensaje de aviso. El carácter delimitador puede ser cualquier carácter siempre que no aparezca en el mensaje. Por este motivo, a menudo se usan símbolos como #.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full extent
of the law. #
S1(config)# exit
S1#
```

Paso 8: Guardar la configuración.

Utilice el comando **copy** para guardar la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil (NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Paso 9: Mostrar la configuración actual

El comando **show running-config** muestra toda la configuración en ejecución, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas. Los comandos configurados en los pasos del 1 al 8 están resaltados a continuación.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
```

```
system mtu routing 1500
!
!
no ip domain-lookup
!

<resultado omitido>

!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
password cisco
login
line vty 0 4
login
line vty 5 15
login
!
end

S1#
```

Paso 10: Mostrar la versión del IOS y otra información útil del switch

Utilice el comando **show version** para que se muestre la versión del IOS que se ejecuta en el switch, junto con otra información útil. Una vez más, necesitará utilizar la barra espaciadora para avanzar por la información que se muestra.

```
S1# show version

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

S1 uptime is 1 hour, 38 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF

Hardware Board Revision Number : 0x0A

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0 (2) SE	C2960-LANBASEK9-M

Configuration register is 0xF

S1#

Paso 11: Mostrar el estado de las interfaces conectadas en el switch

Para revisar el estado de las interfaces conectadas, utilice el comando **show ip interface brief**. Presione la barra espaciadora para avanzar hasta el final de la lista.

```
S1# show ip interface brief
Interface                IP-Address      OK? Method Status  Protocol
Vlan1                    unassigned      YES unset  up      up
FastEthernet0/1          unassigned      YES unset  up      up
FastEthernet0/2          unassigned      YES unset  down    down
FastEthernet0/3          unassigned      YES unset  down    down
FastEthernet0/4          unassigned      YES unset  down    down
FastEthernet0/5          unassigned      YES unset  down    down
FastEthernet0/6          unassigned      YES unset  up      up
FastEthernet0/7          unassigned      YES unset  down    down
FastEthernet0/8          unassigned      YES unset  down    down
FastEthernet0/9          unassigned      YES unset  down    down
FastEthernet0/10         unassigned      YES unset  down    down
FastEthernet0/11         unassigned      YES unset  down    down
FastEthernet0/12         unassigned      YES unset  down    down
FastEthernet0/13         unassigned      YES unset  down    down
FastEthernet0/14         unassigned      YES unset  down    down
FastEthernet0/15         unassigned      YES unset  down    down
FastEthernet0/16         unassigned      YES unset  down    down
FastEthernet0/17         unassigned      YES unset  down    down
FastEthernet0/18         unassigned      YES unset  down    down
FastEthernet0/19         unassigned      YES unset  down    down
FastEthernet0/20         unassigned      YES unset  down    down
FastEthernet0/21         unassigned      YES unset  down    down
FastEthernet0/22         unassigned      YES unset  down    down
FastEthernet0/23         unassigned      YES unset  down    down
FastEthernet0/24         unassigned      YES unset  down    down
GigabitEthernet0/1       unassigned      YES unset  down    down
GigabitEthernet0/2       unassigned      YES unset  down    down
S1#
```

Paso 12: Repetir los pasos del 1 al 12 para configurar el switch S2

La única diferencia para este paso es cambiar el nombre de host a S2.

Paso 13: Registrar el estado de interfaz para las interfaces siguientes

Interfaz	S1		S2	
	Estado	Protocolo	Estado	Protocolo
F0/1	Up	Up	Up	Up
F0/6	Up	Up	Down	Down
F0/18	Down	Down	Up	Up
VLAN 1	Up	Up	Up	Up

¿Por qué algunos puertos FastEthernet en los switches están activos y otros inactivos?

Los puertos FastEthernet están activos cuando los cables están conectados a los puertos, a menos que los administradores los hayan desactivado manualmente. De lo contrario, los puertos están inactivos.

Reflexión

¿Qué podría evitar que se envíe un ping entre las PC?

Dirección IP incorrecta, medios desconectados, switch apagado o puertos administrativamente inactivos, firewall.

Nota: puede ser necesario desactivar el firewall de las PC para hacer ping entre ellas.

Apéndice A: Inicialización y recarga de un switch

Paso 1: Conéctese al switch.

Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Paso 2: Determine si se crearon redes de área local virtuales (VLAN, Virtual Local-Area Networks).

Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash
```

```
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

Paso 3: Elimine el archivo VLAN.

- a. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Entrar si introdujo el nombre de manera correcta.

- b. Cuando se le pregunte sobre la eliminación de este archivo, presione Entrar para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

```
Delete flash:/vlan.dat? [confirm]
Switch#
```


Paso 4: Borre el archivo de configuración de inicio.

Utilice el comando **erase startup-config** para borrar el archivo de configuración de inicio de la NVRAM. Cuando se le pregunte sobre la eliminación del archivo de configuración, presione Entrar para confirmar el borrado. (Si se presiona cualquier otra tecla, se anula la operación).

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Paso 5: Recargar el switch.

Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Cuando se le pregunte sobre la recarga del switch, presione Entrar para continuar con la recarga. (Si se presiona cualquier otra tecla, se anula la recarga).

```
Switch# reload
Proceed with reload? [confirm]
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 6: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Escriba **no** en la petición de entrada y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Configuraciones de dispositivos

Switch S1 (completo)

```
S1#sh run
```

```
Building configuration...
```

```
Current configuration : 1514 bytes
```

```
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname S1
```

```
!
boot-start-marker
boot-end-marker
```

```
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

```
!
```

```
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```

```
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  no ip address  
!  
ip http server  
ip http secure-server  
!  
banner motd ^C  
Unauthorized access is strictly prohibited and prosecuted to the full extent of the  
law. ^C  
!  
line con 0  
  password cisco  
  login  
line vty 0 4  
  login  
line vty 5 15  
  login  
!  
end
```

Switch S2 (completo)

```
S2#sh run  
Building configuration...  
  
*Mar  1 03:20:01.648: %SYS-5-CONFIG_I: Configured from console by console  
Current configuration : 1514 bytes  
!  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S2  
!
```

```
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
  password cisco
  login
line vty 0 4
  login
line vty 5 15
  login
!
end
```

Práctica de laboratorio: Configuración de una dirección de administración del switch (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

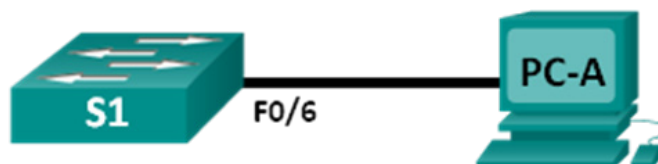


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.2	255.255.255.0	No aplicable
PC-A	NIC	192.168.1.10	255.255.255.0	No aplicable

Objetivos

Parte 1: Configurar un dispositivo de red básico

- Realizar el cableado de red tal como se muestra en la topología.
- Configurar los parámetros básicos del switch, incluidos el nombre de host, la dirección de administración y el acceso por Telnet.
- Configurar una dirección IP en la PC.

Parte 2: Verificar y probar la conectividad de red

- Mostrar la configuración del dispositivo.
- Probar la conectividad de extremo a extremo con ping.
- Probar la capacidad de administración remota con Telnet.
- Guardar el archivo de configuración en ejecución del switch.

Información básica/Situación

Los switches Cisco tienen una interfaz especial, conocida como “interfaz virtual del switch” (SVI). La SVI se puede configurar con una dirección IP, comúnmente conocida como la dirección de administración que se utiliza para el acceso remoto al switch para mostrar o configurar parámetros.

En esta práctica de laboratorio, armará una red simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Configuraré los parámetros básicos del switch y el direccionamiento IP, y demostraré el uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host, y utiliza puertos Ethernet y de consola únicamente.

Nota: los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados producidos pueden variar de lo que se muestra en las prácticas de laboratorio.

Nota: asegúrese de que el switch se haya borrado y no tenga una configuración de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar un dispositivo de red básico

En la parte 1, configurará la red y los parámetros básicos, como nombres de host, direcciones IP de las interfaces y contraseñas.

Paso 1: Conectar la red

- a. Realizar el cableado de red tal como se muestra en la topología.
- b. Establezca una conexión de consola al switch desde la PC-A.

Paso 2: Configurar los parámetros básicos del switch

En este paso, configurará los parámetros básicos del switch, como el nombre de host, y configurará una dirección IP para la SVI. Asignar una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administrará el switch. Telnet y Shell seguro (SSH) son dos de los métodos de administración más comunes; sin embargo, Telnet es un protocolo muy inseguro. Toda la información que fluye entre los dos dispositivos se envía como texto no cifrado. Las contraseñas y otra información confidencial pueden ser fáciles de ver si se las captura mediante un programa detector de paquetes.

- a. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del usuario en el switch, con la petición de entrada `Switch>`. Ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

- b. Verifique que haya un archivo de configuración vacío con el comando `show running-config` del modo EXEC privilegiado. Si previamente se guardó un archivo de configuración, deberá eliminarlo. Según cuál sea el modelo del switch y la versión del IOS, la configuración podría variar. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, solicite ayuda al instructor.

- c. Ingrese al modo de configuración global y asigne un nombre de host al switch.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

- d. Configure el acceso por contraseña al switch.

```
S1(config)# enable secret class
S1(config)#
```

- e. Evite búsquedas no deseadas del Sistema de nombres de dominios (DNS).

```
S1(config)# no ip domain-lookup
S1(config)#
```

- f. Configure un mensaje del día (MOTD) de inicio de sesión.

```
S1(config)# banner motd #
Enter Text message. End with the character `#'.
Unauthorized access is strictly prohibited. #
```

- g. Para verificar la configuración de acceso, alterne entre los modos.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

¿Qué tecla de método abreviado se utilizan para pasar directamente del modo de configuración global al modo EXEC privilegiado?

Ctrl+Z

- h. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario.

```
S1> enable
Password: class
S1#
```

Nota: la contraseña no se mostrará en la pantalla al ingresar.

- i. Ingrese al modo de configuración global para configurar la dirección IP de la SVI para permitir la administración remota de switch.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

- j. Restrinja el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

- k. Configure la línea de terminal virtual (VTY) para que el switch permita el acceso por Telnet. Si no configura una contraseña de VTY, no podrá acceder al switch mediante Telnet.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
```



```
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Paso 3: Configurar una dirección IP en la PC-A

- a. Asigne la dirección IP y la máscara de subred a la PC, como se muestra en la Addressing Table de la página 1. A continuación, se describe el procedimiento para asignar una dirección IP en una PC con Windows 7:
 - 1) Haga clic en el ícono **Inicio de Windows > Panel de control**.
 - 2) Haga clic en **Ver por: > Categoría**.
 - 3) Seleccione **Ver el estado y las tareas de red > Cambiar configuración del adaptador**.
 - 4) Haga clic con el botón secundario en **Conexión de área local** y seleccione **Propiedades**.
 - 5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en **Propiedades > Aceptar**.
 - 6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca manualmente la dirección IP y la máscara de subred.

Parte 2: Verificar y probar la conectividad de red

Ahora verificará y registrará la configuración del switch, probará la conectividad de extremo a extremo entre la PC-A y el S1, y probará la capacidad de administración remota del switch.

Paso 1: Mostrar la configuración del dispositivo S1

- a. Regrese a la conexión de consola utilizando Tera Term en la PC-A para mostrar y verificar la configuración del switch por medio de la emisión del comando **show run**. A continuación, se muestra una configuración de muestra. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
```

```
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2

<resultado omitido>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
login
!
end
```

- b. Verifique el estado de su interfaz de administración SVI. La interfaz VLAN 1 debería tener estado up/up (activo/activo) y tener una dirección IP asignada. Observe que el puerto de switch F0/6 también está activado, porque la PC-A está conectada a él. Dado que todos los puertos de switch están inicialmente en VLAN 1 de manera predeterminada, puede comunicarse con el switch mediante la dirección IP que configuró para VLAN 1.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

Paso 2: Probar la conectividad de extremo a extremo

Abra una ventana del símbolo del sistema (cmd.exe) en la PC-A: haga clic en el ícono **Inicio de Windows** e introduzca **cmd** en el campo **Buscar programas y archivos**. Verifique la dirección IP de la PC-A mediante el comando **ipconfig /all**. Este comando muestra el nombre de host de la PC y la información de la dirección IPv4. Haga ping a la propia dirección de la PC-A y a la dirección de administración del S1.

- a. Haga ping a la dirección de la propia PC-A primero.

```
C:\Users\NetAcad> ping 192.168.1.10
```

El resultado debe ser similar a la siguiente pantalla:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\NetAcad>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo=7ms TTL=120
Respuesta desde 192.168.1.10: bytes=32 tiempo=20ms TTL=120
Respuesta desde 192.168.1.10: bytes=32 tiempo=6ms TTL=120
Respuesta desde 192.168.1.10: bytes=32 tiempo=7ms TTL=120

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Minimo = 6ms, Maximo = 20ms, Media = 10ms

C:\Users\NetAcad>_
  
```

- b. Haga ping a la dirección de administración de SVI del S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla. Si los resultados del ping no son correctos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Si es necesario, revise el cableado físico y el direccionamiento IP.

```

C:\Users\NetAcad>
C:\Users\NetAcad>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.2: bytes=32 tiempo=5ms TTL=248
Respuesta desde 192.168.1.2: bytes=32 tiempo=5ms TTL=248
Respuesta desde 192.168.1.2: bytes=32 tiempo=5ms TTL=248

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 3, perdidos = 1 (25% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Minimo = 5ms, Maximo = 5ms, Media = 5ms

C:\Users\NetAcad>_
  
```

Paso 3: Probar y verificar la administración remota del S1

Ahora utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. En esta práctica de laboratorio, la PC-A y el S1 se encuentran uno junto al otro. En una red de producción, el switch podría estar en un armario de cableado en el piso superior, mientras que la PC de administración podría estar ubicada en la planta baja. Telnet no es un protocolo seguro. Sin embargo, en esta práctica de laboratorio lo usará para probar el acceso remoto. Toda la información enviada por Telnet, incluidos los comandos y las contraseñas, se envían durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, utilizará Shell seguro (SSH) para acceder a los dispositivos de red en forma remota.

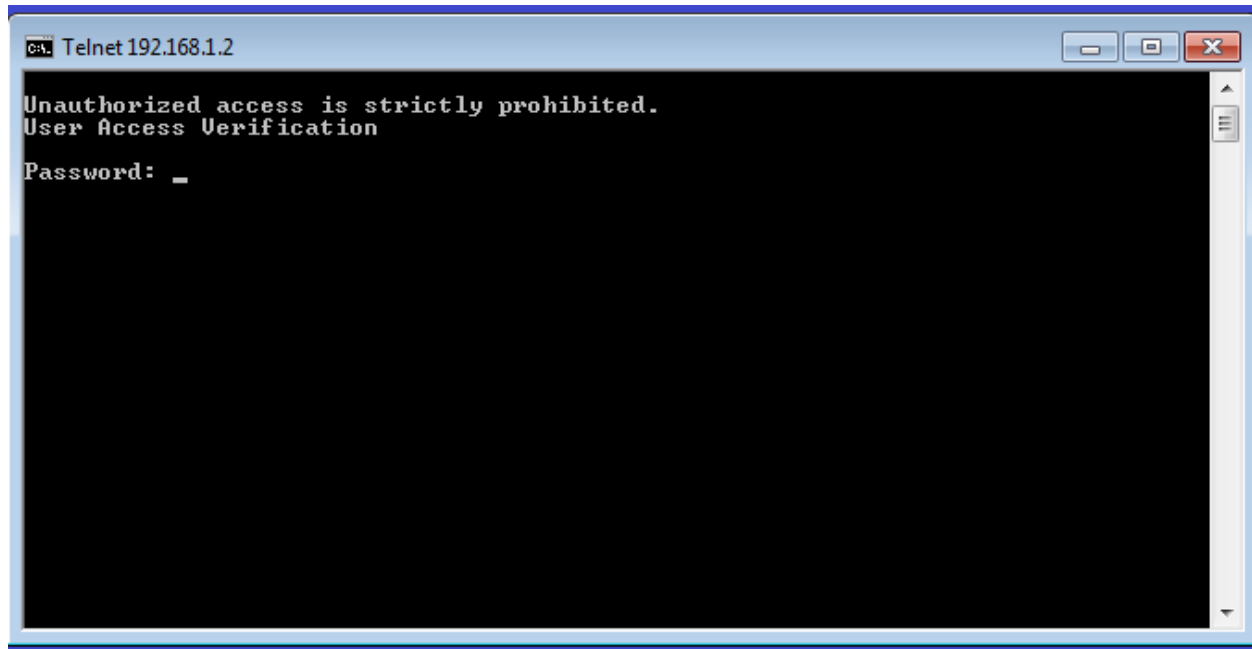
Nota: Windows 7 no admite Telnet en forma nativa. El administrador debe habilitar este protocolo. Para instalar el cliente Telnet, abra una ventana del símbolo del sistema y escriba `pkgmgr /iu:"TelnetClient"`.

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

- a. Con la ventana del símbolo del sistema abierta en la PC-A, emita un comando de Telnet para conectarse al S1 a través de la dirección de administración de SVI. La contraseña es **cisco**.

```
C:\Users\NetAcad> telnet 192.168.1.2
```

El resultado debe ser similar a la siguiente pantalla:



- b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Escriba **enable** en la petición de entrada. Introduzca la contraseña **class** para ingresar al modo EXEC privilegiado y para emitir un comando **show run**.

Paso 4: Guardar el archivo de configuración

- a. Desde la sesión de Telnet, emita el comando **copy run start** en la petición de entrada.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

- b. Salga de la sesión de Telnet escribiendo **quit**. Volverá al símbolo del sistema de Windows 7.

Reflexión

¿Por qué debe usar una conexión de consola para configurar inicialmente el switch? ¿Por qué no conectarse al switch a través de Telnet o SSH?

Todavía no se configuró ningún parámetro de direccionamiento IP. Cuando un switch se pone en servicio por primera vez, no tiene conectividad de red configurada.

Configuraciones de dispositivos

Switch S1 (completo)

```
S1#show run
Building configuration...

!
Current configuration : 1508 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```

```
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
 ip http server
 ip http secure-server
!
 banner motd ^C
 Unauthorized access is strictly prohibited. ^C
!
 line con 0
  password cisco
  login
 line vty 0 4
```

```
password class  
login  
line vty 5 15  
login  
!  
end
```


Enséñenme (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Configurar los parámetros iniciales en un dispositivo de red que utiliza el software Cisco IOS.

- Los estudiantes utilizarán y reforzarán sus conocimientos de la CLI de Cisco IOS al explicarla a otros estudiantes; asimismo, buscarán diferentes maneras de explicar el significado de comandos individuales. Los estudiantes buscarán el grupo óptimo de comandos que se deba utilizar al configurar un dispositivo, a fin de minimizar la cantidad necesaria de cambios de modos durante la configuración.

Información básica/Situación

(Los estudiantes trabajarán de a dos. En esta actividad, se requiere el uso de Packet Tracer).

Suponga que un colega nuevo le pidió que lo oriente sobre la CLI de Cisco IOS. Este colega nunca trabajó con dispositivos Cisco.

Usted le explica los comandos y la estructura básicos de la CLI, porque desea que su colega comprenda que la CLI es un lenguaje de comandos simple pero eficaz que se puede comprender y navegar fácilmente.

Utilice Packet Tracer y una de las actividades disponibles en este capítulo como modelo de red simple (por ejemplo, la actividad de laboratorio 2.3.3.5. Práctica de laboratorio: Configuración de una dirección de administración del switch). Céntrese en estas áreas:

- Si bien los comandos son técnicos, ¿se asemejan a enunciados del lenguaje corriente?
- ¿Cómo se organiza el conjunto de comandos en subgrupos o modos? ¿Cómo sabe un administrador qué modo está utilizando?
- ¿Cuáles son los comandos individuales para configurar los parámetros básicos de un dispositivo Cisco? ¿Cómo explicaría este comando en un lenguaje sencillo? Establezca paralelos con la vida real cuando sea adecuado.

Sugiera cómo agrupar distintos comandos según sus modos de manera que se necesite una cantidad mínima de desplazamientos entre modos.

Notas para el instructor: esta actividad de creación de modelos puede utilizarse como una asignación con calificación. Sin embargo, su objetivo es ayudar a los estudiantes a reflejar el conocimiento adquirido en el capítulo 2 y centrarse en la forma en que Cisco IOS se utiliza directamente para configurar los dispositivos intermediarios. Si el instructor así lo facilita, se alentará el debate entre los alumnos sobre el trabajo de cada uno.

Recursos necesarios

- Packet Tracer
- Cualquier actividad del modelo de red simple disponible del capítulo 2

Reflexión

- Después de completar el capítulo 2, ¿considera que comprende concretamente lo que Cisco IOS hace y cómo funciona? ¿Cuáles fueron algunas de las dificultades que encontró al explicar los comandos y la estructura básicos de la CLI a su colega? Si fuera un “colega nuevo”, ¿cuáles serían algunas de las dificultades que tendría al aprender los comandos y la estructura básicos de la CLI?

2. Responda las siguientes preguntas y analice las respuestas con toda la clase:

- a) Si bien los comandos son técnicos, ¿se asemejan a enunciados del lenguaje corriente?
- b) ¿Cómo se organiza el conjunto de comandos en subgrupos o modos? ¿Cómo sabe un administrador qué modo está utilizando?
- c) ¿Cuáles son los comandos individuales para configurar los parámetros básicos de un dispositivo Cisco? ¿Cómo explicaría este comando en un lenguaje sencillo? Establezca paralelos con la vida real cuando sea adecuado.
- d) Con la ayuda de su colega, intente sugerir cómo agrupar diversos comandos según sus modos, de manera que sea necesario realizar una cantidad mínima de desplazamientos entre modos.

Las respuestas varían (a continuación, se representan las variaciones basadas en el contenido del capítulo 2):

- a) Si bien los comandos son técnicos, ¿se asemejan a enunciados del lenguaje corriente?
Seguro. Las palabras clave como enable, password, banner, address y shutdown son las palabras habituales cuyo significado en la CLI se adapta correctamente, aunque siguen teniendo gran relevancia en su uso habitual.
- b) ¿De qué manera está organizado el conjunto de comandos en subconjuntos o modos? ¿Cómo sabe un administrador qué modo está utilizando en ese momento?

Primero, el nivel de acceso a la CLI puede ser un nivel de usuario (EXEC del usuario) o un nivel de administrador (EXEC privilegiado). En el nivel de administrador, se puede acceder al modo de configuración que está dividido internamente en modo de configuración global, modo de configuración de línea, modo de configuración de interfaz y otros modos, según sea necesario. El modo actual se informa al administrador a través de la petición de entrada, donde el símbolo > representa el nivel de acceso del usuario; # representa el nivel de acceso del administrador, y las palabras clave optativas entre paréntesis designan el modo de configuración y los submodos posibles.

- c) ¿Cuáles son los comandos individuales para acceder y configurar los parámetros básicos de un dispositivo Cisco? ¿Cómo explicaría estos comandos en términos sencillos? Establezca paralelos con la vida real cuando sea adecuado.

enable: tener autorización para ejercer el control total sobre un dispositivo.

configure terminal: iniciar el editor de configuración y aceptar los cambios que provienen de la terminal.

hostname: asignar un nombre a un dispositivo.

service password encryption: hace que el dispositivo oculte todas las contraseñas introducidas en la configuración para que no puedan revelarse.

line con 0: introducir la configuración de la línea, o el "socket", que tiene la etiqueta CONSOLE 0 en el dispositivo y que se utiliza para administrar el dispositivo.

line vty 0 4: introducir la configuración de cinco "sockets" virtuales que permitan la administración remota del dispositivo a través de la red.

password: configurar una contraseña que se utilizará para acceder al dispositivo.

login: proteger el acceso mediante un procedimiento de inicio de sesión que requiere una contraseña definida mediante el comando password.

exit: salir del modo actual para ir al modo ubicado en un nivel superior.

enable secret: frase secreta que protege el uso del comando enable.

banner: mensaje que se muestra a un usuario que intenta acceder el dispositivo.

interface Vlan 1: ingresar al modo de configuración de la interfaz denominada Vlan1.

description: asignar un comentario textual a una interfaz para ayudar al administrador a saber cuál es el propósito y la ubicación de la interfaz.

ip address: asignar una dirección IP numérica a una interfaz.

no shutdown: eliminar el comando shutdown y, de esta manera, crear una interfaz activa.

end: salir del editor de configuración.

Moverse por la configuración y realizar cambios en los parámetros del dispositivo es como transitar por un laberinto. Cada modo de configuración se parece a un sendero del laberinto. Aunque conozca el mapa del laberinto, puede atravesarlo en forma desorganizada y, posiblemente, nunca encontrar la salida. De manera similar, aunque conozca el significado de los comandos individuales y los modos en los que están ubicados, la forma en que se desplaza por estos modos durante la configuración de un dispositivo depende principalmente de usted.

- d) Con la ayuda de su colega, intente sugerir cómo agrupar diversos comandos según sus modos, de manera que sea necesario realizar una cantidad mínima de desplazamientos entre modos.

Una de las posibles secuencias de comandos eficaces para configurar un dispositivo es la siguiente:

```
enable
configure terminal
hostname AtlantaSw
service password-encryption
banner login ^

Access to this device permitted only to authorized personnel!

^
enable secret V3ry5ecr3tP4ssw0rd
line con 0
    password 5ecr3tP4ssw0rd
    login
    exit
line vty 0 4
    password 5ecr3tP4ssw0rd
    login
    exit
interface Vlan 1
    ip address 192.0.2.11 255.255.255.0
    no shutdown
end
```

An ineffective way of configuring would be, for example:

```
enable
```

```
configure terminal
line con 0
  password 5ecr3tP4ssw0rd
  exit
hostname AtlantaSw
service password-encryption
line vty 0 4
  password 5ecr3tP4ssw0rd
  exit
banner login ^

Access to this device permitted only to authorized personnel!

^
line con 0
  login
  exit
interface Vlan 1
  ip address 192.0.2.11 255.255.255.0
  exit
line vty 0 4
  login
  exit
enable secret V3ry5ecr3tP4ssw0rd
interface Vlan 1
  no shutdown
end
```

(Observe que, si bien las dos configuraciones conducen al mismo conjunto de parámetros, la segunda configuración es ligeramente más larga [debido a que se ingresó a modos individuales reiteradas veces] y es muy difícil de seguir, ya que el flujo de comandos es prácticamente aleatorio y no sigue la secuencia lógica ni las instrucciones comunes para los modos).

Identifique los elementos del modelo que corresponden a contenido de TI:

- Comandos
- Modos
- Orientación eficaz en el modo de configuración
- Habilidades de relaciones con los clientes en el mundo real

Solo hablemos de esto... (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la función de los protocolos y de los organismos de estandarización para facilitar la interoperabilidad en las comunicaciones de red.

- Los estudiantes determinarán formas de comunicarse cuando no hay normas presentes o acordadas. También resolverán un problema de comunicación mediante el establecimiento de normas.

Información básica/Situación

Acaba de adquirir un automóvil nuevo para uso personal. Después de conducir el automóvil durante alrededor de una semana, descubre que no funciona correctamente.

Después de analizar el problema con varios de sus compañeros, decide llevarlo a un taller de reparaciones de automóviles que le recomendaron mucho. Se trata del único taller de reparaciones que le queda cerca.

Cuando llega al taller de reparaciones, advierte que todos los mecánicos hablan otro idioma. Tiene dificultades para explicar los problemas de funcionamiento del automóvil, pero es realmente necesario realizar las reparaciones. No está seguro de poder conducirlo de regreso a su hogar para buscar otras opciones.

Debe encontrar una manera de trabajar con el taller para asegurarse de que el automóvil se repare correctamente.

¿Cómo se comunicará con los mecánicos de esa empresa? Diseñe un modelo de comunicaciones para asegurar que el vehículo se repare correctamente.

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la manera en que un sistema de comunicación facilita la transferencia de datos de origen a destino (en persona y en la práctica empresarial). Como resultado de esta actividad, se iniciará un debate.

Reflexión

1. ¿Qué pasos identificó como importantes para comunicar su solicitud de reparación? Justifique su respuesta.

Algunos pasos para resolver este problema podrían incluir los siguientes:

Establecer un lenguaje para la comunicación (puede ser oral o escrito, o cenestésico o físico).

Explicar, con mucho cuidado y en pequeños pasos, el problema que se experimentó con el automóvil (una vez más, mediante la representación oral, escrita, con imágenes, o cenestésica o física).

Solicitarle al mecánico que confirme su comprensión del problema.

Esperar que se realice la reparación.

Conducir el vehículo para asegurar la reparación correcta.

Finalizar el encuentro pagando por las reparaciones y agradeciendo al mecánico.

Identifique los elementos del modelo que corresponden a contenido de TI:

- Establecimiento de un idioma para comunicarse (protocolo de aplicación)

- División del mensaje en pequeños pasos para facilitar la comprensión en partes del problema que se debe resolver (protocolo de transferencia)
- Corroboración de si el mensaje se entregó al mecánico que realizará las reparaciones y de si lo entendió correctamente (protocolo de Internet)
- Entrega del automóvil y tiempo de espera para la realización de las reparaciones (protocolo de acceso a la red)

Práctica de laboratorio: Investigación de estándares de redes

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Investigar organismos de estandarización de redes

- Reunir información sobre los principales organismos de estandarización de redes realizando una búsqueda del tesoro mientras navega por la Web.
- Identificar las características importantes de algunos de los organismos.

Parte 2: Reflexionar sobre las experiencias de Internet y redes informáticas

- Reflexionar sobre la forma en que los distintos organismos de estandarización de redes mejoran la experiencia de Internet y redes informáticas.

Información básica/Situación

Con la ayuda de motores de búsqueda como Google, investigue las organizaciones sin fines de lucro que son responsables de establecer estándares internacionales para Internet y el desarrollo de tecnologías de Internet.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Investigar organismos de estandarización de redes

En la parte 1, identificará algunos de los organismos principales de estandarización y características importantes de estos, como la cantidad de años en existencia, la cantidad de miembros, personalidades históricas importantes, algunas de las responsabilidades y obligaciones, el rol de supervisión organizativa y la ubicación de la sede central de la organización.

Utilice un explorador Web o sitios Web de diversas organizaciones para buscar información sobre los siguientes organismos y las personas que jugaron un papel decisivo en mantenerlos.

Para obtener las respuestas a las siguientes preguntas, busque los términos y acrónimos de las siguientes organizaciones: ISO, ITU, ICANN, IANA, IEEE, EIA, TIA, ISOC, IAB, IETF, W3C, RFC y Wi-Fi Alliance.

1. ¿Quién es Jonathan B. Postel y por qué es conocido? (Ayuda de búsqueda: Jon Postel)

Jonathan Postel fue un informático estadounidense que hizo importantes contribuciones al desarrollo de los estándares de Internet, a la creación de la Internet Assigned Numbers Authority (IANA) y como editor de RFC.

2. ¿Cuáles son los dos organismos relacionados responsables de administrar el espacio de nombres de dominio de nivel superior y los servidores de nombres de raíz del Sistema de nombres de dominios (DNS) en Internet? (Ayuda de búsqueda: ICANN, IANA)

International Corporation for Assigned Names and Numbers (ICANN) e Internet Assigned Numbers Authority (IANA)

3. Vinton Cerf fue nombrado uno de los padres capitales de Internet. ¿Qué organismos de Internet presidió o contribuyó a fundar? ¿Qué tecnologías de Internet ayudó a desarrollar? (Ayuda de búsqueda: Vint Cerf, IAB, ISOC, ICANN)

Vinton Cerf cofundó la Internet Society (ISOC) con Bob Kahn en 1992, colaboró en la creación de ICANN y presidió el Internet Architecture Board (IAB) desde 1989 hasta 1991.

4. ¿Qué organismo es responsable de publicar la solicitud de comentarios (RFC)? (Ayuda de búsqueda: IETF)

Internet Engineering Task Force (IETF)

5. ¿Qué tienen en común RFC 349 y RFC 1700? (Ayuda de búsqueda: Solicitud de comentarios, Google, RFC 349, RFC 1700)

Números de puerto. La lista actual se puede encontrar en <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

6. ¿Qué número de RFC es ARPAWOCKY? ¿Qué es? (Ayuda de búsqueda: Solicitud de comentarios, Google, ARPAWOCKY)

RFC 527. La primera RFC humorística que luego llevó al IETF a iniciar, en 1989, la RFC del día de los inocentes.

7. ¿Quién fundó el World Wide Web Consortium (W3C)? (Ayuda de búsqueda: W3C)

Lo fundó Tim Berners-Lee en el MIT.

8. Nombre 10 estándares de World Wide Web (WWW) que el W3C desarrolla y mantiene. (Ayuda de búsqueda: W3C)

Algunos ejemplos: interfaz de gateway común (CGI), modelo de objetos de documento (DOM), lenguaje de marcado de hipertexto (HTML), lenguaje de marcado extensible (XML)

9. ¿Dónde está ubicada la sede central del Instituto de Ingenieros en Electricidad y Electrónica (IEEE) y qué importancia tiene su logotipo? (Ayuda de búsqueda: IEEE)

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE) tiene su sede central en la ciudad de Nueva York, Nueva York, Estados Unidos. El logotipo del IEEE es un diseño en forma de diamante que ilustra la regla de la mano derecha dentro de la cometa de Benjamín Franklin.

10. ¿Cuál es el estándar IEEE para el protocolo de seguridad de acceso protegido Wi-Fi 2 (WPA2)? (Ayuda de búsqueda: WPA2)

WPA2 está basado en el estándar IEEE 802.11i. Normalmente, se utiliza en la red inalámbrica Wi-Fi.

11. ¿Wi-Fi Alliance es un organismo de estandarización sin fines de lucro? ¿Cuál es su objetivo? (Ayuda de búsqueda: Wi-Fi Alliance)

Sí, Wi-Fi Alliance es una asociación comercial sin fines de lucro, y sus objetivos son asegurar la interoperabilidad y la compatibilidad con las versiones anteriores y respaldar las innovaciones.

12. ¿Quién es Hamadoun Touré? (Ayuda de búsqueda: UIT)

Hamadoun Touré, de Mali, es el secretario general de la Unión Internacional de Telecomunicaciones (UIT).

13. ¿Qué es la Unión Internacional de Telecomunicaciones (UIT) y dónde está ubicada su sede central? (Ayuda de búsqueda: UIT)

La UIT es un organismo de las Naciones Unidas dedicado a las tecnologías de información y comunicación. La sede central de la UIT se encuentra en Ginebra, Suiza.

14. Nombre los tres sectores de la UIT. (Ayuda de búsqueda: UIT)

Los tres sectores de la UIT son los siguientes: Radiocomunicación, Estandarización y Desarrollo.

15. ¿Qué significa RS en RS-232 y qué organismo lo introdujo? (Ayuda de búsqueda: EIA)

RS significa estándar recomendado. El RS-232 fue introducido por la sección Radio de la Electronic Industries Alliance (EIA).

16. ¿Qué es SpaceWire? (Ayuda de búsqueda: Spacewire, IEEE)

SpaceWire es un estándar de redes y enlaces de comunicación de alta velocidad que se usa en vehículos espaciales.

17. ¿Cuál es la misión de la ISOC y dónde está ubicada su sede central? (Ayuda de búsqueda: ISOC)

La sede central de la Internet Society (ISOC) se encuentra en Reston, Virginia, y en Ginebra, Suiza. Su misión es “asegurar el desarrollo, la evolución y el uso abiertos de Internet en beneficio de todas las personas del mundo”.

18. ¿Qué organismos supervisa el IAB? (Ayuda de búsqueda: IAB)

El IAB supervisa el Internet Engineering Task Force (IETF) y el Internet Research Task Force (IRTF).

19. ¿Qué organismo supervisa el IAB? (Ayuda de búsqueda: IAB, ISOC)

La ISOC supervisa el IAB.

20. ¿Cuándo se fundó la ISO y dónde está ubicada su sede central? (Ayuda de búsqueda: ISO)

La International Organization for Standardization (ISO) se fundó en 1947 y su sede central se encuentra en Ginebra, Suiza.

Parte 2: Reflexionar sobre las experiencias de Internet y redes informáticas

Tómese un momento para pensar acerca de Internet hoy en día en relación con los organismos y las tecnologías que acaba de investigar. Luego, responda las siguientes preguntas.

1. ¿De qué manera los estándares de Internet permiten un mayor comercio? ¿Qué posibles problemas podríamos tener si no contáramos con el IEEE?

Cada compañía desarrollaría sus propios protocolos y productos, que podrían no funcionar con los equipos de terceros.

2. ¿Qué posibles problemas podríamos tener si no contáramos con el W3C?

No tendríamos un idioma “común” en Internet para mostrar la información y comunicarnos.

3. ¿Cómo podemos aprender del ejemplo de Wi-Fi Alliance con respecto a la necesidad de estándares de redes?

El hecho de que los fabricantes de equipos sigan los mismos estándares o reglas permite la interoperabilidad y compatibilidad con versiones anteriores. Esto fomenta la competencia, ofrece opciones a los consumidores y alienta a los fabricantes a crear mejores productos.

Práctica de laboratorio: Investigación de RFC

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Editor de RFC

- Navegar hasta el editor de RFC.
- Buscar RFC utilizando palabras clave.
- Encontrar RFC según el estado.
- Buscar RFC humorísticas.

Parte 2: Publicación de RFC

Información básica/Situación

En 1969, Steve Crocker creó la solicitud de comentarios (RFC) con el objetivo de ayudar a registrar notas sobre el desarrollo de la Advanced Research Projects Agency Network (ARPANET), que finalmente evolucionó en una colección oficial de memorándums que describe los temas relacionados principalmente con Internet y la suite de protocolos TCP/IP. Actualmente, las RFS son administradas por el IETF. Actualmente, hay más de 6000 RFC, y la lista completa está disponible en <http://www.ietf.org/download/rfc-index.txt>.

En esta práctica de laboratorio, aprenderá cómo el IETF publica una RFC en la actualidad. Además, identificará algunas RFC conocidas que se utilizan en la red. Asimismo, puede encontrar algunas RFC no técnicas que pueden proporcionar información o humor ingenieril.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Editor de RFC

Las RFC comenzaron como una colección de memorándums sobre el desarrollo de la primera Internet (ARPANET). En esta colección, solo algunas RFC se consideran estándares de Internet. La mayoría describe protocolos experimentales y algunas son solo informativas. El propósito principal de las RFC es estimular los comentarios y el debate.

Paso 1: Navegar hasta el editor de RFC.

Todas las RFC publicadas están disponibles para consultarlas en <http://www.rfc-editor.org>. El editor de RFC es un repositorio de RFC que mantiene el IETF.

En el mensaje de aviso superior de esta página, puede hacer clic en cualquiera de los enlaces; estos lo dirigen a las diversas búsquedas, bases de datos y tipos de información. En este mensaje de aviso de color azul, también se incluye un enlace a la **página de inicio del IETF**.

Al ubicar una RFC, tiene acceso al texto completo del documento.

Paso 2: Buscar RFC utilizando palabras clave.

- a. Abra un explorador y navegue hasta <http://www.rfc-editor.org>. En la página de inicio del editor de RFC, puede buscar y recuperar RFC y demás información relacionada con Internet.



- b. En el panel **Finding and Retrieving RFCs. etc.** (Buscar y recuperar RFC, etc.), los enlaces pueden ayudarlo a buscar RFC mediante distintos métodos. En el enlace **Search for an RFC and its meta-data** (Buscar una RFC y sus metadatos), se muestra una lista de RFC después de introducir parámetros de búsqueda, como número, autor, título o palabra clave. En el ejemplo siguiente, se utiliza la palabra **pop**.

[About this page](#)

Additional Criteria

Status:

☒ Any

☐ Standards

Track :: Any

☐ Best Current Practice

☐ Informational

☐ Experimental

☐ Historic

☐ Unknown

Publication Date:

Range (inclusive):

From Month Year

To Month Year

Stream: Any

Area: Any

WG Acronym:

Author (last name):

Abstract contains:

Search Clear all

RFC Number (or Subseries Number):

Title/Keyword: pop

Search

☐ Show Abstract ☐ Show Keywords

21 results

Number	Files	Title	Authors	Date	More Info	Status
RFC 937	ASCII , PDF	Post Office Protocol: Version 2	M. Butler, J. Postel, D. Chase, J. Goldberger, J.K. Reynolds	February 1985	Obsoletes RFC 918	Historic
RFC 1725	ASCII , PDF	Post Office Protocol - Version 3	J. Myers, M. Rose	November 1994	Obsoletes RFC 1460 , Obsoleted by RFC 1939 , Errata	Internet Standard (was published as Draft Standard)
RFC 1734	ASCII , PDF	POP3 AUTHentication command	J. Myers	December 1994	Obsoleted by RFC 5034	Proposed Standard
RFC 1939 part of STD 53	ASCII , PDF	Post Office Protocol - Version 3	J. Myers, M. Rose	May 1996	Obsoletes RFC 1725 , Updated by RFC 1957 , RFC 2449 , RFC 6186 , Errata	Internet Standard

En la lista, busque **Post Office Protocol – Version 3** (Protocolo de oficina de correos, versión 3). El número de RFC asociado es **RFC 1939**. Esta RFC también es un estándar de Internet, como lo indica el número STD en la columna **Number** (Número).

Después de publicar una RFC y de asignarle un número, esta no puede cambiarse, y el número de RFC nunca se vuelve a usar para una RFC más nueva. Por ejemplo, en la columna **More Info** (Más información), la RFC 1939 volvió obsoleta la RFC 1725 anterior. La información de la RFC 1725 no se modificó, pero se reemplazó por la información de la RFC 1939. La RFC 1939 se actualizó con las RFC 1957, 2449 y 6186, como se indica en la columna **More Info**. Si hace clic en cualquiera de estos enlaces, se muestra el texto completo de la RFC.

Consulte la columna **Status** (Estado) y ubique el estado **Proposed Standard** (Estándar propuesto). Pueden ser técnicamente correctas, pero requerir prueba y validación adicionales.

Consulte la columna **Status** y ubique el estado **Informational** (Informativa). Las RFC informativas pueden ser de técnicas a humorísticas. Por ejemplo, la RFC 0035 (Network Meeting [Reunión sobre la red]) proporciona un enfoque sobre el desarrollo de un protocolo de red en los primeros días de Internet.

Paso 3: Encontrar RFC según el estado.

Para buscar una lista de RFC que sean estándares de Internet (STD) o para buscarlas por su estado, realice las siguientes tareas:

- Navegue de vuelta hasta la página de inicio del editor de RFC.
- Haga clic en el enlace **Official Internet Protocol Standard RFCs** (RFC de estándares oficiales de protocolos de Internet), en la columna izquierda. Encontrará una lista de RFC de estándares oficiales, seguida por otras listas de estados de RFC. Cada enlace de RFC lleva al texto completo de la RFC determinada.

Official Internet Protocol Standards

This page shows the current definitions of STD and BCP numbers. It also lists those standards-track and BEST CURRENT PRACTICE RFCs that have not been obsoleted, as well as current EXPERIMENTAL and HISTORIC RFCs.

RFC numbers more recent than Nov 2007 are starred.

Results are as of Nov-15-2012

Standards Ordered by STD #	Standards Ordered by RFC #
Draft Standards	
Proposed Standards	
Best Current Practice by BCP #	Best Current Practice by RFC #
Experimental RFCs	
Historic RFCs	

[Return to Finding&Retrieving Page](#) [Go to RFC Editor home page](#)

< STANDARDS Ordered by STD > Back to Top			
Mnemonic	Title	RFC#	STD#
-----	[Reserved for Assigned Numbers. See RFC 1700 and RFC 3232 .]	xxx	2
-----	Requirements for Internet Hosts - Communication Layers	1122	3
-----	Requirements for Internet Hosts - Application and Support	1123	3

Paso 4: Buscar RFC humorísticas.

También se puede encontrar humor ingenieril en las RFC, como en la RFC 1300 (Remembrances of Things Past [Recuerdos del pasado]). Para buscar información sobre las RFC, se puede utilizar un motor de búsqueda de Internet.

- Busque "RFC * humor * ingeniería" en Internet para ver más ejemplos de RFC divertidas. ¿Qué descubrió?

Las respuestas varían, pero pueden incluir: entradas de wiki, referencias a la tradición del IETF de lanzar RFC divertidas el día de los inocentes y otras RFC humorísticas.

- Busque la RFC 2795 ¿Cuál es el tema de esta RFC? _____

La suite de protocolos de infinitos monos (IMPS).

¿Para qué compañía trabaja el autor de esta RFC? _____

MonkeySeeDoo, Inc.

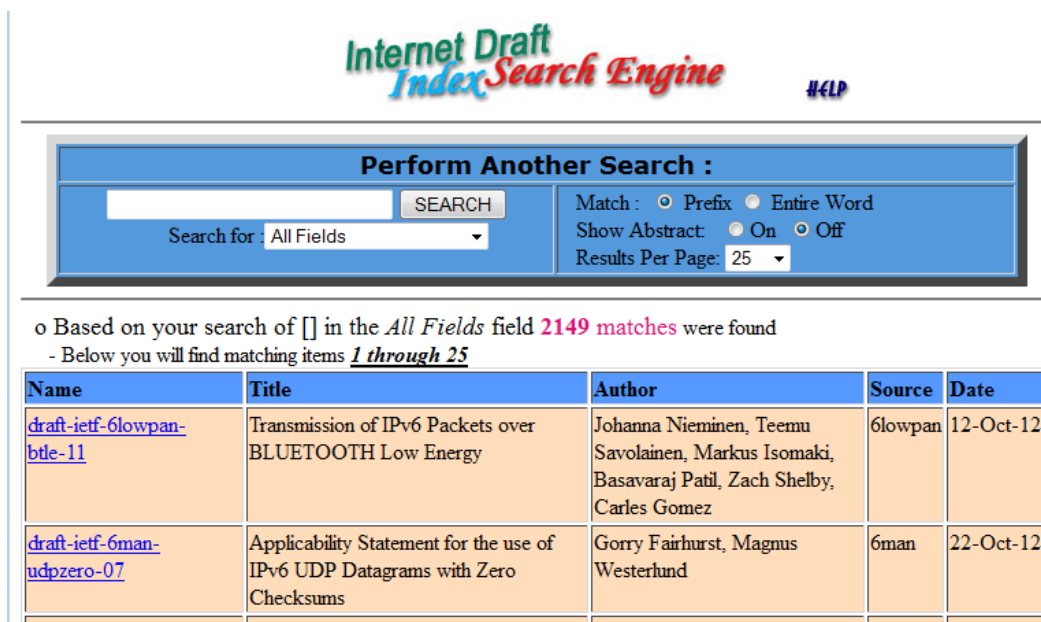
Parte 2: Publicación de RFC

El difunto Dr. Jonathan Postel mantuvo y administró el archivo de RFC durante 28 años (RFC 2468). Actualmente, las RFC son una colección de documentos publicados y administrados por el IETF. El IETF es una gran comunidad internacional abierta de diseñadores, operadores, proveedores e investigadores de redes relacionada con Internet y la suite de protocolos de Internet.

Cualquiera puede enviar una propuesta al editor de RFC para su posible publicación. La propuesta inicialmente se publica como un borrador de Internet (I-D). Una vez que la comunidad la revisa y un editor de RFC la aprueba, entra al mismo proceso de publicación que una presentación del IETF. Para obtener más detalles sobre la presentación independiente, consulte <http://www.rfc-editor.org/indsubs.html>.

Las propuestas que pueden convertirse en un estándar de Internet o en prácticas recomendadas vigentes así como algunas RFC experimentales o informativas se publican como borradores de Internet. Los borradores de Internet están disponibles para su revisión y comentarios informales. No tienen ningún estado formal y están sujetos a cambios o eliminación en cualquier momento. Se los puede encontrar en <http://www.rfc-editor.org/>.

- Navegue hasta <http://www.rfc-editor.org>.
- Haga clic en **I-D Search** (Búsqueda de borrador de Internet) en la parte superior de la página de inicio y, a continuación, haga clic en **SEARCH** (Buscar). Aparece una lista de los borradores de Internet vigentes.



Name	Title	Author	Source	Date
draft-ietf-6lowpan-btle-11	Transmission of IPv6 Packets over BLUETOOTH Low Energy	Johanna Nieminen, Teemu Savolainen, Markus Isomaki, Basavaraj Patil, Zach Shelby, Carles Gomez	6lowpan	12-Oct-12
draft-ietf-6man-udpzero-07	Applicability Statement for the use of IPv6 UDP Datagrams with Zero Checksums	Gorry Fairhurst, Magnus Westerlund	6man	22-Oct-12

La lista de resultados proporciona enlaces al texto completo del I-D y a otra información útil. En la columna **Source** (Origen), se indica el grupo de trabajo del IETF que es responsable del borrador. Como ejemplo, **6man** es un grupo de trabajo que presentó varios borradores. Para obtener más información sobre este grupo de trabajo, haga clic en **IETF HOME** en la parte superior de la página de resultados.

- Al llegar a la página de inicio del IETF, haga clic en **WG Charters** (Procedimientos del grupo de trabajo) en la columna izquierda, debajo de los grupos de trabajo.

Aparece la página Active IETF Working Groups (Grupos de trabajo del IETF activos). La función principal del grupo de trabajo (WG) del IETF es desarrollar pautas y especificaciones del IETF. Muchas de estas pautas y especificaciones pretenden convertirse en estándares o recomendaciones. Al desplazarse por la página, puede ver una lista de los grupos de trabajo activos en diferentes áreas de desarrollo de la tecnología relacionada con redes. El grupo de trabajo **6man** puede encontrarse en la lista Internet Area (Área de Internet). Este grupo de trabajo es responsable del mantenimiento y el avance de la arquitectura de direccionamiento y las especificaciones del protocolo IPv6.

- d. Haga clic en **6man** para ver la lista completa de las propuestas actuales y otra información de este grupo de trabajo.

Una vez que el I-D se somete a una revisión significativa por parte de la comunidad, y esta la considera útil, estable y bien comprendida, se convierte en una propuesta de estándar. El texto completo de la propuesta de estándar se puede encontrar mediante una búsqueda en [RFC-Editor](#) (Editor de RFC). La propuesta de estándar puede convertirse en un estándar de Internet después de la implementación significativa y la experiencia operativa correcta.

Nota: solo algunas RFC que publica el IETF se convierten en estándares de Internet.

Reflexión

1. ¿Por qué las RFC son importantes para el historial y los estándares de Internet?

Como las RFC publicadas nunca se modifican, constituyen un registro escrito de la evolución de los estándares y las prácticas de Internet. Consulte la RFC 2026, The Internet Standards Process, Revision 3 (Proceso de estándares de Internet, revisión 3) para obtener más información sobre las RFC y el proceso de RFC.

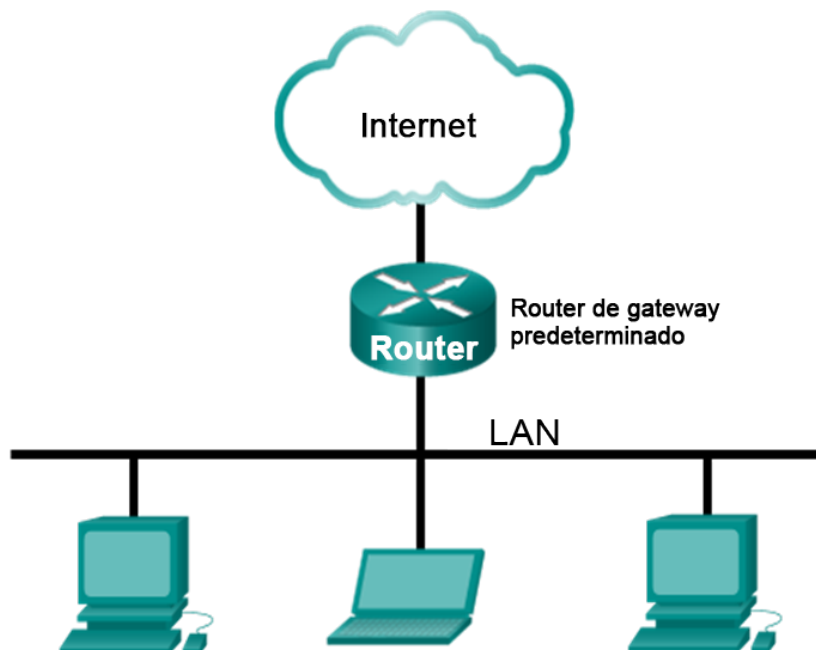
2. ¿Cuáles son las ventajas de las RFC como esfuerzo de colaboración?

Cualquier persona puede contribuir al desarrollo de Internet. La información de las RFC no es de propiedad exclusiva de ninguna compañía; por lo tanto, lo más probable que los equipos de diferentes empresas trabajen juntos.

Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Descargar e instalar Wireshark (Optativo)

Parte 2: Capturar y analizar datos ICMP locales en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts locales.
- Ubicar la información de la dirección MAC y de la dirección IP en las PDU capturadas.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

- Inicie y detenga la captura de datos del tráfico de ping a los hosts remotos.
- Ubicar la información de la dirección MAC y de la dirección IP en las PDU capturadas.
- Explicar por qué las direcciones MAC para los hosts remotos son diferentes de las direcciones MAC para los hosts locales.

Información básica/Situación

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Mientras los streams de datos van y vienen por la red, el programa detector “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con la RFC correcta u otras especificaciones.

Wireshark es una herramienta útil para cualquier persona que trabaje con redes y se puede utilizar con la mayoría de las prácticas de laboratorio en los cursos de CCNA para tareas de análisis de datos y resolución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En esta práctica de laboratorio, usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con acceso a Internet)
- Se utilizarán PC adicionales en una red de área local (LAN) para responder a las solicitudes de ping.

Nota para el instructor: esta práctica de laboratorio supone que el alumno utiliza una PC con acceso a Internet y puede hacer ping a otras PC en la red de área local. Si usa PC de la academia, el instructor puede preferir instalar previamente Wireshark en las PC y recomendar a los alumnos que lean la parte 1 y realicen las partes 2 y 3 de la práctica de laboratorio. El procedimiento de instalación de Wireshark y las capturas de pantalla pueden cambiar según la versión de Wireshark. En esta práctica de laboratorio, se utiliza Wireshark v1.8.3 para Windows 7 (64 bits).

El uso de un programa detector de paquetes como Wireshark se puede considerar una infracción de la política de seguridad del lugar de estudios. Se recomienda obtener permiso para realizar esta práctica de laboratorio antes de ejecutar Wireshark. Si el uso de un programa detector de paquetes como Wireshark constituye un problema, se sugiere que el instructor asigne la práctica de laboratorio como tarea para el hogar o realice una demostración explicativa.

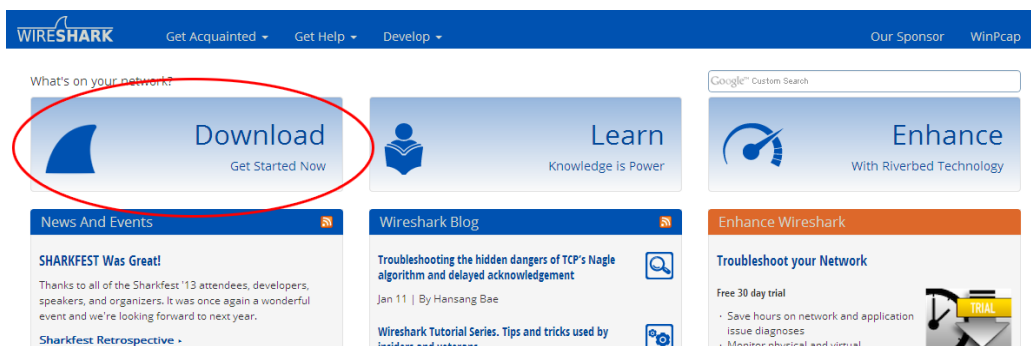
Parte 1: Descargar e instalar Wireshark (optativo)

Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux. En la parte 1 de esta práctica de laboratorio, descargará e instalará el programa de software Wireshark en la PC.

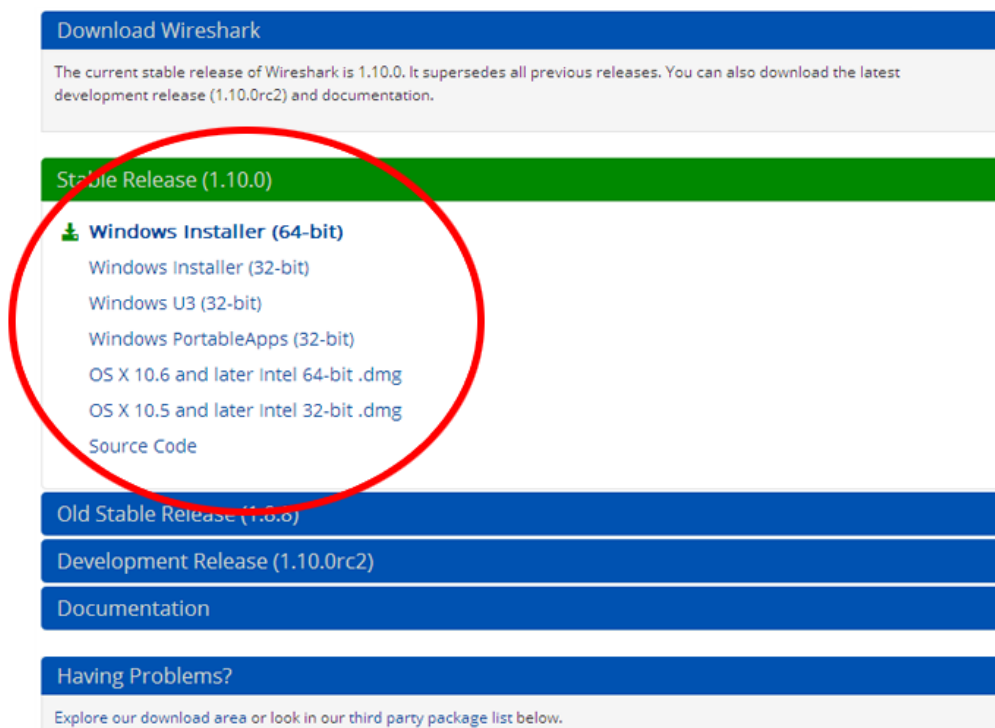
Nota: si Wireshark ya está instalado en la PC, puede saltar la parte 1 e ir directamente a parte 2. Si Wireshark no está instalado en la PC, consulte con el instructor acerca de la política de descarga de software de la academia.

Paso 1: Descargar Wireshark

- Wireshark se puede descargar de www.wireshark.org.
- Haga clic en **Download Wireshark** (Descargar Wireshark).



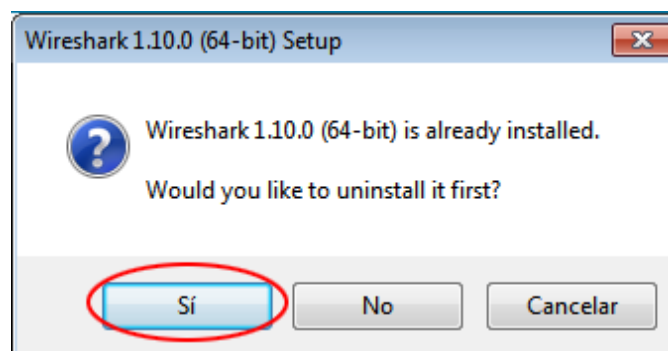
- c. Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione **Windows Installer (64-bit)** (Instalador de Windows [64 bits]).



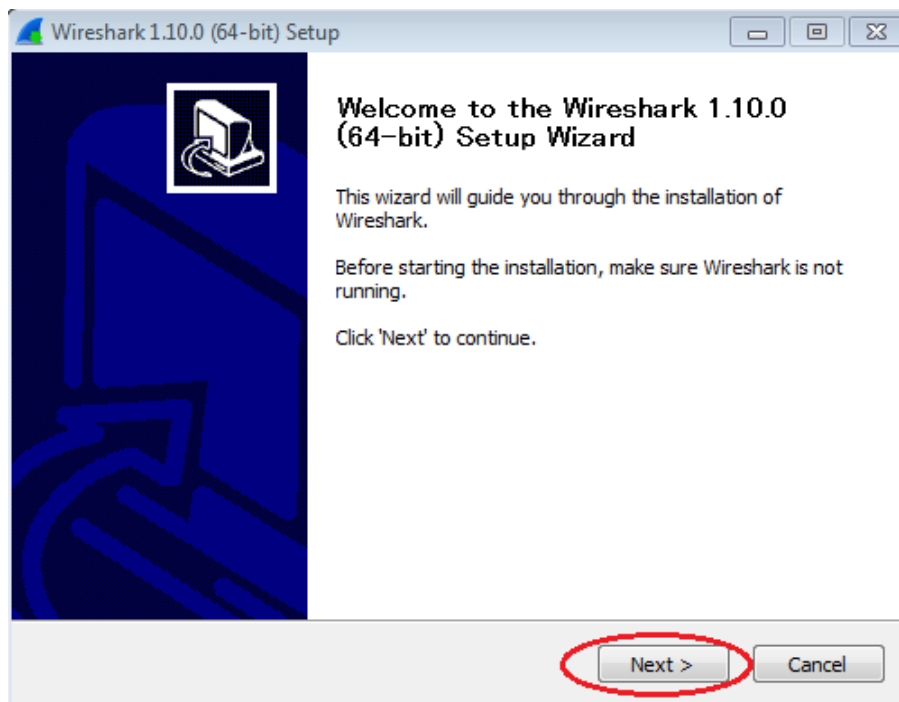
Después de realizar la selección, comienza la descarga. La ubicación del archivo descargado depende del explorador y del sistema operativo que utiliza. Para usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas**.

Paso 2: Instalar Wireshark

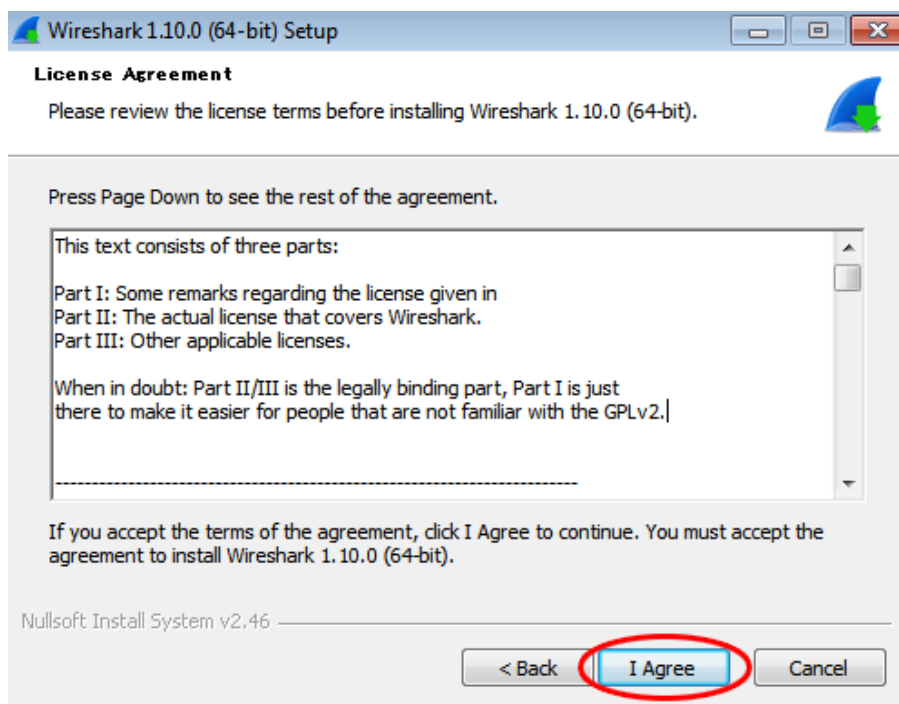
- a. El archivo descargado se denomina **Wireshark-win64-x.x.x.exe**, en el que **x** representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.
- b. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí** para desinstalar la versión anterior de Wireshark.



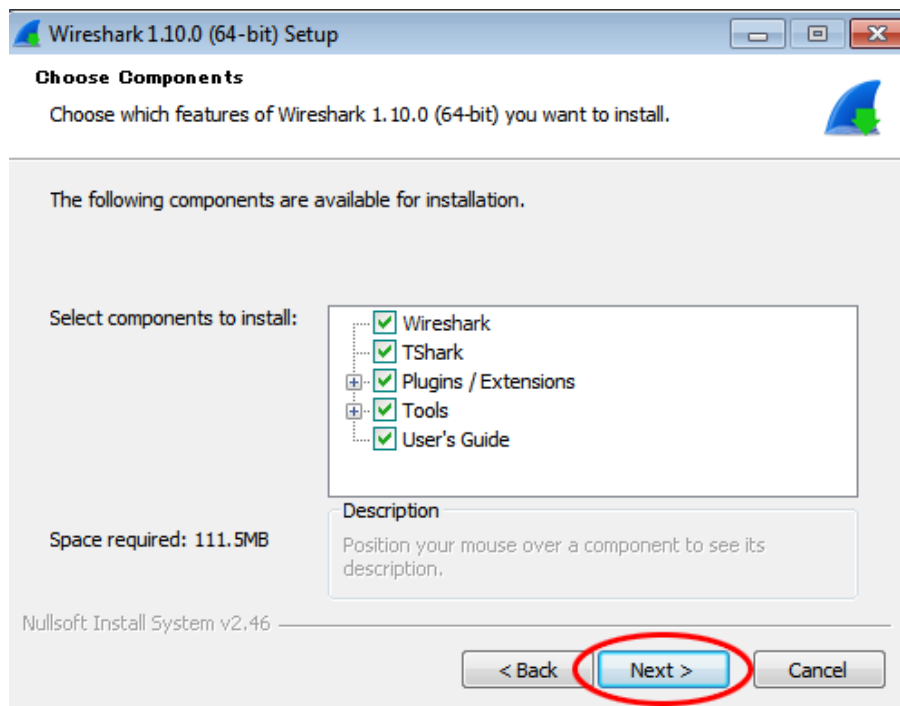
- c. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Next** (Siguiente).



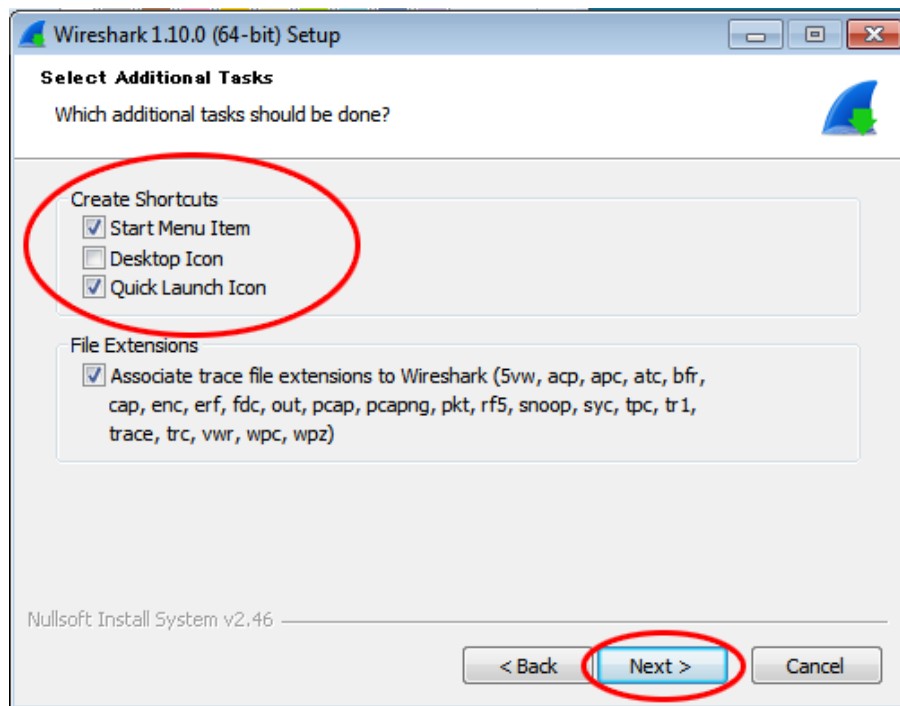
- d. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement (Contrato de licencia), haga clic en **I agree** (Acepto).



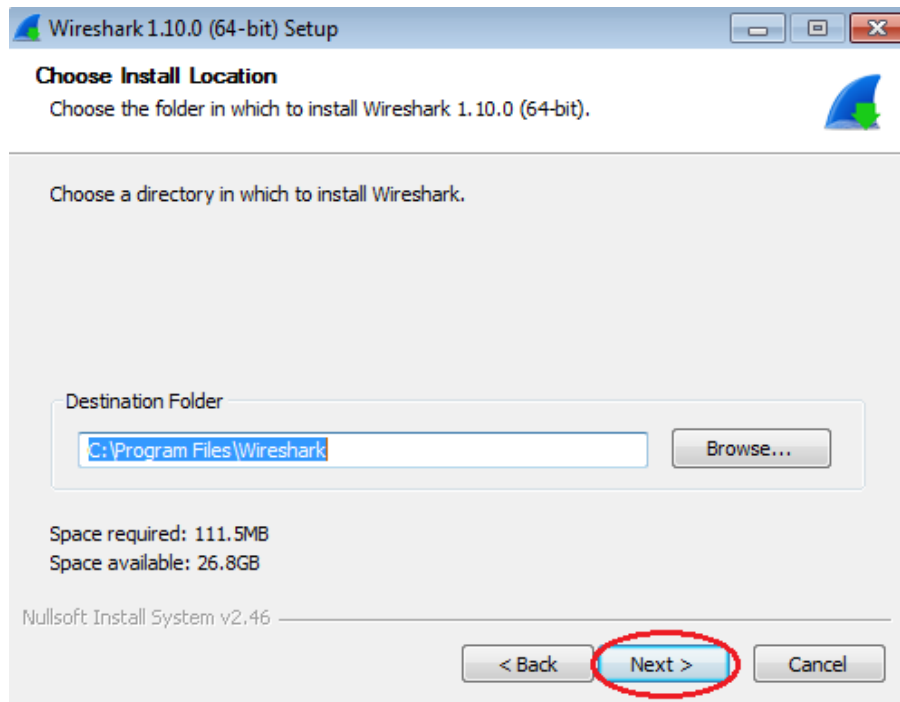
- e. Guarde la configuración predeterminada en la ventana Choose Components (Elegir componentes) y haga clic en **Next** (Siguiente).



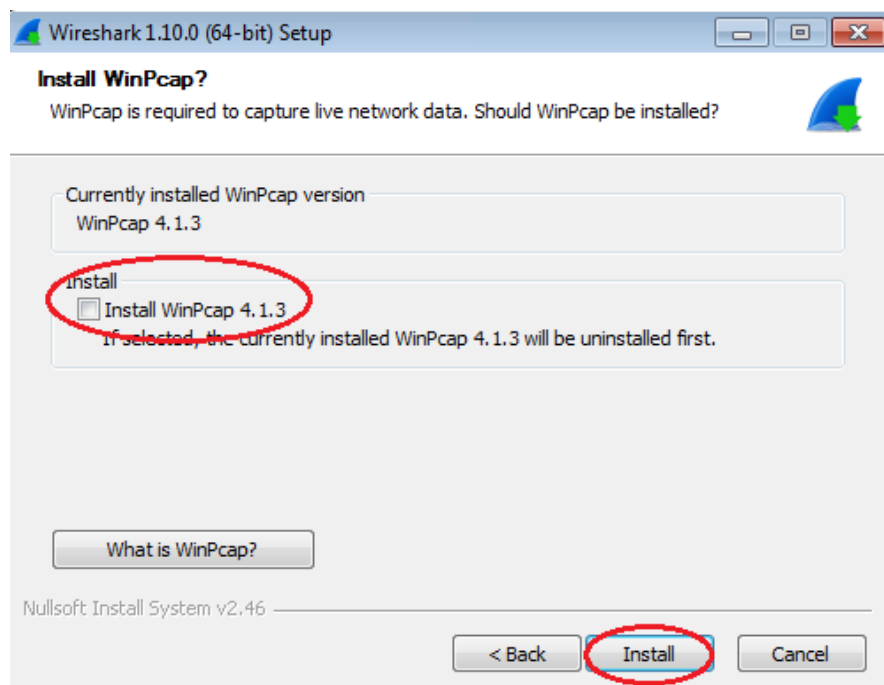
- f. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Next** (Siguiente).



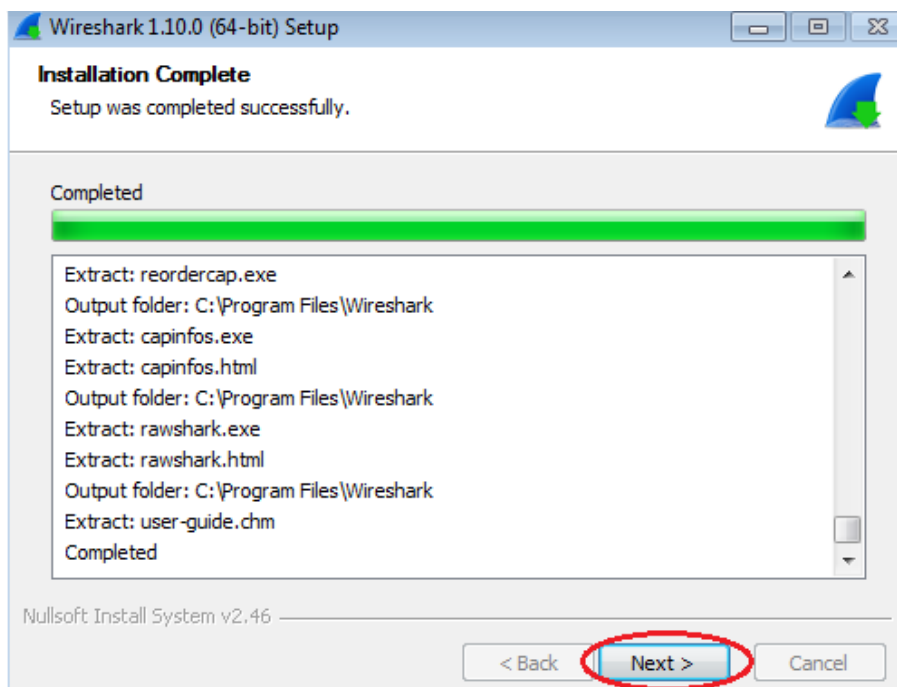
- g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.



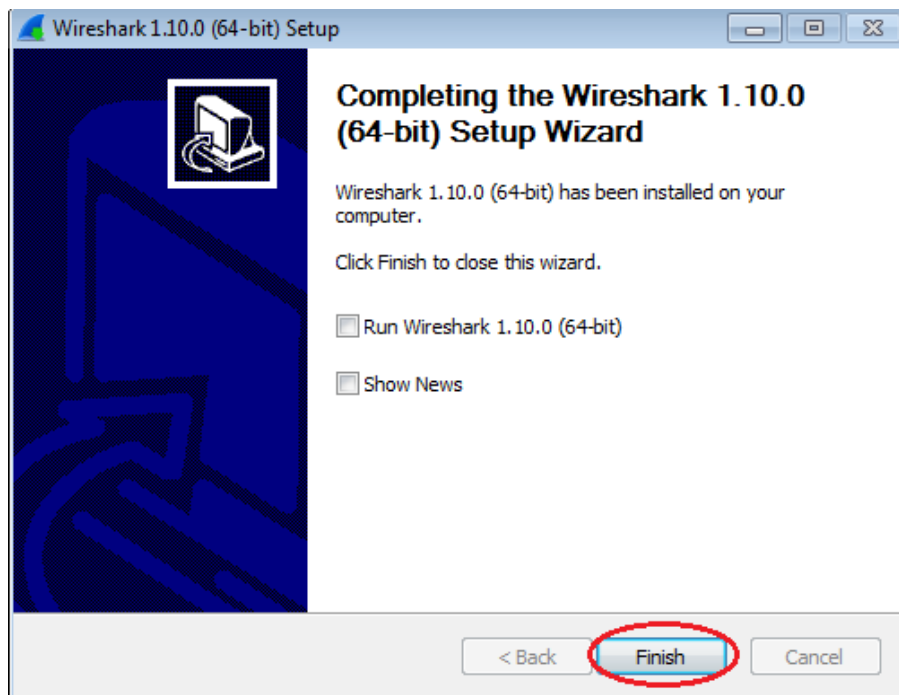
- h. Para capturar datos de la red activa, WinPcap debe estar instalado en la PC. Si WinPcap ya está instalado en la PC, la casilla de verificación **Install** (Instalar) estará desactivada. Si la versión instalada de WinPcap es anterior a la versión que incluye Wireshark, se recomienda que permita que la versión más reciente se instale haciendo clic en la casilla de verificación **Install WinPcap x.x.x** (Instalar WinPcap [número de versión]).
- i. Finalice el asistente de instalación de WinPcap si instala WinPcap.



- j. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Next** (Siguiente) cuando la instalación esté completa.



- k. Haga clic en **Finish** (Finalizar) para completar el proceso de instalación de Wireshark.



Parte 2: Capturar y analizar datos ICMP locales en Wireshark

En la parte 2 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

- Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Entrar.
- Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.

```
C:\Windows\system32\cmd.exe
G:\>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : PC-A
Sufijo DNS principal . . . . : 
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . : jonckers.be
Descripción . . . . . : Intel(R) 82566DM-2 Gigabit Network
Dirección física. . . . . : 00-0C-29-CE-91-82
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::a4de:a76e:64a1:e650%11<Preferido>

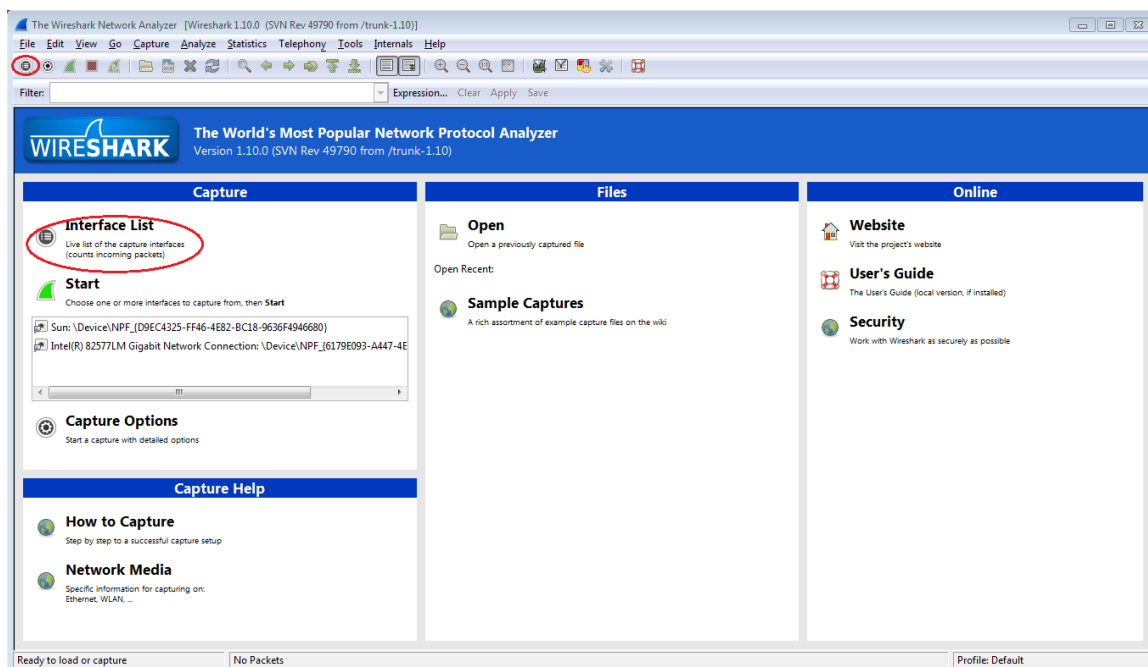
Dirección IPv4. . . . . : 10.84.9.65<Preferido>
Máscara de subred . . . . . : 255.255.0.0
```

- Solicite a un miembro del equipo la dirección IP de su PC y proporcione la suya. En esta instancia, no proporcione su dirección MAC.

Paso 2: Iniciar Wireshark y comenzar a capturar datos

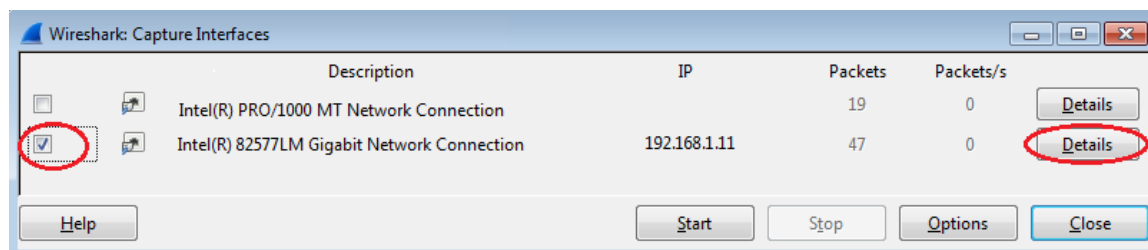
- En la PC, haga clic en el botón **Inicio** de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en **Wireshark**.

- b. Una vez que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).

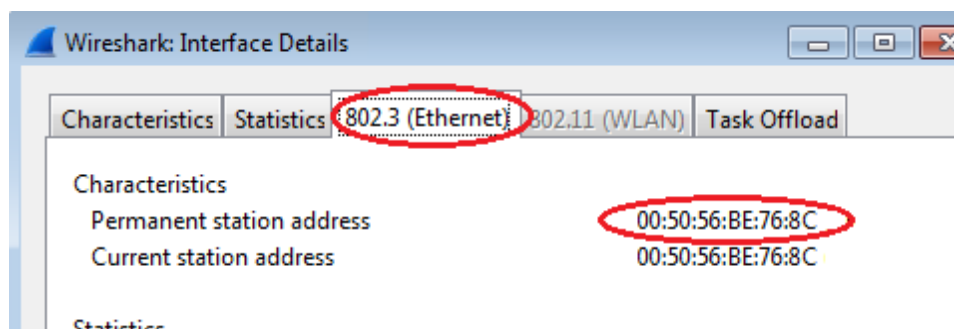


Nota: al hacer clic en el ícono de la primera interfaz de la fila de íconos, también se abre Interface List (Lista de interfaces).

- c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.

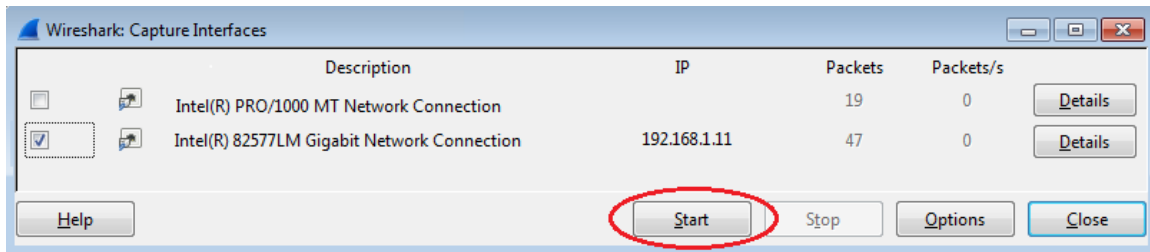


Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón **Details** (Detalles) y, a continuación, haga clic en la ficha **802.3 (Ethernet)**. Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana Interface Details (Detalles de la interfaz).

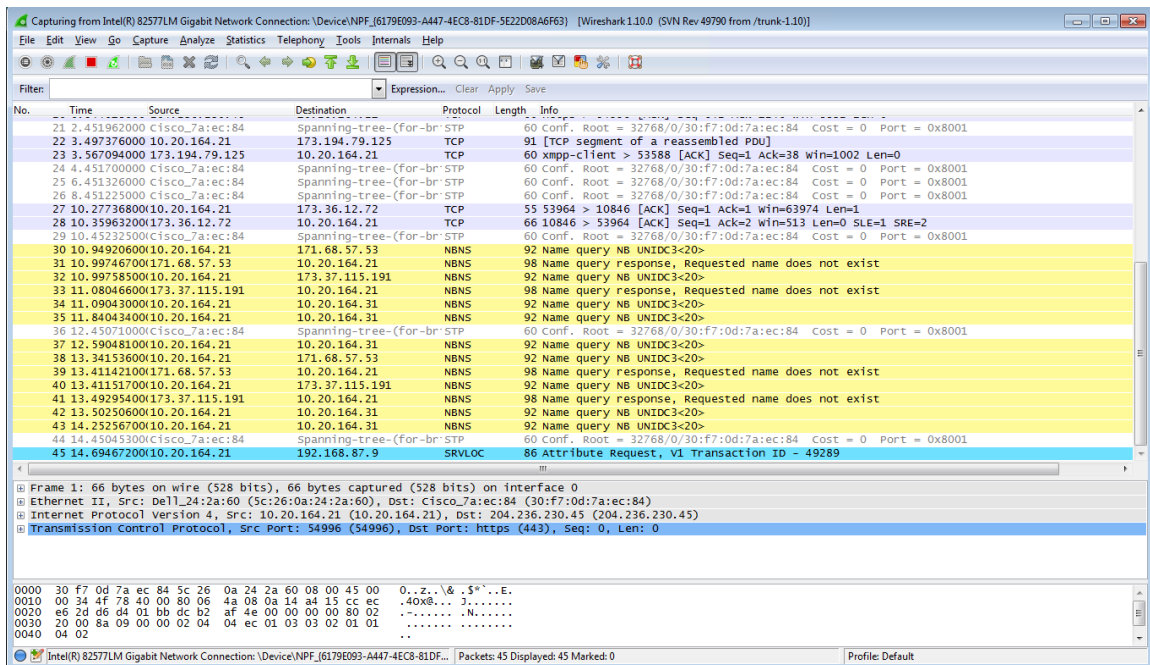


Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red

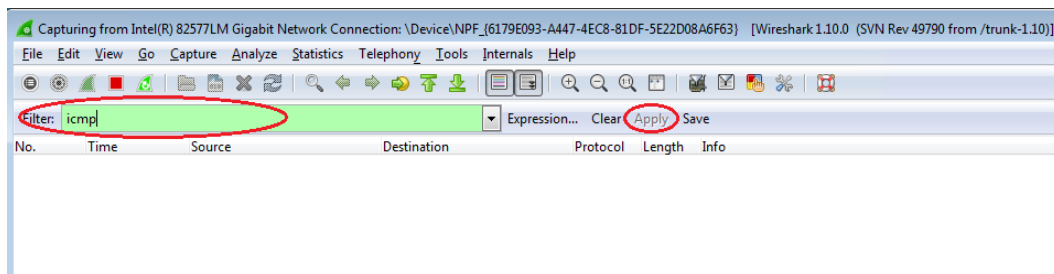
- d. Después de activar la interfaz correcta, haga clic en **Start** (Comenzar) para comenzar la captura de datos.



La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.

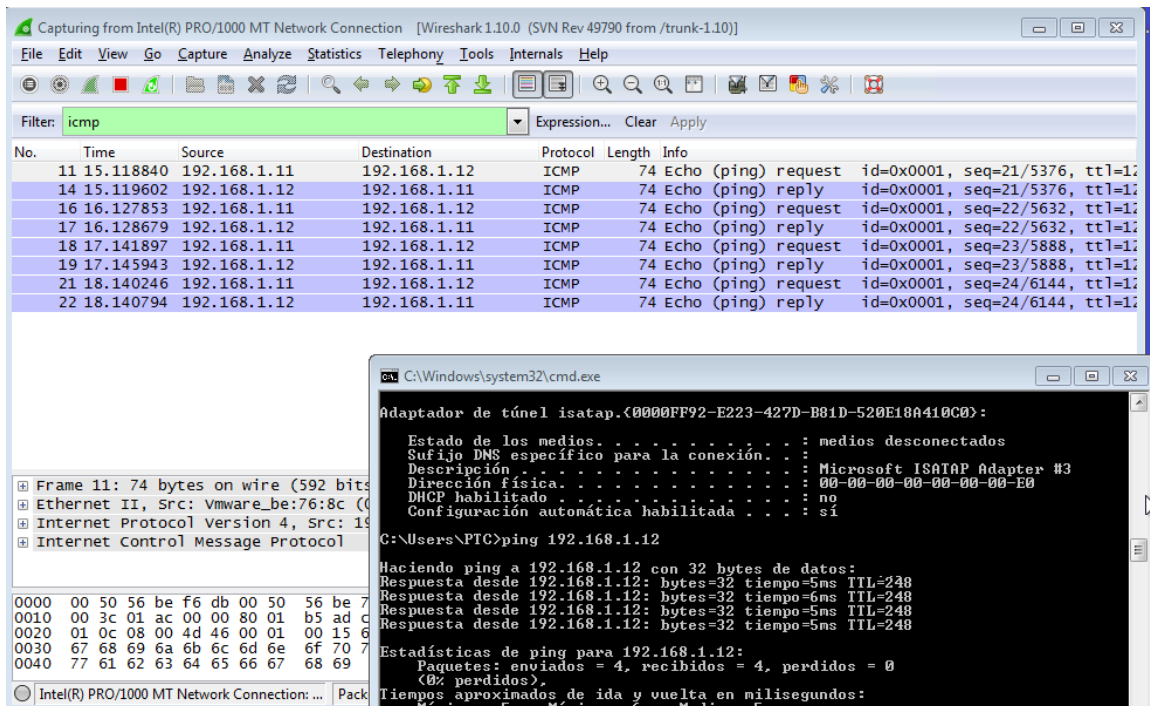


- e. Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro Filter (Filtro) que se encuentra en la parte superior de Wireshark y presione Entrar o haga clic en el botón **Apply** (Aplicar) para ver solamente PDU de ICMP (ping).



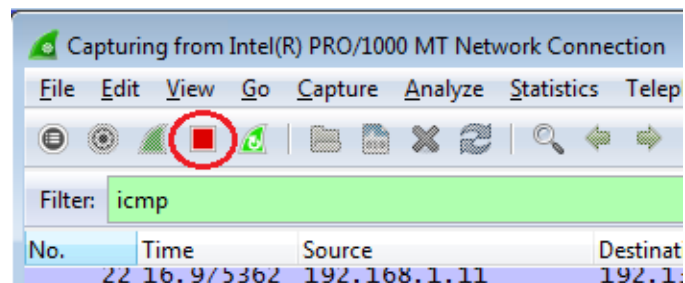
Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red

- f. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.



Nota: si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Apéndice A: Permitir el tráfico ICMP a través de un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows 7.

- g. Detenga la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).



Paso 3: Examinar los datos capturados

En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.

Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6) - Capturing from Intel(R) PRO/1000 MT Network Connection

Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
11	15.118840	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=12
14	15.119602	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=12
16	16.127853	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=12
17	16.128679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=12
18	17.141897	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=12
19	17.145943	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=12
21	18.140246	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=12
22	18.140794	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=12

Top Section

Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: IntelOf:91:48 (00:11:11:0f:91:48)

Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: IntelOf:91:48 (00:11:11:0f:91:48)

Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)

Internet Control Message Protocol

Middle Section

```

0000  00 50 56 be f6 db 00 50 56 be 76 8c 08 00 45 00  .PV...P V.v...E.
0010  00 3c 01 ac 00 00 80 01 b5 ad c0 a8 01 0b c0 a8  .<.....
0020  01 0c 08 00 4d 46 00 01 00 15 61 62 63 64 65 66  ....MF..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefgh i
  
```

Bottom Section

Intel(R) PRO/1000 MT Network Connection: ... Packets: 199 Displayed: 8 Marked: 0 Profile: Default

- Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Source (Origen) contiene la dirección IP de su PC y la columna Destination (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.

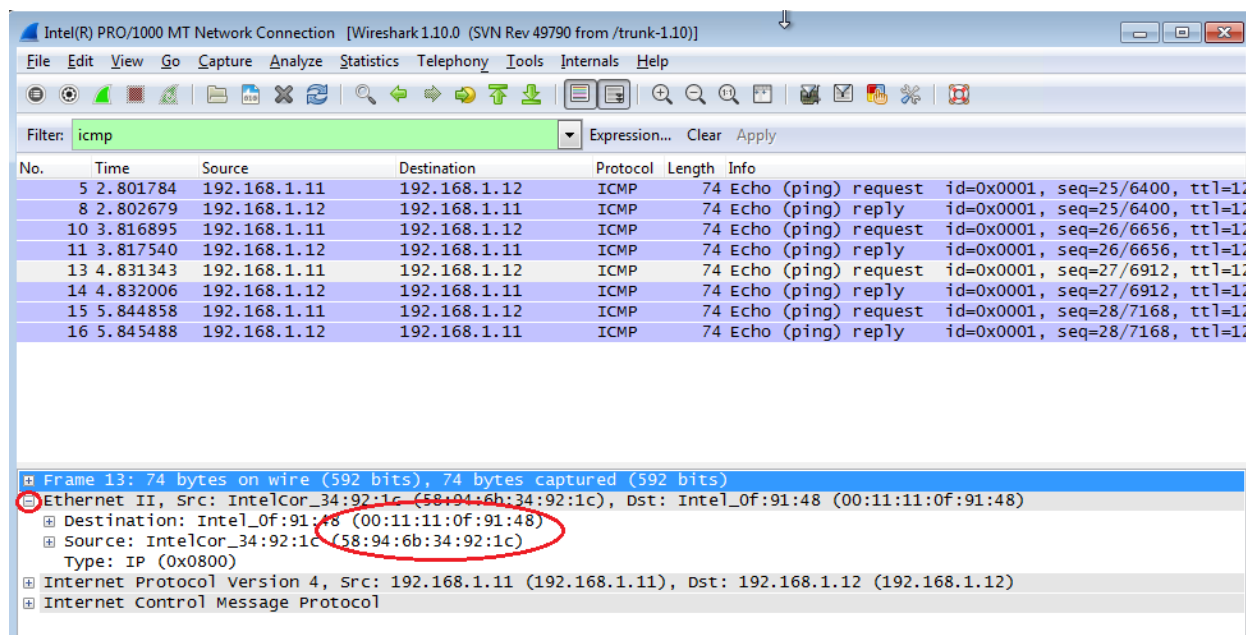
Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10) - Intel(R) PRO/1000 MT Network Connection

Filter: icmp

No.	Time	Source	Destination	Protocol	Length	Info
5	2.801784	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=12
8	2.802679	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=12
10	3.816895	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=12
11	3.817540	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=12
13	4.831343	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=12
14	4.832006	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=12
15	5.844858	192.168.1.11	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=12
16	5.845488	192.168.1.12	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=12

Bottom Section

- b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.



¿La dirección MAC de origen coincide con la interfaz de su PC? _____ **Sí**

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del miembro del equipo? _____ **Sí**

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

La dirección MAC se obtiene a través de una solicitud de ARP.

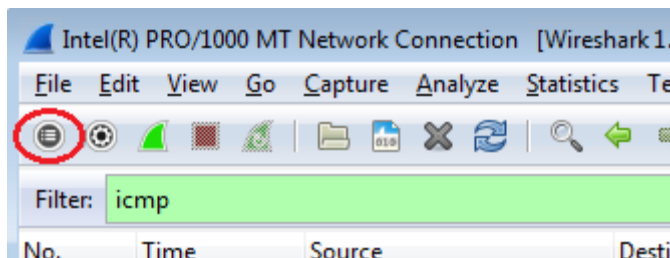
Nota: en el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPV4 (encabezado de IPV4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Parte 3: Capturar y analizar datos ICMP remotos en Wireshark

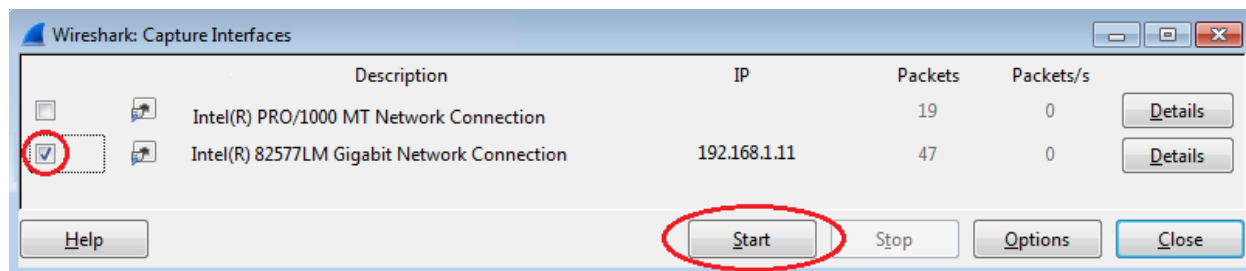
En la parte 3, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 2.

Paso 1: Comenzar a capturar datos en la interfaz

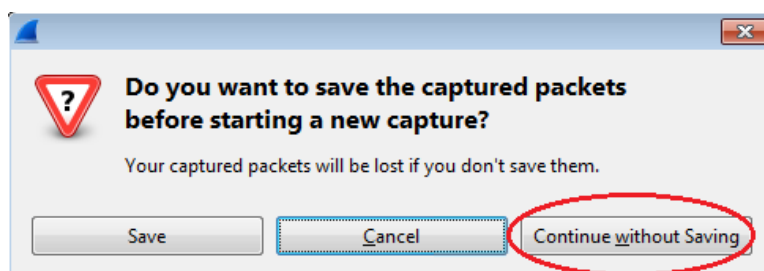
- a. Haga clic en el ícono **Interface List** (Lista de interfaces) para volver a abrir la lista de interfaces de la PC.



- b. Asegúrese de que la casilla de verificación junto a la interfaz LAN esté activada y, a continuación, haga clic en **Start** (Comenzar).



- c. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



- d. Con la captura activa, haga ping a los URL de los tres sitios Web siguientes:
- 1) www.yahoo.com
 - 2) www.cisco.com
 - 3) www.google.com


```
C:\Windows\system32\cmd.exe

C:\>ping www.yahoo.com

Haciendo ping a ds-eu-fp3.wai.b.yahoo.com [87.248.122.122] con 32 bytes de datos:
Respuesta desde 87.248.122.122: bytes=32 tiempo=385ms TTL=50
Respuesta desde 87.248.122.122: bytes=32 tiempo=385ms TTL=50
Respuesta desde 87.248.122.122: bytes=32 tiempo=385ms TTL=50
Respuesta desde 87.248.122.122: bytes=32 tiempo=385ms TTL=50

Estadísticas de ping para 87.248.122.122:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 385ms, Máximo = 385ms, Media = 385ms

C:\>ping www.cisco.com

Haciendo ping a e144.ds.ch.akamaiedge.net [2.21.96.170] con 32 bytes de datos:
Respuesta desde 2.21.96.170: bytes=32 tiempo=395ms TTL=52
Respuesta desde 2.21.96.170: bytes=32 tiempo=398ms TTL=52
Respuesta desde 2.21.96.170: bytes=32 tiempo=395ms TTL=52
Respuesta desde 2.21.96.170: bytes=32 tiempo=395ms TTL=52

Estadísticas de ping para 2.21.96.170:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 395ms, Máximo = 398ms, Media = 395ms

C:\>ping www.google.com

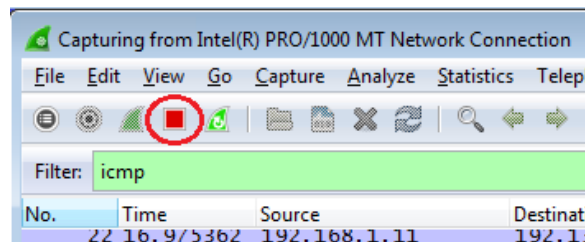
Haciendo ping a www.google.com [173.194.127.113] con 32 bytes de datos:
Respuesta desde 173.194.127.113: bytes=32 tiempo=54ms TTL=51
Respuesta desde 173.194.127.113: bytes=32 tiempo=54ms TTL=51
Respuesta desde 173.194.127.113: bytes=32 tiempo=52ms TTL=51
Respuesta desde 173.194.127.113: bytes=32 tiempo=53ms TTL=50

Estadísticas de ping para 173.194.127.113:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 52ms, Máximo = 54ms, Media = 53ms

C:\>_
```

Nota: al hacer ping a los URL que se indican, observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IP. Observe la dirección IP recibida para cada URL.

- e. Puede detener la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).



Paso 2: Inspeccionar y analizar los datos de los hosts remotos

- a. Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las tres ubicaciones a las que hizo ping. Indique las direcciones IP y MAC de destino para las tres ubicaciones en el espacio proporcionado.

1.^a ubicación: IP: _____ MAC: _____

2.^a ubicación: IP: _____ MAC: _____

3.^a ubicación: IP: _____ MAC: _____

Direcciones IP: 72.30.38.140, 192.133.219.25, 74.125.129.99 (estas direcciones IP pueden variar).

Dirección MAC: será la misma para las tres ubicaciones. Es la dirección física de la interfaz LAN del gateway predeterminado del router.

- b. ¿Qué es importante sobre esta información?

La dirección MAC para las tres ubicaciones es la misma.

- c. ¿En qué se diferencia esta información de la información de ping local que recibió en la parte 2?

Un ping a un host local devuelve la dirección MAC de la NIC de la PC. Un ping a un host remoto devuelve la dirección MAC de la interfaz LAN del gateway predeterminado.

Reflexión

¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

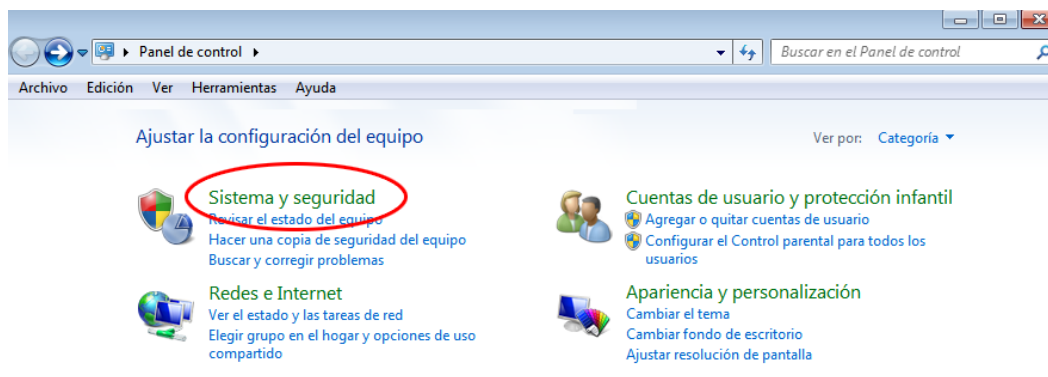
Las direcciones MAC de los hosts remotos no se conocen en la red local; por eso, se utiliza la dirección MAC del gateway predeterminado. Una vez que el paquete llega al router del gateway predeterminado, la información de la capa 2 se elimina del paquete y un nuevo encabezado de capa 2 se asocia a la dirección MAC de destino del router del salto siguiente.

Apéndice A: Permitir el tráfico ICMP a través de un firewall

Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio.

Paso 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

- a. En el panel de control, haga clic en la opción **Sistema y seguridad**.



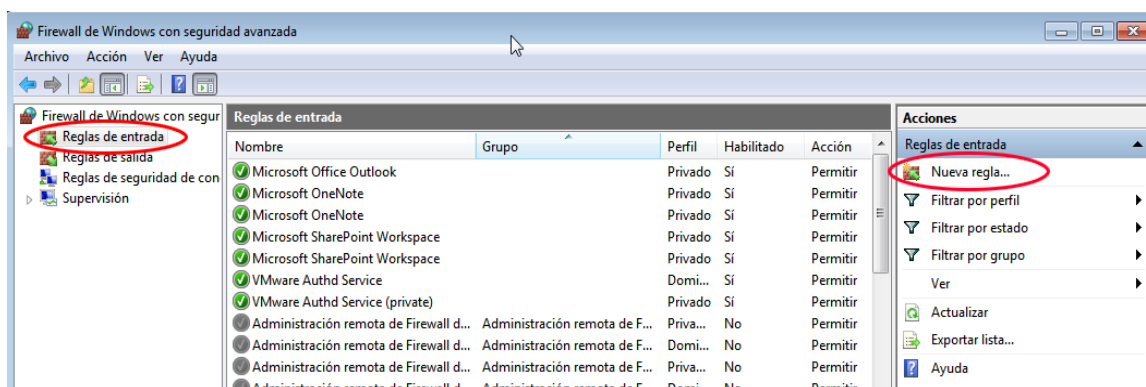
- b. En la ventana Sistema y seguridad, haga clic en **Firewall de Windows**.



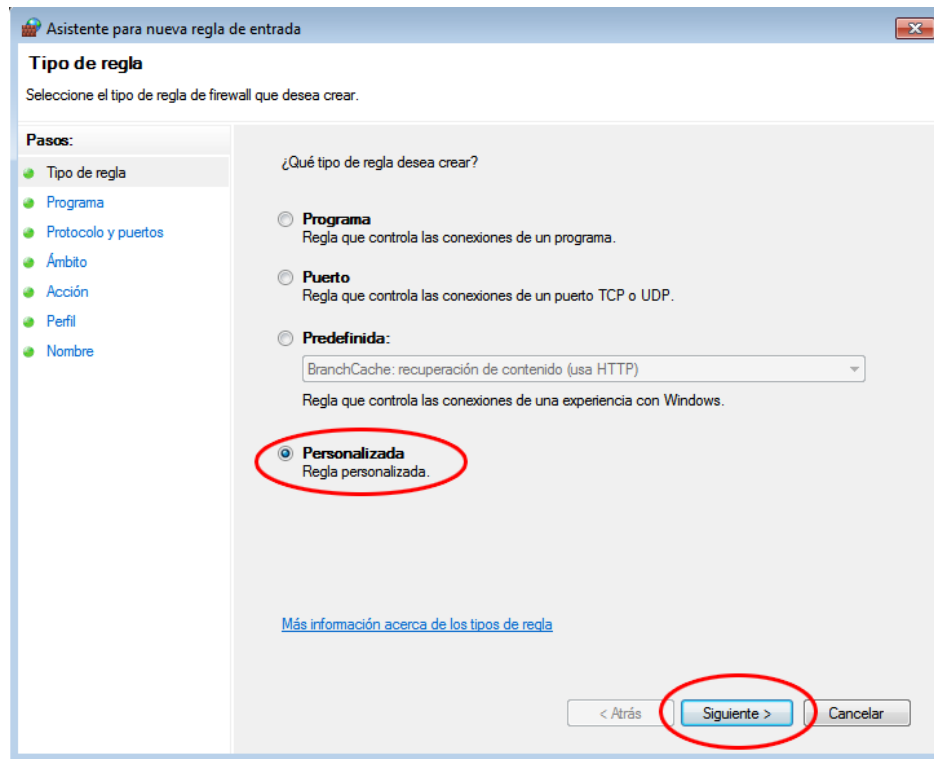
- c. En el panel izquierdo de la ventana Firewall de Windows, haga clic en **Configuración avanzada**.



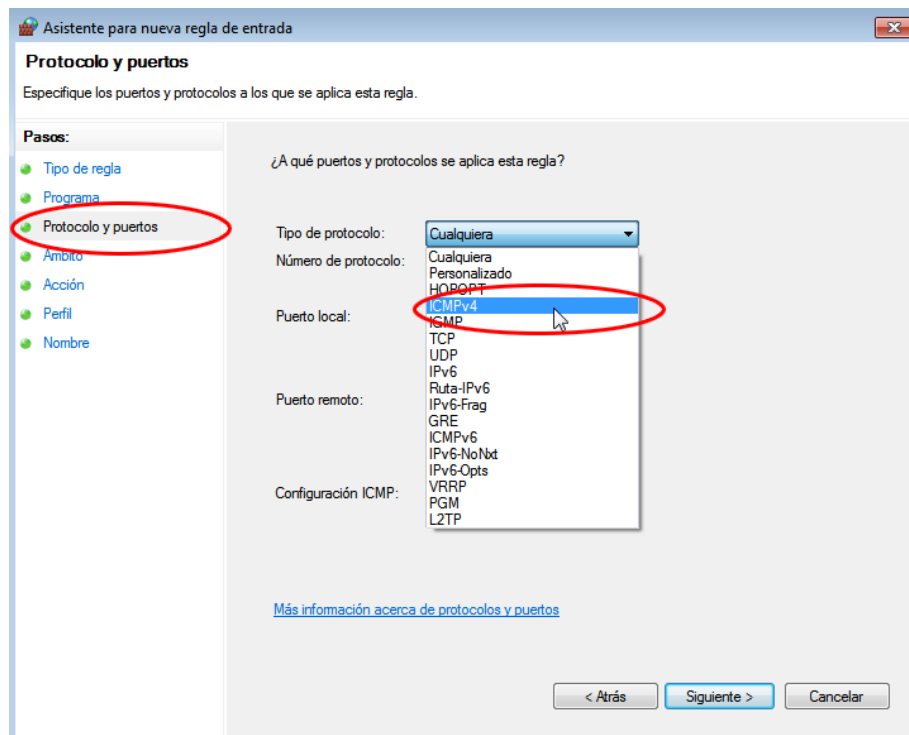
- d. En la ventana Seguridad avanzada, seleccione la opción **Reglas de entrada** en la barra lateral izquierda y, a continuación, haga clic **Nueva regla** en la barra lateral derecha.



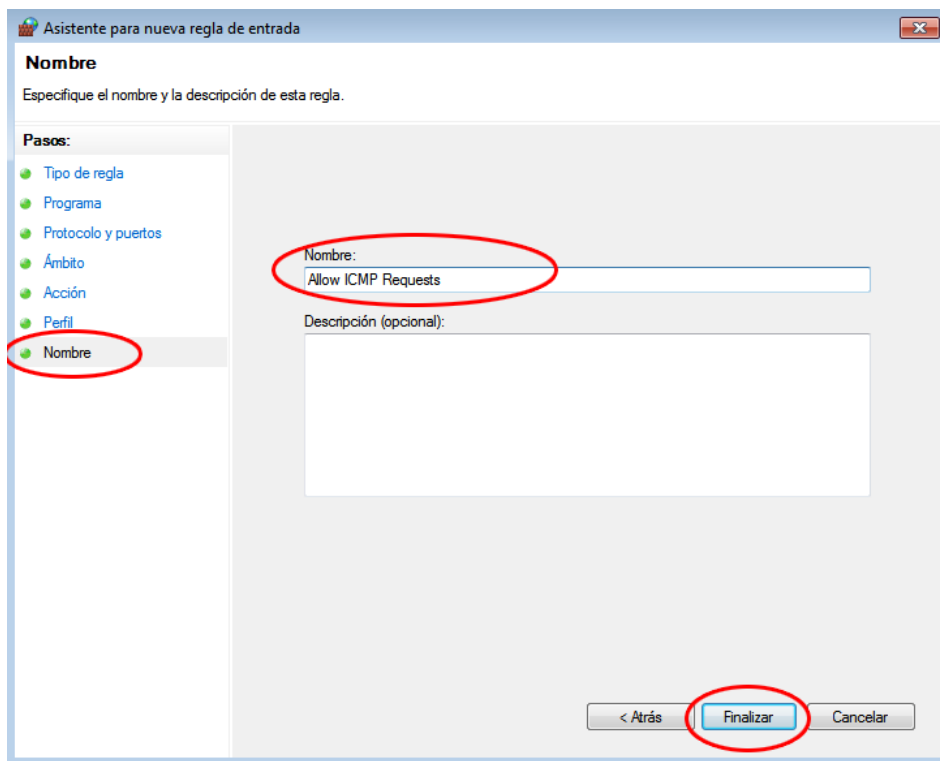
- e. Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción **Personalizada** y, a continuación, en **Siguiente**.



- f. En el panel izquierdo, haga clic en la opción **Protocolo y puertos**, y en el menú desplegable Tipo de protocolo, seleccione **ICMPv4**; a continuación, haga clic en **Siguiente**.



- g. En el panel izquierdo, haga clic en la opción **Nombre**, y en el campo Nombre, escriba **Allow ICMP Requests** (Permitir solicitudes ICMP). Haga clic en **Finish** (Finalizar).

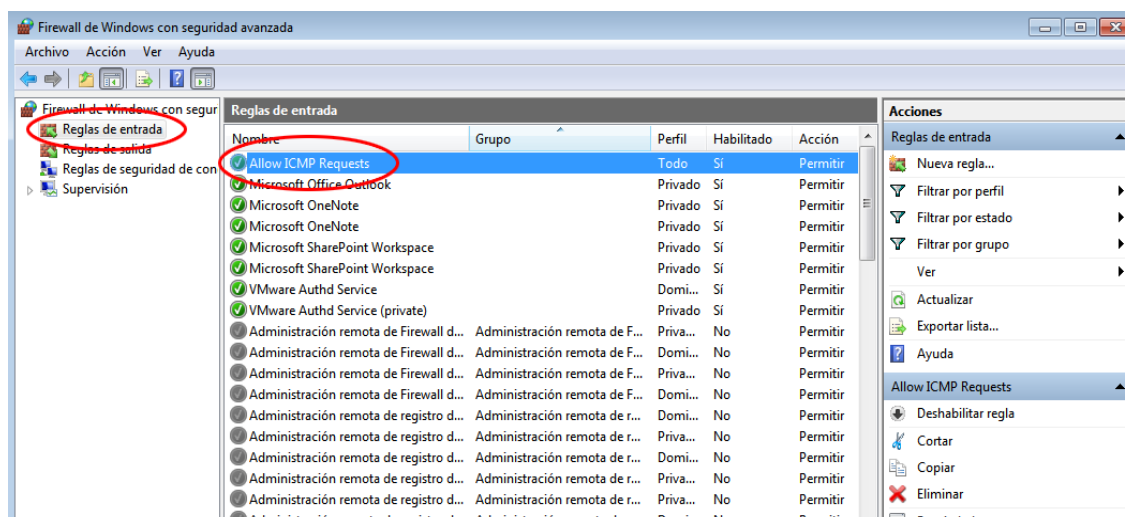


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

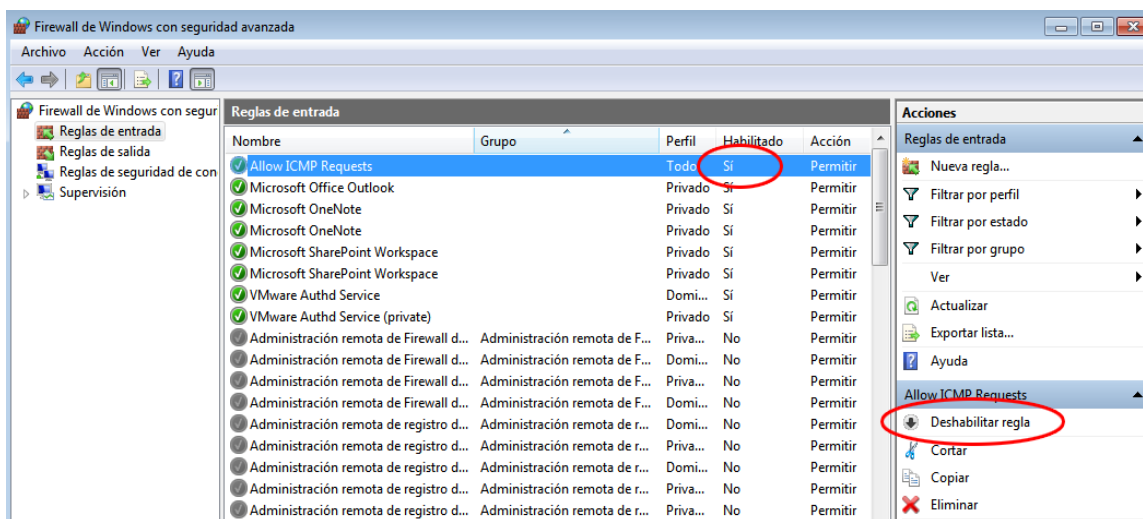
Paso 3: Deshabilitar o eliminar la nueva regla ICMP

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso eliminar la nueva regla que creó en el paso 1. La opción **Deshabilitar regla** permite volver a habilitar la regla en una fecha posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de Reglas de entrada.

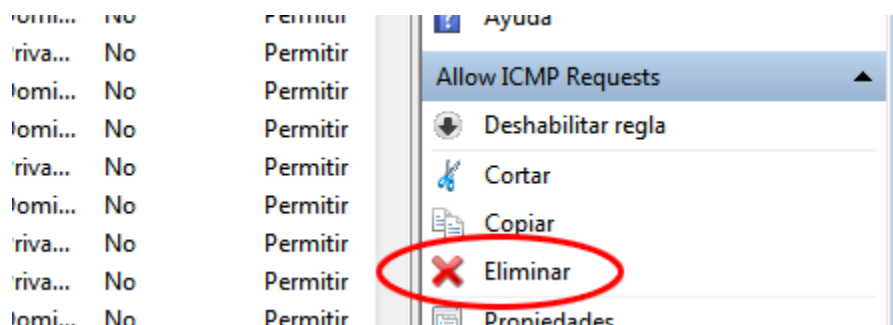
- a. En el panel izquierdo de la ventana Seguridad avanzada, haga clic en **Reglas de entrada** y, a continuación, ubique la regla que creó en el paso 1.



- b. Para deshabilitar la regla, haga clic en la opción **Deshabilitar regla**. Al seleccionar esta opción, verá que esta cambia a **Habilitar regla**. Puede alternar entre deshabilitar y habilitar la regla; el estado de la regla también se muestra en la columna Habilitada de la lista Reglas de entrada.



- c. Para eliminar permanentemente la regla ICMP, haga clic en **Eliminar**. Si elige esta opción, deberá volver a crear la regla para permitir las respuestas de ICMP.



Funcionamiento garantizado (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la función de los protocolos y de los organismos de estandarización para facilitar la interoperabilidad en las comunicaciones de red.

- Los estudiantes demostrarán cómo se pueden comparar las comunicaciones de red con las actividades diarias mediante procedimientos y estándares establecidos.

Información básica/Situación

Acaba de completar el contenido del capítulo 3 con respecto a los protocolos y estándares de red.

Suponiendo que resolvió la actividad de creación de modelos que se encuentra al comienzo de este capítulo, ¿cómo compararía los siguientes pasos para diseñar un sistema de comunicaciones con los modelos de networking utilizados para las comunicaciones?

Pasos para comunicarse	Respuestas posibles	Promociones de precios Capa del modelo TCP/IP
Establecimiento de un idioma para comunicarse.		
División del mensaje en pequeños pasos, entregados poco a poco, para facilitar la comprensión del problema.		
Corroboración de si el mensaje llegó correctamente al mecánico que realizará las reparaciones.		
Entrega del automóvil y tiempo de espera para la realización de la reparaciones		

Nota para el instructor: esta actividad de creación de modelos puede utilizarse como una asignación con calificación. Debe demostrar de qué forma los protocolos y estándares de red facilitan la transferencia de datos de origen a destino, tanto en prácticas personales como corporativas. La facilitación del debate debe incluir conversaciones entre los alumnos para mostrar cómo cambió la percepción de estos.

Recursos necesarios

- Tabla “Pasos para comunicarse” (arriba) en blanco para que los estudiantes registren sus respuestas sobre la base de su conocimiento del capítulo 3.

Reflexión

- ¿Cómo se compara el modelo de red en lo que respecta al desarrollo de un plan de comunicaciones de reparación de automóviles con un plan de interoperabilidad de comunicaciones de red?

Las tablas de los estudiantes pueden verse como esta (con algunas variaciones).

Pasos para comunicarse	Respuestas posibles	Promociones de precios Capa del modelo TCP/IP
Establecimiento de un idioma para comunicarse.	Voz/idioma (inglés, español, francés, etc.). Imágenes escritas Cenestésica/física	Capa de aplicación (HTTP, VoIP, POP, etc.)
División del mensaje en pequeños pasos, entregados poco a poco, para facilitar la comprensión del problema.	Breves descripciones compartidas poco a poco.	Capa de transporte (segmentos)
Corroboración de si el mensaje llegó correctamente al mecánico que realizará las reparaciones.	Solicitud al mecánico de que repita el problema completo que ocurre con el vehículo.	Capa de Internet (Paquetes)
Entrega del automóvil y tiempo de espera para la realización de la reparaciones	Entrega física del automóvil para efectuar las reparaciones (acuerdo sobre la entrega y el tiempo de espera para las reparaciones).	Capa de acceso de red (bits)

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Establecimiento de un idioma para comunicarse (Protocolo de aplicación)
- División del mensaje en pequeños pasos, entregados poco a poco, para facilitar la comprensión del problema que se debe resolver (protocolo de transporte).
- Corroboración de si el mensaje llegó correctamente al mecánico que realizará las reparaciones. (protocolo de Internet)
- Entrega del automóvil y tiempo de espera para la realización de las reparaciones (protocolo de acceso a la red)

Permítanme contarles lo que escuché en una conferencia...

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Describir el objetivo y la función de la capa de enlace de datos en la preparación de comunicaciones para su transmisión por medios específicos.

- Los estudiantes analizarán la forma en que puede realizarse de inmediato la comunicación dentro del dominio de una sola capa de enlace de datos al direccionar el nodo previsto directamente. También considerarán la dificultad cada vez mayor para establecer la comunicación cuando varios nodos de un solo dominio necesitan comunicarse.

Información básica/Situación

Usted y un colega asisten a una conferencia de networking. Durante el evento, se llevan a cabo muchas charlas y presentaciones. Debido a que estas se superponen, cada uno puede elegir solo un conjunto limitado de sesiones a las cuales asistir. Por lo tanto, deciden separarse. Cada uno asistirá a un conjunto distinto de presentaciones y, una vez que el evento finalice, compartirán las diapositivas y los conocimientos obtenidos por cada uno.

Responda las siguientes preguntas:

- ¿Cómo organizaría personalmente una conferencia donde se llevarán a cabo varias sesiones al mismo tiempo? ¿Los ubicaría a todos en una misma sala de conferencias o utilizaría varias salas? Justifique su respuesta.
- Suponga que la sala de conferencias cuenta con el equipo audiovisual adecuado para mostrar videos de gran tamaño y amplificar la voz del orador. Si una persona deseara asistir a una sesión específica, ¿importa qué asiento ocupa la persona o es suficiente que se siente en cualquier lugar mientras se encuentre en la sala de conferencias adecuada?
- ¿Cuáles son las posibles consecuencias o los beneficios de que el discurso pronunciado en una sala de conferencias de alguna manera se filtrara en otra sala?
- Si surgen preguntas durante una presentación, ¿los asistentes deben simplemente hacer sus preguntas gritando o debe existir algún proceso para garantizar que tengan la oportunidad de hacer preguntas que todos puedan oír? ¿Qué sucedería sin este proceso?
- ¿Puede terminarse el tiempo de una sesión sin haber analizado todo el contenido previsto si un tema interesante genera un debate más amplio en el cual muchos asistentes tienen preguntas? Si no deseara que suceda esto, ¿cuál sería la mejor manera de garantizar que no ocurra?
- Imagine que la sesión se lleva a cabo en un formato de panel, el cual permite un debate más libre entre los asistentes y los panelistas, y entre los asistentes entre sí. Si una persona desea dirigirse a otra persona dentro de la misma sala, ¿puede hacerlo directamente? De ser así, ¿cómo es posible? ¿Cómo invitaría un panelista a otra persona que no se encuentra actualmente en la sala a que se una al debate?
- ¿Qué beneficio, si existe alguno, se obtendría mediante el aislamiento de varias sesiones en salas de conferencias independientes si, después del evento, las personas pudieran reunirse y compartir la información?

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la forma en que se prepara una red para utilizar medios específicos en la transmisión de datos para la práctica personal y corporativa. Como resultado de esta actividad, se facilitará el debate.

Recursos necesarios

- Capacidades de registro (papel, tablet PC, etc.) para compartir los comentarios de reflexión con la clase.

Reflexión

1. ¿Cómo organizaría personalmente una conferencia donde se llevarán a cabo varias sesiones al mismo tiempo? ¿Los ubicaría a todos en una misma sala de conferencias o utilizaría varias salas? ¿Por qué? Justifique su respuesta.

Si se llevan a cabo varias sesiones independientes, es necesario realizarlas en salas separadas. De lo contrario, los oradores se superpondrían, y sería muy difícil, y en ocasiones imposible, comprender lo que expresan los presentadores. Llevar a cabo las distintas sesiones en salas independientes no se realiza con fines de seguridad (aunque puede haber sesiones privadas solo para ciertos invitados con restricciones en cuanto a quién puede unirse y lo que puede compartirse después de la sesión), sino con el propósito de mantener la comunicación separada para una mayor claridad y eficacia.

Nuestras redes se separan en varios dominios de la capa de enlace de datos (dominios de broadcast) con el objetivo de contener la comunicación de propiedades similares (grupos de trabajo, aplicaciones, pisos, requisitos de seguridad, etc.). Esto se parece a separar todas las sesiones en varias salas de conferencia según los temas.

2. Suponga que la sala de conferencias cuenta con el equipo audiovisual adecuado para mostrar videos de gran tamaño y amplificar la voz del orador. Si una persona deseara asistir a una sesión específica, ¿importa qué asiento ocupa la persona o es suficiente que se siente en cualquier lugar mientras se encuentre en la sala de conferencias adecuada?

Es suficiente que visite la sala de conferencias apropiada. Un asiento determinado no es importante, siempre y cuando el asistente pueda oír y escuchar sin obstrucciones desde cualquiera asiento.

La independencia relativa de un asiento determinado es similar a la independencia relativa de un nodo dentro de una red desde su dirección de host determinada. Para facilitar la comunicación dentro de una misma red, es suficiente que los nodos estén en el mismo dominio de la capa de enlace de datos y tengan direcciones únicas, pero no es importante cuáles son estas direcciones exactas. Dos nodos en un dominio común de la capa de enlace de datos pueden comunicarse entre sí y oírse inmediatamente.

3. ¿Cuáles son las posibles consecuencias o los beneficios de que el discurso pronunciado en una sala de conferencias de alguna manera se filtrara en otra sala?

Definitivamente, sería por lo menos molesto y provocaría la distracción de los asistentes, o podría dañar directamente el flujo de la sesión.

En las redes reales, existen situaciones en que dos dominios de la capa de enlace de datos que originalmente se propusieron para estar separados, se unen (por cableado incorrecto, configuración errónea, errores, etc.), y la información se filtra de uno al otro. Esta no es una situación correcta. Aunque los nodos de dos dominios diferentes de la capa de enlace de datos se comuniquen entre sí, la conexión debe realizarse de una manera controlada mediante routers que interconecten dominios separados de la capa de enlace de datos (similar a una persona que asiste a una sola sesión y luego, al finalizar, comparte el conocimiento con otra persona que no asistió; es decir, que enruta el conocimiento).

4. Si surgen preguntas durante una presentación, ¿los asistentes deben simplemente hacer sus preguntas gritando o debe existir algún proceso para garantizar que tengan la oportunidad de hacer preguntas que todos puedan oír? ¿Qué sucedería sin este proceso?

Las preguntas, los comentarios, las consultas, etc. del público deben realizarse de manera controlada. De lo contrario, dos o más personas hablarán al mismo tiempo, y eso hará que sus vecinos no comprendan a ninguno de ellos, y cada orador deberá repetir lo que expresó. Por lo general, levantar la mano indica que la persona tiene algo que decir.

En las redes, existen dos métodos principales para acceder al medio: determinista o aleatorio. Levantar la mano y esperar el turno es un enfoque determinista, similar al paso de tokens. Aprovechar la oportunidad de formular una pregunta en un momento de silencio sin esperar que se le otorgue el turno es un enfoque aleatorio, o estocástico. Observe que cualquiera de estos enfoques permite que la información se intercambie en ambos sentidos (entre el público y el presentador); es decir, que esté presente un tipo de dúplex. Sin embargo, como una sala de conferencias es un dominio de un medio compartido donde solo una persona puede hablar por vez (ya que, de lo contrario, se producen colisiones), el duplex aquí es un half-duplex.

¿Puede terminarse el tiempo de una sesión sin haber analizado todo el contenido previsto si un tema interesante genera un debate más amplio en el cual muchos asistentes tienen preguntas? Si no deseara que suceda esto, ¿cuál sería la mejor manera de garantizar que no ocurra?

Absolutamente. Al aumentar la cantidad de información que se compartirá a través del mismo medio, cada orador debe esperar a que los demás terminen su discurso. Esto, a su vez, demora a otros oradores, lo que posiblemente cause que el presentador no pueda desarrollar todo el contenido de la presentación. Al aumentar el número de estaciones en una red, en particular si la comunicación es de uno a todos, puede volverse cada vez más difícil transmitir datos a tiempo.

5. Imagine que la sesión se lleva a cabo en un formato de panel, el cual permite un debate más libre entre los asistentes y los panelistas, y entre los asistentes entre sí. Si una persona desea dirigirse a otra persona dentro de la misma sala, ¿puede hacerlo directamente? De ser así, ¿cómo es posible? ¿Cómo invitaría un panelista a otra persona que no se encuentra actualmente en la sala a que se una al debate?

Dentro de la misma sala, los asistentes pueden comunicarse entre ellos directamente: están en el mismo dominio, en el mismo medio, y pueden oírse de inmediato. No se necesita ningún proceso intermedio para entregar los datos. Aunque haya un dispositivo que ayude a transmitir la información solo al destinatario previsto dentro de la sala (como una persona que le pide a otra que transmita su mensaje a alguien más alejado), si cualquier persona se pusiera de pie y comenzara a gritar, todos podrían oírla. Si un panelista quisiera invitar a otra persona a la sala, tendría que pedir a los asistentes que busquen a esa persona y la inviten. Estos asistentes necesitarían enrutar decididamente la invitación hasta que llegue a la persona invitada.

La comunicación dentro de la misma red se realiza de inmediato. La comunicación con los nodos fuera de la red se realiza mediante los routers.

6. ¿Qué beneficio, si existe alguno, se obtendría mediante el aislamiento de varias sesiones en salas de conferencias independientes si, después del evento, las personas pudieran reunirse y compartir la información?

Como se explicó, el aislamiento no se realizó para proporcionar seguridad en primer lugar. El aislamiento se realizó para contener la comunicación de iguales propiedades o de propiedades similares en un entorno bien administrado que permita a los participantes interactuar directamente y comunicarse de manera mediada, de manera enrutada, con aquellos que no están dentro del mismo dominio. Esto redujo la cantidad de colisiones posibles y también disminuye el impacto de los broadcasts (gritos) en la red.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- **Sala de conferencias:** dominio de la capa de enlace de datos, dominio de broadcast.
- **Asiento en una sala de conferencias:** corresponde a una dirección L3 o L2 determinada.
- **Preguntas, consultas:** corresponde a una comunicación bidireccional, duplex.
- **Método para formular una pregunta:** corresponde al método de control de acceso al medio.
- **Gritos en una sala de conferencias:** corresponde al broadcast.

Práctica de laboratorio A: Identificación de dispositivos y cableado de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Identificar dispositivos de red

- Describir las funciones y las características físicas del dispositivo de red.

Parte 2: Identificar medios de red

- Describir las funciones y las características físicas de los medios.

Información básica/Situación

Como parte del personal de soporte de red, debe poder identificar distintos equipos de red. También debe comprender la función de los equipos en la parte apropiada de la red. En esta práctica de laboratorio, tendrá acceso a dispositivos y a medios de red. Identificará el tipo y las características de los equipos y los medios de red.

Nota para el instructor: esta es una práctica de laboratorio abierta. Los dispositivos y el cableado para identificar dependerán de lo que la academia y el instructor tengan disponible (ya sean equipos independientes o en bastidores). Si bien se prefieren equipos reales, el instructor puede complementar los dispositivos reales con fotos de buena calidad de dispositivos, si lo desea.

Nota para el instructor: se recomienda a los instructores que se comuniquen con la compañía telefónica y con operadores de cable locales para obtener ejemplos de cableado. Un recorrido por el centro de datos de la academia (con la aprobación del director de TI) puede ser una experiencia valiosa para los estudiantes. El instructor puede coordinar con el departamento de TI o de redes para rotular diversos dispositivos de un entorno real para propósitos de identificación.

Parte 1: Identificar dispositivos de red

El instructor proporcionará diversos dispositivos de red para su identificación. Cada uno se rotulará con un número de identificación.

Nota para el instructor: los diversos dispositivos de red que se muestren pueden ser hubs, switches, routers, puntos de acceso inalámbrico, routers inalámbricos (Linksys) y NIC. Los dispositivos pueden colocarse sobre una mesa o en bastidores, donde los estudiantes puedan acceder para examinarlos. Los estudiantes deben registrar el número de ID del dispositivo, el fabricante y el modelo, el tipo de dispositivo (hub, router o switch, etcétera), la funcionalidad (tecnología inalámbrica, router, switch o una combinación de estas), la cantidad y el tipo de interfaces y otras características físicas destacadas.

Complete la siguiente tabla con el número de ID del rótulo del dispositivo, el fabricante, el modelo de dispositivo, el tipo (hub, switch y router), la funcionalidad (tecnología inalámbrica, router, switch o una combinación de estas) y otras características físicas, como la cantidad de tipos de interfaces. La primera línea se completó como referencia.

ID	Fabricante	Modelo	Tipo	Funcionalidad	Características físicas
1	Cisco	1941	Router	Router	2 puertos GigabitEthernet 2 ranuras EHWIC 2 ranuras CompactFlash 1 ranura ISM 2 puertos de consola: USB, RJ-45
2					
3					
4					
5					
6					

Parte 2: Identificar los medios de red

El instructor proporcionará diversos medios de red para su identificación. Debe nombrar los medios de red, identificar el tipo de medio (cobre, fibra óptica o tecnología inalámbrica) y proporcionar una breve descripción de los medios que incluya qué tipos de dispositivos conectan. Use la siguiente tabla para registrar sus conclusiones. La primera línea de la tabla se completó como referencia.

Nota para el instructor: a continuación, se incluye una lista de medios de red para su referencia.

Cobre: Ethernet (STP, UTP, directo y cruzado, Cat 5, Cat 5E, Cat 6, etcétera), cable telefónico (el de dos hilos admite ADSL, por lo que es un cable de red válido), cable coaxial (red por cable), cables seriales (DB 60 y serial inteligente, macho/hembra).

Fibra óptica: (multimodo, monomodo, diversos tipos de conectores).

Tecnología inalámbrica: NIC, antenas Wi-Fi (Linksys o similar).

ID	Medios de red	Tipo	Descripción y a qué se conecta
1	UTP	Cobre	Conecta puertos NIC y Ethernet por cable en dispositivos de red. Cable directo Cat 5. Conecta PC y routers con switches y paneles de cableado.
2			
3			
4			
5			
6			

Reflexión

Después de que identificar los equipos de red, ¿dónde puede encontrar más información sobre los equipos?

RFC, sitio Web o material impreso de fabricantes de los equipos

Práctica de laboratorio: Armado de un cable cruzado Ethernet

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

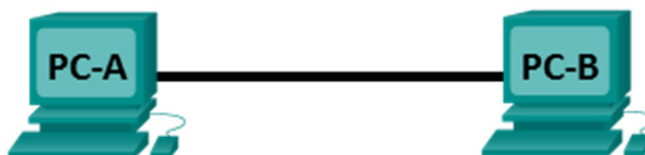


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC-A	NIC	192.168.10.1	255.255.255.0	No aplicable
PC-B	NIC	192.168.10.2	255.255.255.0	No aplicable

Objetivos

Parte 1: Analizar los estándares de cableado y los diagramas de pines de Ethernet

- Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-A.
- Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-B.

Parte 2: Armar un cable cruzado Ethernet

- Armar y conectar un extremo del cable TIA/EIA 568-A.
- Armar y conectar un extremo del cable TIA/EIA 568-B.

Parte 3: Probar un cable cruzado Ethernet

- Probar un cable cruzado Ethernet con un comprobador de cables.
- Conectar dos PC mediante un cable cruzado Ethernet.

Información básica/Situación

En esta práctica de laboratorio, armará y conectará un cable cruzado Ethernet, y lo probará conectando dos PC y haciendo ping entre ellas. Primero analizará los estándares 568-A y 568-B de la Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) y la forma en que se aplican a los cables Ethernet. Luego armará un cable cruzado Ethernet y lo probará. Por último, utilizará el cable que acaba de armar para conectar dos PC y lo probará haciendo ping entre ellas.

Nota: las capacidades de detección automática disponibles en muchos dispositivos, como el switch del router de servicios integrados (ISR) Cisco 1941, le permitirán ver los cables directos que conectan dispositivos similares.

Nota para el instructor: esta práctica de laboratorio puede ser bastante exigente para algunos estudiantes. Se pueden utilizar muchos conectores RJ-45 antes de armar un cable correcto. Si los recursos son limitados, quizá prefiera que dos estudiantes armen un cable en lugar de hacer que cada estudiante arme un cable individualmente.

Recursos necesarios

- Un tramo de cable, ya sea de categoría 5e o 5. El tramo de cable debe ser de 0,6 m a 0,9 m (de 2 ft a 3 ft).
- 2 conectores RJ-45
- Tenaza engarzadora RJ-45
- Alicates
- Pelacables
- Comprobador de cables Ethernet (optativo)
- 2 PC (Windows 7, Vista o XP)

Parte 1: Analizar los estándares de cableado y los diagramas de pines de Ethernet

La TIA/EIA especificó estándares de cableado de par trenzado no blindado (UTP) para el uso en entornos de cableado LAN. Los estándares 568-A y 568-B de la TIA/EIA estipulan los estándares de cableado comercial para las instalaciones de LAN. Estos son los estándares que se utilizan con mayor frecuencia en el cableado LAN de las organizaciones y determinan qué color de hilo se utiliza en cada pin.

Con un cable cruzado, el segundo y el tercer par del conector RJ-45 en un extremo del cable se invierten en el otro extremo, lo que invierte los pares de envío y recepción. Los diagramas de pines de los cables se realizan conforme al estándar 568-A en un extremo y al estándar 568-B en el otro extremo. Los cables cruzados se suelen utilizar para conectar hubs a hubs o switches a switches, pero también se pueden usar para conectar directamente dos hosts, a fin de crear una red simple.

Nota: en los dispositivos de red modernos, a menudo se puede utilizar un cable directo, incluso cuando se conectan dispositivos similares, debido a su característica de detección automática. La detección automática permite a las interfaces detectar si los pares de los circuitos de envío y recepción están conectados correctamente. Si no es así, las interfaces invierten un extremo de la conexión. La detección automática también modifica la velocidad de las interfaces para que coincidan con la más lenta. Por ejemplo, si se conecta una interfaz del router Gigabit Ethernet (1000 Mb/s) a una interfaz del switch Fast Ethernet (100 Mb/s), la conexión utiliza Fast Ethernet.

El switch Cisco 2960 tiene la función de detección automática activada de manera predeterminada; por lo tanto, la conexión de dos switches 2960 funciona con un cable cruzado o con un cable directo. Con algunos switches anteriores, este no es el caso, y se debe usar un cable cruzado.

Además, las interfaces Gigabit Ethernet del router Cisco 1941 cuentan con la función de detección automática, y se puede usar un cable directo para conectar una PC directamente a la interfaz del router (lo que omite el switch). Con algunos routers anteriores, este no es el caso, y se debe usar un cable cruzado.

Cuando se conectan dos hosts directamente, por lo general, se recomienda utilizar un cable cruzado.

Paso 1: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-A.

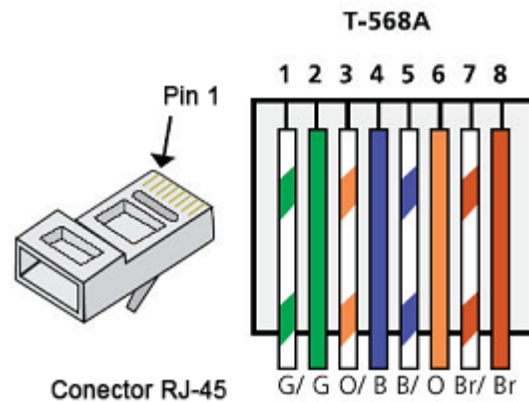
En la tabla y los diagramas siguientes, se muestran el esquema de colores y el diagrama de pines, así como la función de los cuatro pares de hilos que se utilizan para el estándar 568-A.

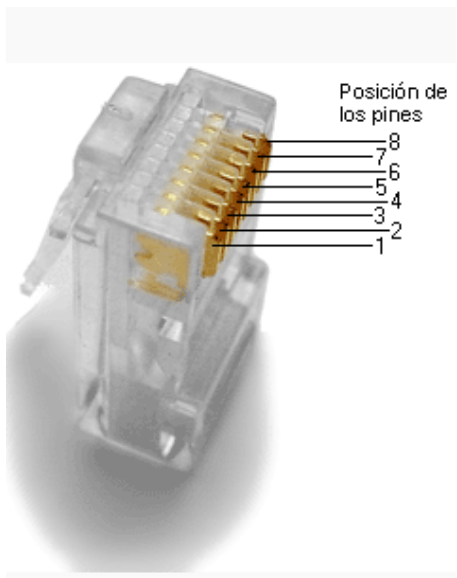
Nota: en las instalaciones de LAN que utilizan 100Base-T (100 Mb/s), se usan solo dos de los cuatro pares.

Ethernet 10/100/1000Base-TX conforme al estándar 568-A

Número de pin	Número de par	Color de hilo	Señal 10Base-T Señal 100Base-TX	Señal 1000Base-T
1	2	Blanco/Verde	Transmitir	BI_DA+
2	2	Verde	Transmitir	BI_DA-
3	3	Blanco/Naranja	Recibir	BI_DB+
4	1	Azul	No se utiliza	BI_DC+
5	1	Blanco/Azul	No se utiliza	BI_DC-
6	3	Naranja	Recibir	BI_DB-
7	4	Blanco/Marrón	No se utiliza	BI_DD+
8	4	Marrón	No se utiliza	BI_DD-

En los diagramas siguientes, se muestra la forma en que el color del hilo y el diagrama de pines se alinean con un conector RJ-45 conforme al estándar 568-A.



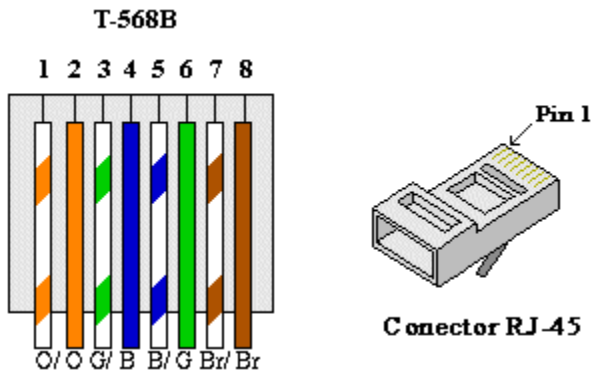


Paso 2: Analizar diagramas y tablas para el cable Ethernet estándar TIA/EIA 568-B.

En la tabla y el diagrama siguientes, se muestran el esquema de colores y el diagrama de pines conforme al estándar 568-B.

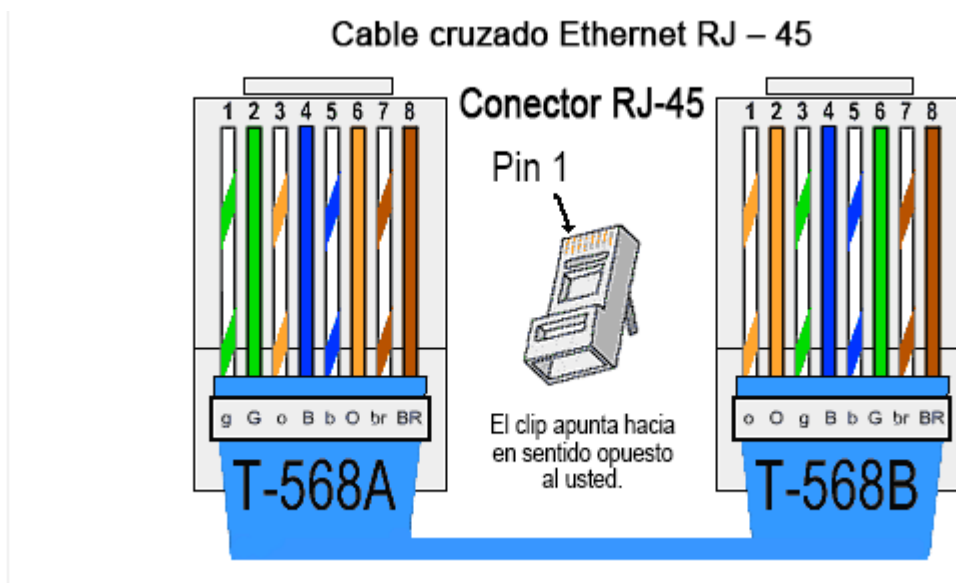
Ethernet 10/100/1000-BaseTX conforme al estándar 568-B

Número de pin	Número de par	Color de hilo	Señal 10Base-T Señal 100Base-TX	Señal 1000Base-T
1	2	Blanco/Naranja	Transmitir	BI_DA+
2	2	Naranja	Transmitir	BI_DA-
3	3	Blanco/Verde	Recibir	BI_DB+
4	1	Azul	No se utiliza	BI_DC+
5	1	Blanco/Azul	No se utiliza	BI_DC-
6	3	Verde	Recibir	BI_DB-
7	4	Blanco/Marrón	No se utiliza	BI_DD+
8	4	Marrón	No se utiliza	BI_DD-



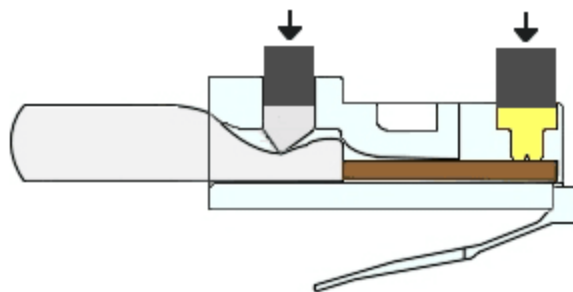
Parte 2: Armar un cable cruzado Ethernet

Un cable cruzado tiene el segundo par y el tercer par del conector RJ-45 en un extremo, invertido en el otro extremo (consulte la tabla de la parte 1, paso 2). Los diagramas de pines de los cables se realizan conforme al estándar 568-A en un extremo y al estándar 568-B en el otro extremo. Los diagramas que siguen ilustran este concepto.



Paso 1: Armar y conectar un extremo del cable TIA/EIA 568-A.

- Determine la longitud de cable requerida. (El instructor le informará la longitud de cable que debe armar).
- Nota:** si estuviera armando un cable en un ambiente de producción, la pauta general indica agregar otras 12 in (30,48 cm) a la longitud.
- Corte un trozo de cable de la longitud deseada y, con un pelacables, retire 5,08 cm (2 in) del revestimiento de ambos extremos del cable.
 - Sujete con firmeza los cuatro pares de cables trenzados donde se cortó el revestimiento. Reorganice los pares de cables en el orden que indica el estándar de cableado 568-A. Consulte los diagramas, si es necesario. Tome todas las precauciones posibles para mantener las torsiones del cable, a fin de proporcionar anulación de ruidos.
 - Aplane, enderece y alinee los hilos con los dedos pulgar e índice.
 - Los hilos de los cables deben estar en el orden correcto conforme al estándar 568-A. Utilice el alicate para cortar los cuatro pares en línea recta de 1,25 cm a 1,9 cm (de 1/2 in a 3/4 in).
 - Coloque un conector RJ-45 en el extremo del cable, con la punta de la parte inferior hacia abajo. Inserte con firmeza los hilos en el conector RJ-45. Todos los hilos se deben poder ver en el extremo del conector en la posición correcta. Si los hilos no se extienden hacia el extremo del conector, retire el cable, vuelva a organizar los hilos según sea necesario y vuelva a insertarlos en el conector RJ-45.
 - Si todo está bien, inserte el conector RJ-45 con el cable en la engarzadora. Engarce con fuerza para que los contactos del conector RJ-45 pasen a través del material aislante de los hilos y, de ese modo, completen el camino conductor. Consulte el diagrama siguiente para obtener un ejemplo.



Paso 2: Armar y conectar un extremo del cable TIA/EIA 568-B.

Repita los pasos 1a a 1g utilizando el esquema de colores de hilos establecido en el estándar 568-B para el otro extremo.

Parte 3: Probar un cable cruzado Ethernet

Paso 1: Probar el cable

Muchos comprobadores de cables permiten probar la longitud y el trazado de los hilos. Si el comprobador de cables tiene una característica de trazado, permite comprobar qué pines de un extremo del cable están conectados a qué pines del otro extremo.

Si el instructor tiene un comprobador de cables, pruebe el cable cruzado para corroborar la funcionalidad. Si falla, corrobore primero con el instructor si debe volver a conectar los extremos de los cables y vuelva a probarlos.

Paso 2: Conectar dos PC mediante NIC utilizando el cable cruzado Ethernet

- Trabaje con un compañero para configurar la PC en una de las direcciones IP que aparecen en la tabla de direccionamiento (consulte la página 1). Por ejemplo, si la PC es la **PC-A**, la dirección IP debe configurarse en **192.168.10.1** con una **máscara de subred de 24 bits**. La dirección IP de su compañero debe ser **192.168.10.2**. La dirección de gateway predeterminado puede dejarse en blanco.
- Utilice el cable cruzado que armó y conecte las dos PC con las NIC.
- En el símbolo del sistema de la PC-A, haga ping a la dirección IP de la PC-B.

Nota: es posible que el Firewall de Windows tenga que deshabilitarse temporalmente para que los pings sean correctos. Si el firewall se deshabilita, vuelva a habilitarlo al final de esta práctica de laboratorio.

- Repita el proceso y haga ping de la PC-B a la PC-A.

Si el direccionamiento IP y el firewall no son un problema, los pings deben ser correctos si los cables se armaron como corresponde.

Reflexión

- ¿Qué parte del armado de cables le pareció más difícil?

Las respuestas varían. Insertar los cables en el orden correcto en el conector RJ-45 suele ser lo más difícil.

- ¿Por qué tiene que aprender a armar un cable si puede comprar cables ya armados?

Un cable puede volverse defectuoso en un ambiente de producción. Reemplazarlo puede llevar mucho tiempo o ser muy costoso, y, a menudo, es más simple volver a cablear cada extremo, en el caso de ser necesario.

Práctica de laboratorio: Visualización de información de NIC conectadas por cable e inalámbricas (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Identificar y trabajar con NIC de PC

Parte 2: Identificar y utilizar los iconos de red de la bandeja del sistema

Información básica/Situación

Para esta práctica de laboratorio, es necesario que determine la disponibilidad y el estado de las tarjetas de interfaz de red (NIC) en la PC que utiliza. Windows proporciona diversas maneras de ver y de trabajar con las NIC.

En esta práctica de laboratorio, tendrá acceso a la información de la NIC de su PC y cambiará el estado de estas tarjetas.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con dos NIC, conectadas por cable o inalámbricas, y una conexión inalámbrica)

Nota: al comenzar esta práctica de laboratorio, la NIC Ethernet conectada por cable de la PC se conectó a uno de los puertos de switch integrado en un router inalámbrico, y la conexión de área local (conectada por cable) estaba habilitada. La NIC inalámbrica estaba deshabilitada inicialmente. Si la NIC conectada por cable y la NIC inalámbrica están habilitadas, la PC recibe dos direcciones IP diferentes y la NIC inalámbrica tiene prioridad.

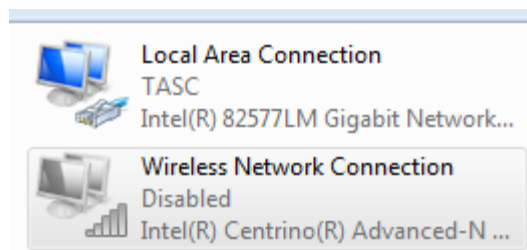
Parte 1: Identificar y trabajar con NIC de PC

En la parte 1, identificará los tipos de NIC de la PC que está utilizando. Explorará las diferentes formas de extraer información acerca de estas NIC y cómo activarlas y desactivarlas.

Nota: esta práctica de laboratorio se realizó utilizando una PC con sistema operativo Windows 7. Debería poder realizar la práctica de laboratorio con uno de los otros sistemas operativos Windows que se indican; no obstante, las selecciones de menú y las pantallas pueden variar.

Paso 1: Utilizar el Centro de redes y recursos compartidos

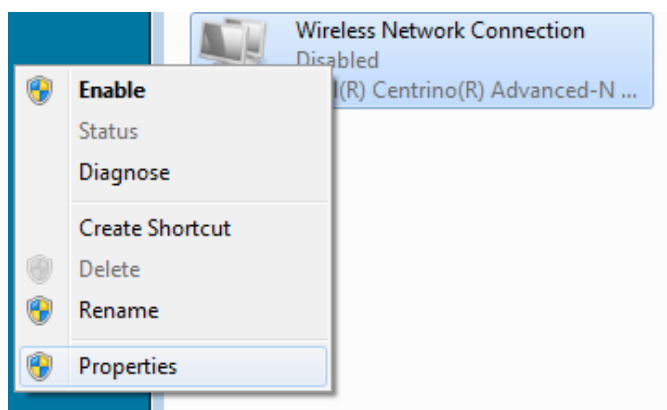
- Abra el **Centro de redes y recursos compartidos** haciendo clic en el botón **Inicio** de Windows > **Panel de control** > **Ver el estado y las tareas de red** en el encabezado Red e Internet de la vista Categoría.
- En el panel izquierdo, haga clic en el enlace **Cambiar configuración del adaptador**.
- Aparece la ventana Conexiones de red, en la que se proporciona la lista de NIC disponibles en esta PC. En esta ventana, busque los adaptadores de conexión de área local y conexión de red inalámbrica.



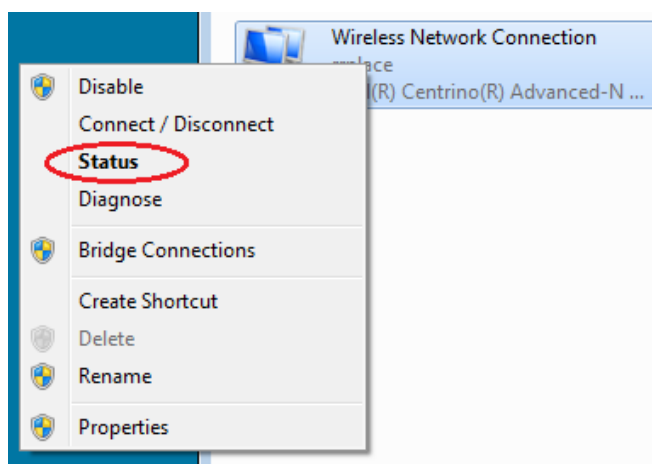
Nota: en esta ventana, también se pueden mostrar adaptadores de la red privada virtual (VPN) y otros tipos de conexiones de red.

Paso 2: Trabajar con la NIC inalámbrica

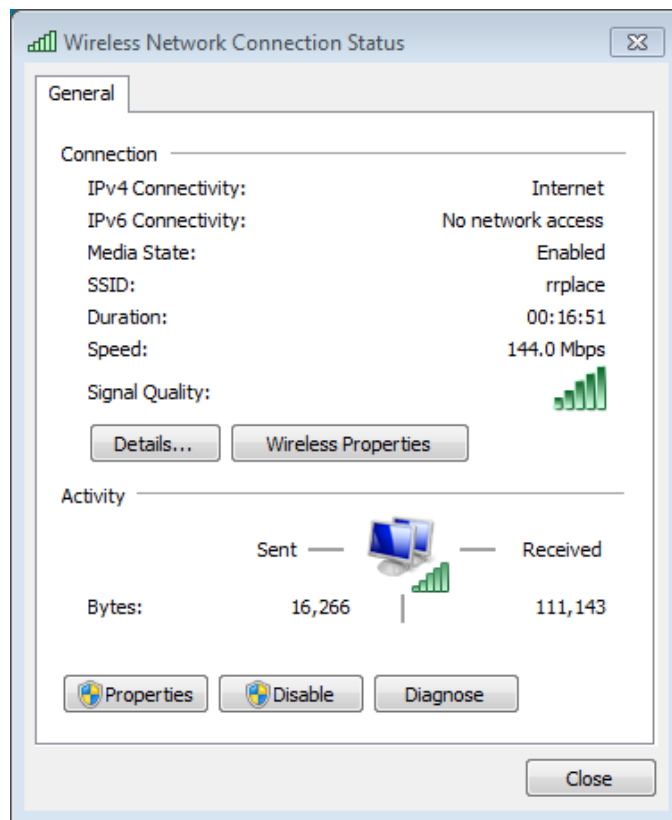
- a. Seleccione la opción **Conexión de red inalámbrica** y haga clic con el botón secundario para abrir una lista desplegable. Si la NIC inalámbrica está deshabilitada, la opción **Habilitar** le permitirá habilitarla. Si la NIC ya está habilitada, entonces **Deshabilitar** sería la primera opción en este menú desplegable. Si la opción **Conexión de red inalámbrica** está deshabilitada, haga clic en **Habilitar**.



- b. Haga clic con el botón secundario en **Conexión de red inalámbrica** y, a continuación, haga clic en **Estado**.



- c. Aparece la ventana Estado de la conexión de red inalámbrica, donde puede ver información sobre la conexión inalámbrica.



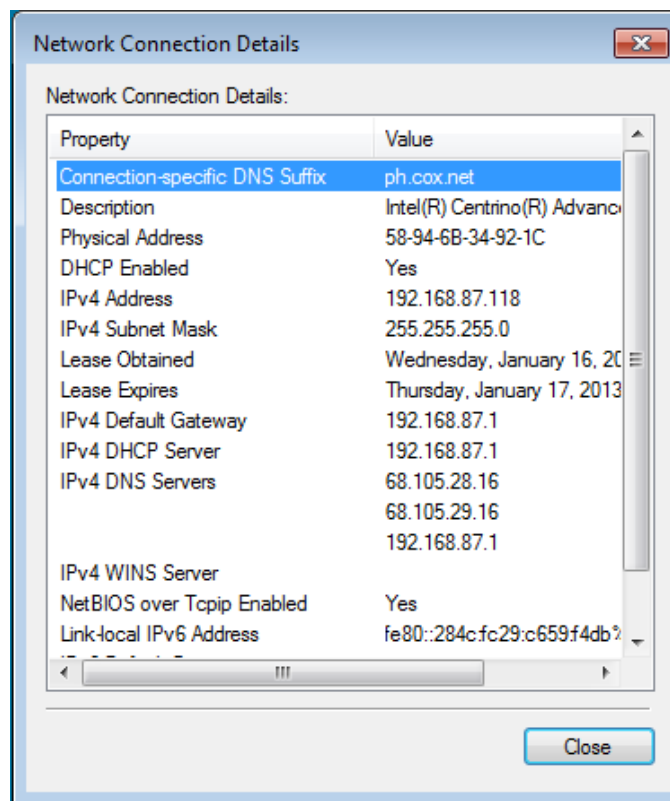
¿Cuál es el identificador de conjunto de servicios (SSID) para el router inalámbrico de la conexión?

_____ rrplace (en el ejemplo anterior)

¿Cuál es la velocidad de la conexión inalámbrica?

_____ 144 Mb/s (en el ejemplo anterior)

- d. Haga clic en **Detalles** para visualizar la ventana Detalles de la conexión de red.



¿Cuál es la dirección MAC de la NIC inalámbrica?

_____ 58-94-6b-34-92-1c (en el ejemplo anterior)

¿Se indican varios servidores DNS IPv4 en la lista?

_____ Sí (en el ejemplo anterior)

¿Por qué se indicarían varios servidores DNS?

Las respuestas varían, pero se indican varios servidores DNS en caso de que el primer servidor DNS no responda. Entre los motivos, se puede incluir que el servidor está desactivado por cuestiones de mantenimiento o tiene un problema. Si el primer servidor DNS no responde, entonces se utiliza el segundo servidor DNS, y así sucesivamente.

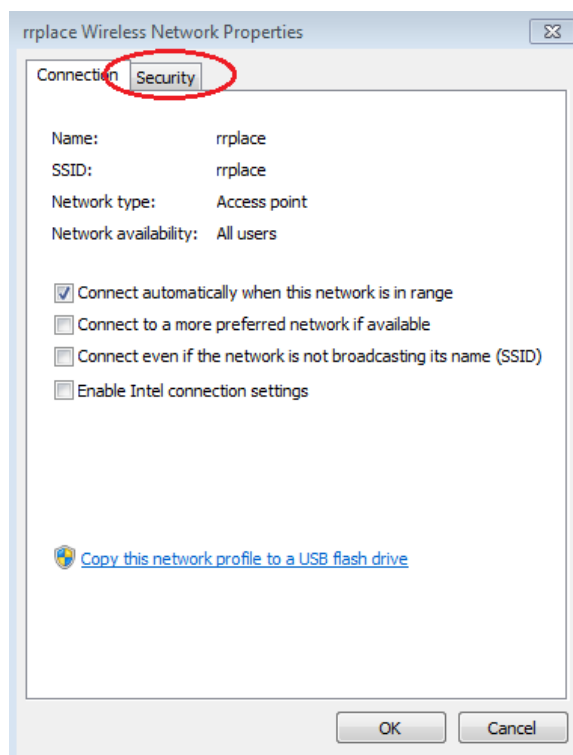
- e. Después de revisar los detalles de la conexión de red, haga clic en Close (**Cerrar**).

- f. Abra una ventana de petición de entrada de comandos y escriba **ipconfig /all**.

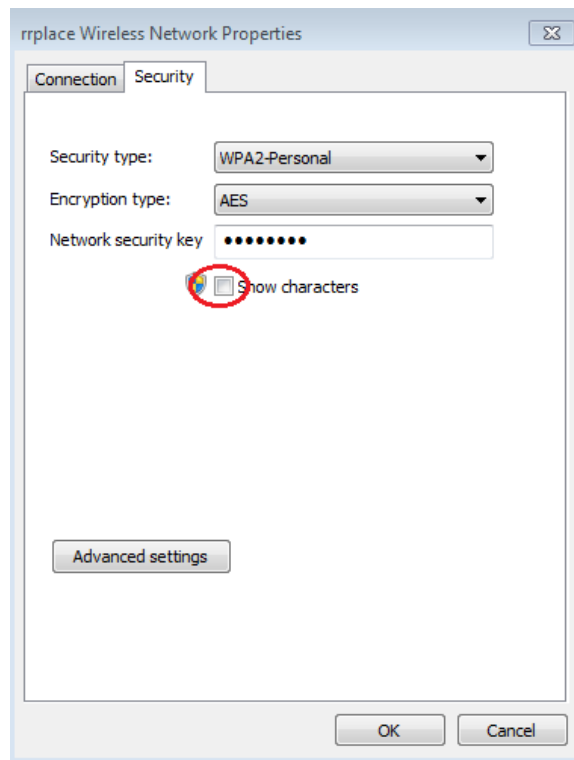
```
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : ph.cox.net
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 58-94-6B-34-92-1C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::284c:fc29:c659:f4db%11(Preferred)
IPv4 Address. . . . . : 192.168.87.118(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, January 17, 2013 8:30:40 AM
Lease Expires . . . . . : Friday, January 18, 2013 8:30:41 AM
Default Gateway . . . . . : 192.168.87.1
DHCP Server . . . . . : 192.168.87.1
DHCPv6 IAID . . . . . : 307795051
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-AC-22-0A-5C-26-0A-24-2A-60
DNS Servers . . . . . : 68.105.28.16
                       : 68.105.29.16
                       : 192.168.87.1
NetBIOS over Tcpip. . . . . : Enabled
```

Observe que la información que se muestra aquí es la misma que se mostró en la ventana Detalles de la conexión de red, en el paso d.

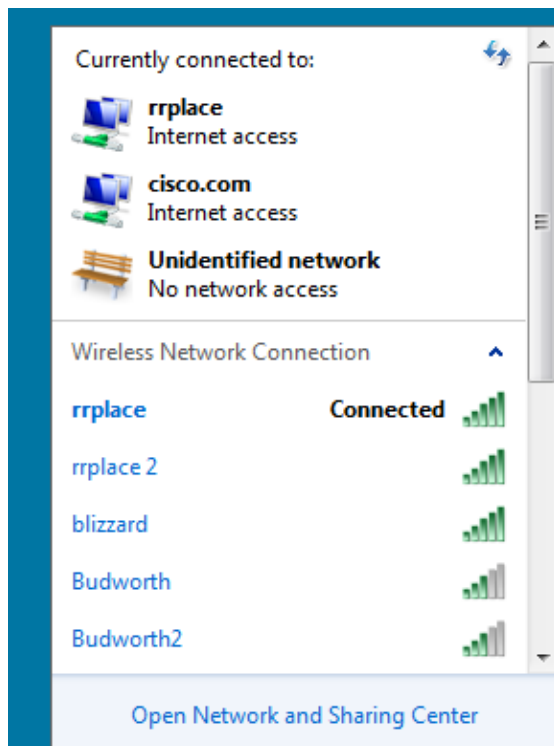
- g. Cierre la ventana de comandos y la ventana Detalles de la conexión de red. Esta acción debería llevarlo de nuevo a la ventana Estado de la conexión de red inalámbrica. Haga clic en **Propiedades inalámbricas**.
- h. En la ventana **Propiedades de la red inalámbrica**, haga clic en la ficha **Seguridad**.



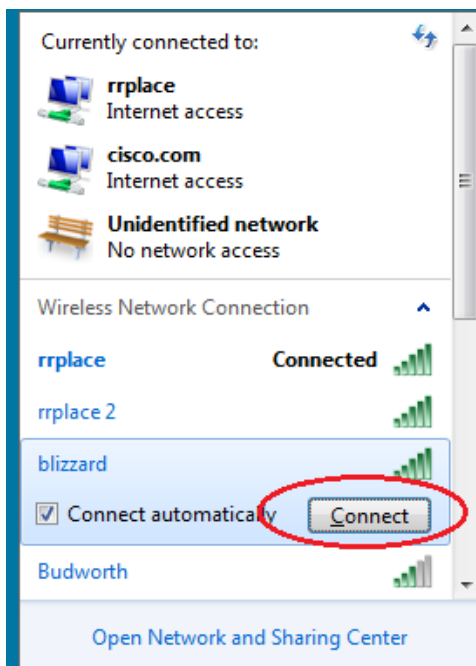
- i. Se muestra el tipo de seguridad que implementó el router inalámbrico conectado. Haga clic en la casilla de verificación **Mostrar caracteres** para visualizar la clave de seguridad de la red tal cual es, en lugar de los caracteres ocultos, y luego haga clic en **Aceptar**.



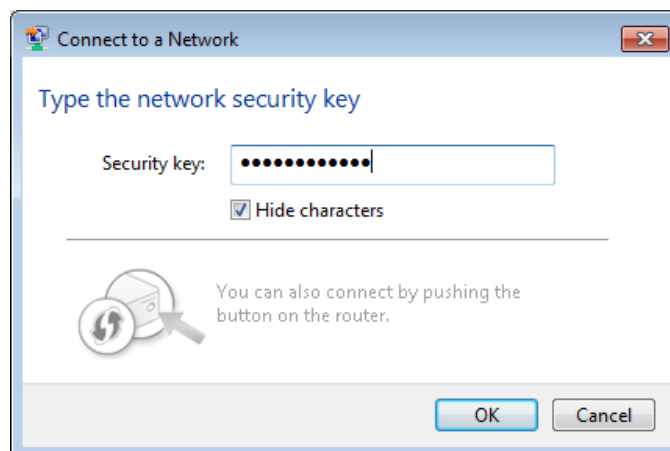
- j. Cierre las ventanas Propiedades de la red inalámbrica y Estado de la conexión de red inalámbrica. Seleccione y haga clic con el botón secundario en la opción **Conexión de red inalámbrica > Conectar/Desconectar**. Aparece una ventana emergente en la esquina inferior derecha del escritorio en la que se muestran las conexiones actuales junto con una lista de SSID que están dentro del alcance de la NIC inalámbrica de la PC. Si aparece una barra de desplazamiento a la derecha de esta ventana, puede utilizarla para ver más SSID.



- k. Para unirse a uno de los otros SSID de red inalámbrica que se enumeran, haga clic en el SSID al que desea unirse y, a continuación, haga clic en **Conectar**.



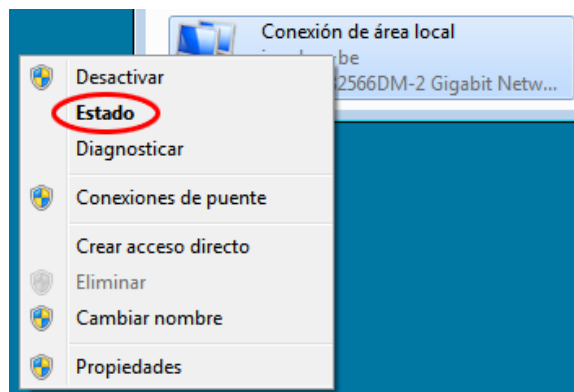
- I. Si seleccionó un SSID seguro, se le solicitará que introduzca la **Clave de seguridad** del SSID. Escriba la clave de seguridad para ese SSID y haga clic en **Aceptar**. Puede hacer clic en la casilla de verificación **Ocultar caracteres** para evitar que otros usuarios vean lo que escribe en el campo **Clave de seguridad**.



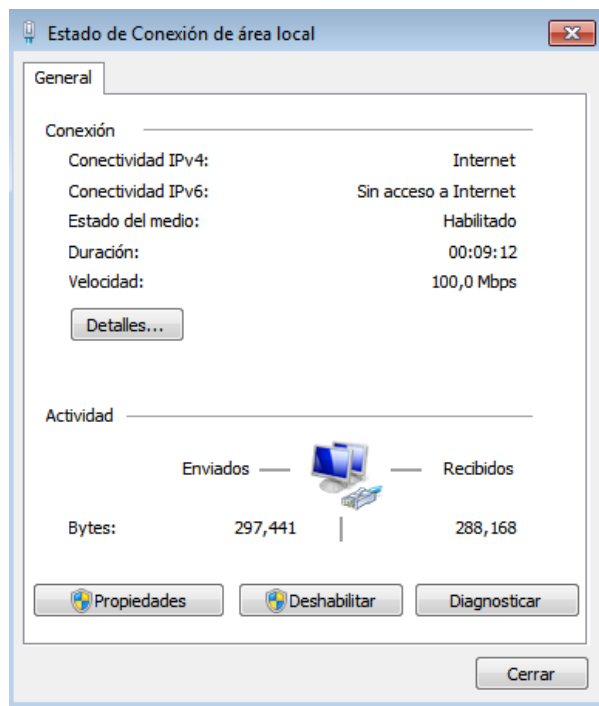
Paso 3: Trabajar con la NIC conectada por cable

- a. En la ventana Conexiones de red, seleccione y haga clic con el botón secundario en la opción **Conexión de área local** para que aparezca la lista desplegable. Si la NIC está deshabilitada, habilítela, y luego haga clic en la opción **Estado**.

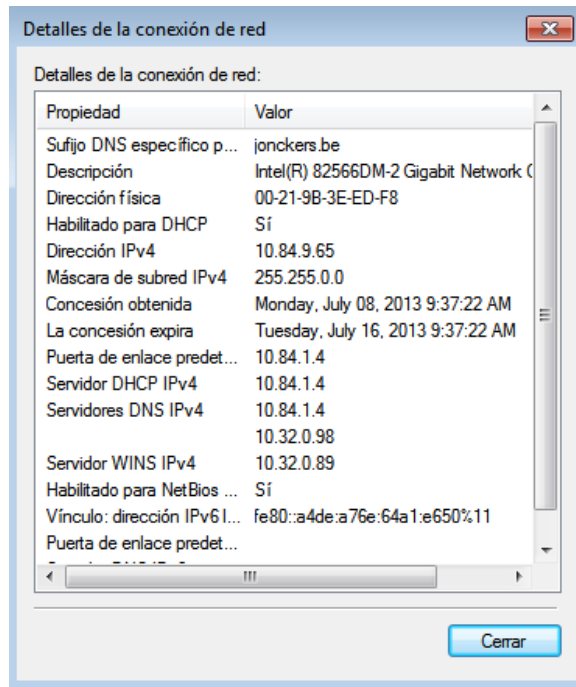
Nota: para ver el estado, la NIC de la PC debe estar conectada a un switch o a un dispositivo similar a través de un cable Ethernet. Muchos routers inalámbricos tienen un pequeño switch Ethernet incorporado de cuatro puertos. Puede conectarse a uno de los puertos utilizando un cable directo de conexión de Ethernet.



- b. Se abrirá la ventana Estado de conexión de área local. Esta ventana muestra información acerca de la conexión por cable a la LAN.



Haga clic en **Detalles...** para ver la información de la dirección para la conexión LAN.



- c. Abra una ventana de petición de entrada de comandos y escriba **ipconfig /all**. Busque la información de la conexión de área local y compárela con la información que se muestra en la ventana Detalles de la conexión de red.

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : jonckers.be
    Descripción . . . . . : Intel(R) 82566DM-2 Gigabit Network
    Dirección física. . . . . : 00-21-9B-3E-ED-F8
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Vínculo: dirección IPv6 local. . . : fe80::a4de:a76e:64a1:e650%11(Preferido)

    Dirección IPv4. . . . . : 10.84.9.65(Preferido)
    Máscara de subred . . . . . : 255.255.0.0
    Concesión obtenida. . . . . : Monday, July 08, 2013 9:37:22 AM
    La concesión expira . . . . . : Tuesday, July 16, 2013 9:37:22 AM

    Puerta de enlace predeterminada . . . . : 10.84.1.4
    Servidor DHCP . . . . . : 10.84.1.4
    ID DHCPv6 . . . . . : 234889627
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-51-52-00-00-21-9B-
    3E-ED-F8
    Servidores DNS. . . . . : 10.84.1.4
    10.32.0.98
    Servidor WINS principal . . . . . : 10.32.0.89
    NetBIOS sobre TCP/IP. . . . . : habilitado
```

- d. Cierre todas las ventanas del escritorio.

Parte 2: Identificar y utilizar los íconos de red de la bandeja del sistema

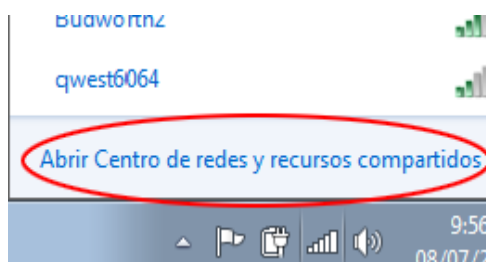
En la parte 2, utilizará los íconos de red de la bandeja del sistema para determinar y controlar las NIC de la PC.

Paso 1: Utilizar el ícono de red inalámbrica

- a. Haga clic en el ícono **Red inalámbrica** de la bandeja del sistema para visualizar la ventana emergente que muestra los SSID que están dentro del alcance de la NIC inalámbrica. Cuando la bandeja del sistema muestra el ícono Red inalámbrica, la NIC inalámbrica está activa.

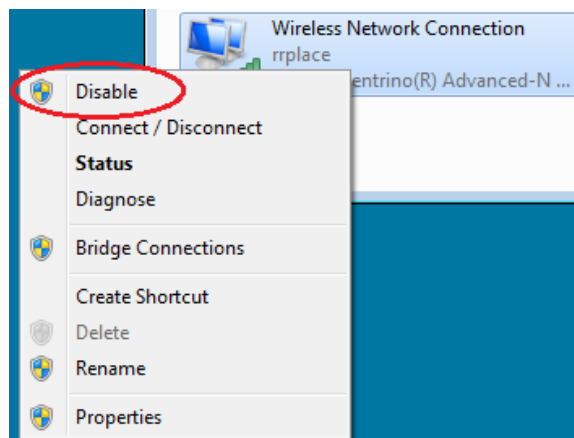


- b. Haga clic en el enlace **Abrir Centro de redes y recursos compartidos**. **Nota:** esta es una forma de método abreviado para abrir esta ventana.



- c. En el panel izquierdo, haga clic en el enlace **Cambiar configuración del adaptador** para visualizar la ventana Conexiones de red.

- d. Seleccione y haga clic con el botón secundario en **Conexión de red inalámbrica** y, a continuación, haga clic en **Deshabilitar** para deshabilitar la NIC inalámbrica.



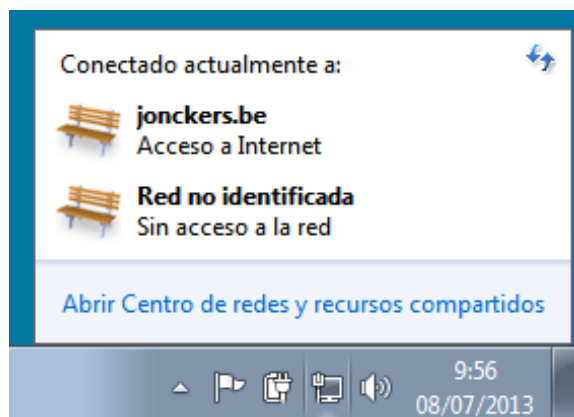
- e. Examine la bandeja del sistema. El ícono **Conexión de red inalámbrica** debe reemplazarse por el ícono **Red conectada por cable**, que indica que está utilizando la NIC conectada por cable para la conectividad de red.



Nota: si las dos NIC están activas, el ícono que se muestra es el de **Red inalámbrica**.

Paso 2: Utilizar el ícono de red conectada por cable

- a. Haga clic en el ícono **Red conectada por cable**. Observe que los SSID inalámbricos ya no se muestran en esta ventana emergente, pero aún puede acceder a la ventana Centro de redes y recursos compartidos desde aquí.



- b. Haga clic en el enlace **Abrir Centro de redes y recursos compartidos > Cambiar configuración del adaptador** y, a continuación, haga clic en **Habilitar** para habilitar la conexión de red inalámbrica. El ícono **Red inalámbrica** debe reemplazar el ícono **Red conectada por cable** en la bandeja del sistema.

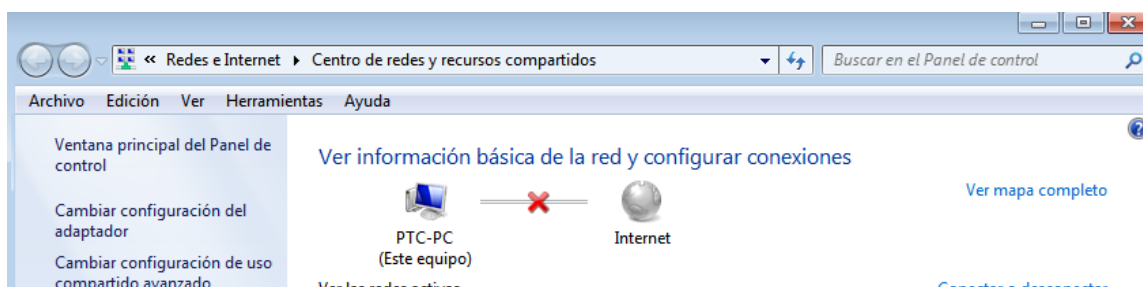


Paso 3: Identificar el ícono Problema de red

- En la ventana Conexiones de red, deshabilite **Conexión de red inalámbrica** y **Conexión de área local**.
- La bandeja del sistema ahora muestra el ícono **Red deshabilitada**, que indica que la conectividad de red está deshabilitada.



- Puede hacer clic en este ícono para volver a la ventana Centro de redes y recursos compartidos (examine el diagrama de red en la parte superior).



Puede hacer clic en la **X** roja para que la PC resuelva el problema con la conexión de red. La resolución de problemas intenta resolver el problema de red por usted.

- Si la resolución de problemas no habilitó una de las NIC, entonces debe hacerlo manualmente para restaurar la conectividad de red de la PC.

Nota: si está habilitado un adaptador de red y la tarjeta NIC no puede establecer la conectividad de red, aparece el ícono **Problema de red** en la bandeja del sistema.



Si aparece este ícono, puede resolver este problema tal como lo hizo en el paso 3c.

Reflexión

¿Por qué activaría más de una NIC en una PC?

Las respuestas pueden variar. Se pueden utilizar varias NIC si se necesita más de una ruta para la PC. Un ejemplo de esto sería si la PC se utiliza como servidor proxy.

Conectados (Versión para el instructor)

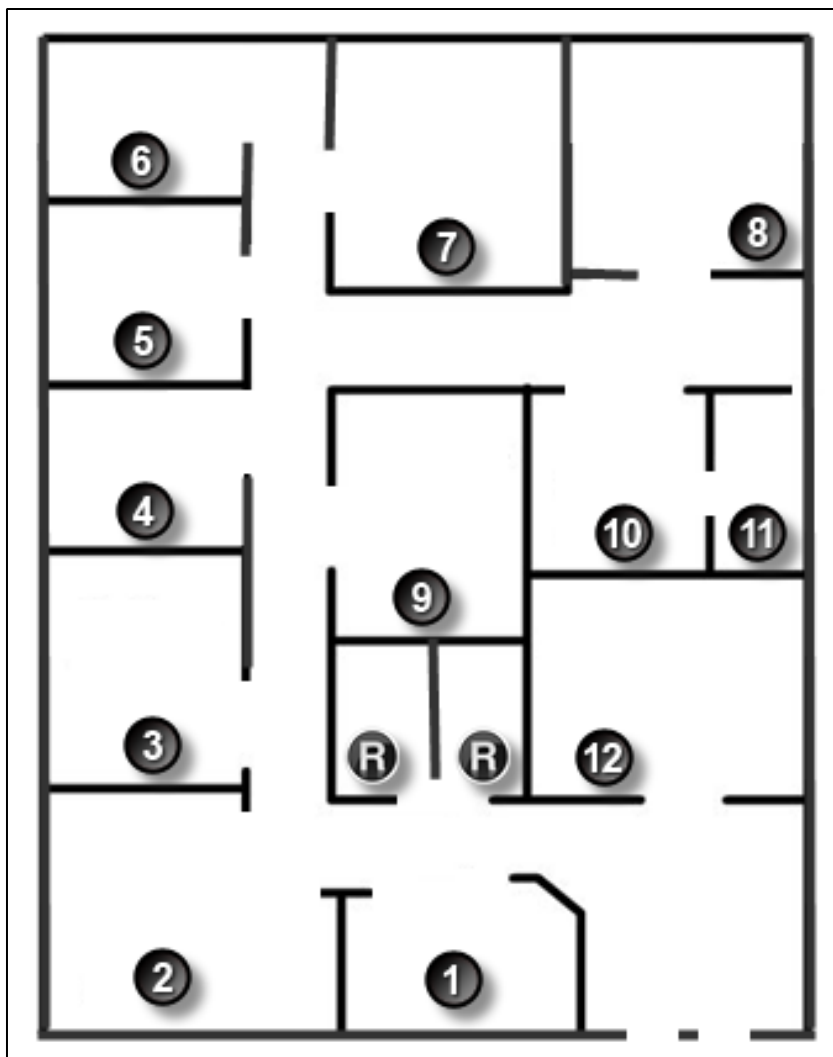
Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Conectar dispositivos utilizando medios conectados por cable e inalámbricos.

Los estudiantes asociarán sus ideas sobre cableado de red y tipo de tecnología a una topología física. Este capítulo se centra en la capa de acceso a la red, por lo que los estudiantes deberán preparar un modelo físico básico. Para esta actividad, se requieren esquemas no lógicos (de direccionamiento IP).

Topología física



Información básica/Situación

Nota: conviene realizar esta actividad en grupos de dos a tres estudiantes.

Su pequeña empresa se traslada a una nueva ubicación. El edificio es completamente nuevo, y usted debe presentar una topología física para que pueda iniciarse la instalación del puerto de red.

El instructor le proporcionará un anteproyecto creado para esta actividad. En el anteproyecto, el área indicada con el número 1 corresponde al área de recepción, y el área indicada con las letras RR corresponde al área de los baños.

Todas las salas están dentro de la categoría 6 de las especificaciones UTP (100 m), por lo que no debe preocuparse por adaptar el cableado del edificio al código. Cada sala del diagrama debe tener, al menos, una conexión de red disponible para usuarios o dispositivos intermediarios.

Junto con sus compañeros de equipo, indique lo siguiente en el plano:

- ¿Dónde ubicaría su instalación de distribución principal de red, teniendo en cuenta la seguridad?
- ¿Cuántos dispositivos intermediarios utilizaría y dónde los ubicaría?
- ¿Qué tipo de cableado utilizaría (UTP, STP, tecnología inalámbrica, fibra óptica, etc.) y dónde se ubicarían los puertos?
- ¿Qué tipos de dispositivos finales utilizaría (conectados por cable, inalámbricos, computadoras portátiles, computadoras de escritorio, tablet PC, etc.)?

No sea extremadamente detallista en el diseño. Simplemente, utilice el contenido del capítulo para poder justificar sus decisiones a la clase.

Notas para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes para que reflexionen acerca de su entendimiento de la capa de enlace de datos desde una perspectiva física (conectividad por cable e inalámbrica). Como resultado de esta actividad, se debe facilitar el debate.

Recursos necesarios

- Software Packet Tracer

Reflexión

1. ¿Dónde ubicaría su instalación de distribución principal de red, teniendo en cuenta la seguridad?

La sala 11 es la más pequeña y serviría perfectamente como la instalación de distribución principal o el centro de redes. Está ubicada lejos de las tuberías, lo que podría interferir con la calidad del cobre. También está ubicada lejos de la mayoría de las otras oficinas o salas por motivos de seguridad y tiene solo una puerta de entrada.

2. ¿Cuántos dispositivos intermediarios utilizaría y dónde los ubicaría?

Se podrían colocar uno o dos switches en la sala 11 para la escalabilidad y el acceso a los demás dispositivos finales. También se podría colocar un router en la sala 11 para la conectividad al ISP. Se podrían colocar uno o dos ISR inalámbricos en el diagrama, posiblemente en la sala 7 o 12, para el acceso inalámbrico en todo el espacio físico.

3. ¿Qué tipo de cableado utilizaría (UTP, STP, tecnología inalámbrica, fibra óptica, etc.) y dónde se ubicarían los puertos?

Cada sala incorporaría, por lo menos, un conector UTP para la conectividad del dispositivo intermediario o el acceso de un solo usuario. La sala de la red central (instalación de distribución principal) necesitaría más de un puerto de red, ya que se encarga de las conexiones internas (LAN) y de las conexiones externas (WAN). Para la WAN, probablemente se utilizaría fibra óptica para la conectividad ISP.

4. ¿Qué tipos de dispositivos finales utilizaría (conectados por cable, inalámbricos, computadoras portátiles, computadoras de escritorio, tablet PC, etc.)?
-

Si se tienen en cuenta las respuestas anteriores, se podría utilizar una combinación de dispositivos conectados por cable, computadoras portátiles inalámbricas, computadoras de escritorio, servidores, tablet PC, etc. En este modelo, se consideran la seguridad y la escalabilidad.

Identifique los elementos del modelo que corresponden a contenido del mundo real:

- Cuando se conecta una red a la capa de acceso a la red, se tiene en cuenta la seguridad de la red.
- También se consideran los tipos de cableado y los diferentes modos de tecnología al diseñar una red en la capa de acceso a la red.
- Las diferentes tecnologías de datos son opciones disponibles para los diseñadores, a fin de facilitar el flujo del tráfico de datos en la capa de acceso a la red.

Únase a mi círculo social (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Describir el impacto de solicitudes de ARP en el rendimiento de la red y el host.

Los estudiantes analizarán las maneras en que el direccionamiento local (origen y destino) es fundamental para la identificación de la comunicación de datos al utilizar mensajería, conferencias, envío de mensajes por correo electrónico e incluso juegos.

Información básica/Situación

Nota: esta actividad se puede completar en forma individual en clase o fuera de la clase.

Gran parte de nuestra comunicación de red se realiza mediante correo electrónico, mensajería (de texto o instantánea), contacto por video y publicaciones de medios sociales.

Para esta actividad, elija uno de los siguientes tipos de comunicaciones de red que utiliza:

- Mensajería de texto o instantánea
- Conferencias de audio o video
- Envío de mensajes por correo electrónico
- Juegos en línea

Ahora que seleccionó un tipo de comunicación de red, registre sus respuestas a las siguientes preguntas:

- ¿Existe un procedimiento que deba seguir para registrarse usted mismo y registrar a otras personas, a fin de formar una cuenta de comunicaciones? ¿Por qué piensa que se necesita un procedimiento?
- ¿Cómo inicia el contacto con la persona o las personas con quienes desea comunicarse?
- ¿Cómo puede garantizar que solamente las personas con quienes desea comunicarse reciban sus conversaciones? Esté preparado para comentar sus respuestas en clase.

Notas para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes para que reflexionen acerca de sus percepciones respecto de la identificación de hosts de origen y destino en comparación con los medios sociales. Las respuestas de los estudiantes deben generar un debate sobre cómo nos identificamos cuando nos comunicamos a través de estos tipos de redes.

Recursos necesarios

- Capacidades de registro (papel, tablet PC, etc.) para compartir los comentarios de reflexión con la clase.

Reflexión

1. ¿Existe un procedimiento que deba seguir para registrarse usted mismo y registrar a otras personas, a fin de formar una cuenta de comunicaciones? ¿Por qué piensa que se necesita un procedimiento?

En cada uno de estos servicios, trae a la persona con la que desea comunicarse “directamente a su red”. Esto lo hace para tener un contacto directo con sus corresponsales y poder comunicarse directamente, sin requerir de ningún intermediario para transmitir los mensajes entre usted y sus amigos en la red.

Esencialmente, al registrarse usted y a sus corresponsales en la lista de contactos, crea su propia red de comunicación (social).

Durante el proceso de registro, a usted, como persona con un nombre civil, se le asigna un identificador de usuario específico del servicio que lo identifica en el servicio de comunicación determinado. De la misma manera, cuando agrega a sus amigos a la lista de contactos, busca sus identificadores de usuario específico del servicio y los agrega a su lista de contactos. Este identificador puede tener diversos formatos: para el servicio de correo electrónico, es una dirección de correo electrónico; para las cuentas ICQ, es un número; para las cuentas de Skype, LinkedIn o Facebook, el identificador sería un nombre de usuario. Cada vez que se comunica con la persona, la selecciona en la lista de contactos por su nombre civil, y el sistema contacta al usuario mediante el identificador de usuario asociado. Una sola persona puede tener distintos identificadores de usuario, según a cuántas redes sociales esté suscrita.

En las redes de comunicación, existe un proceso similar. Si bien un nodo de red, por ejemplo, una PC, es una entidad única, puede tener varias tarjetas de interfaz de red (NIC). Cada NIC utiliza un identificador único diferente según la tecnología (las NIC Ethernet y Wi-Fi utilizan direcciones MAC; las tarjetas ATM utilizan identificadores de ruta y circuito de acceso virtual; las interfaces ISDN utilizan identificadores de terminales; las interfaces Frame Relay utilizan identificadores de circuito de enlace de datos; y hay muchos ejemplos más). En estas tecnologías, cuando accede a una red, se le puede asignar este identificador para su propia NIC (en especial, para ATM, Frame Relay o ISDN cuando el identificador se asignó dinámicamente en lugar de estar incorporado al hardware de la NIC). Además, estas tecnologías de red pueden requerir que se registre para poder comenzar a comunicarse (en Wi-Fi, tiene que autenticarse y asociarse a un punto de acceso determinado; en Ethernet, es posible que deba autenticarse). Por último, un nodo de red tiene que crear su propia lista de contactos para cada red a la que está conectado (para comunicarse con un punto diferente en la misma red, si conoce su identidad lógica, necesita saber bajo qué tipo de identificador de NIC se puede acceder al punto).

En las redes IP, este sería un proceso que consistiría en asociar la dirección IP del punto en la misma red con su dirección de capa de enlace de datos de la capa 2. En Ethernet y Wi-Fi, las dos tecnologías de red que más se utilizan, IP utiliza un protocolo de soporte denominado “protocolo de resolución de direcciones” (ARP) para realizar esta traducción.

2. ¿Cómo inicia el contacto con la persona o las personas con quienes desea comunicarse?

La secuencia de pasos exacta dependería del servicio que utiliza para comunicarse con su par. Sin embargo, siempre habrá pasos comunes. Primero, decide en qué red se puede acceder a su par. Segundo, busca el contacto de la persona en la lista de contactos y luego utiliza este contacto para enviar un mensaje a su par. Según el servicio, el mensaje será recibido solo por esta persona (como en los servicios de mensajería instantánea o correo electrónico) o podrá estar de hecho visible para otras personas de la red del destinatario (como en paneles de mensajes de LinkedIn o Facebook). No obstante, nunca existe la duda de quién es el destinatario propuesto.

En las redes IP, un nodo que envía un mensaje a otro nodo decide en qué red se encuentra directamente el punto, y luego realiza la traducción de la dirección IP de destino, o IP de siguiente salto, a la dirección de capa 2 para saber cómo direccionar la NIC de ese nodo. Luego, el mensaje se puede entregar solo a la NIC del destinatario (si hay, por ejemplo, switches en el trayecto entre el emisor y el receptor), o puede ser visto, de hecho, por otras estaciones (como en Wi-Fi, donde las estaciones pueden oírse entre sí).

3. ¿Cómo puede garantizar que solamente las personas con quienes desea comunicarse reciban sus conversaciones?

El principal requisito previo es que el mensaje esté dirigido inequívocamente a un solo destinatario previsto. Este es exactamente el propósito de usar una lista de contactos que asocie a personas individuales con sus identificadores de usuario únicos. De lo contrario, si no conociéramos el identificador de usuario del destinatario, tendríamos que enviar el mensaje a todos, y realizar efectivamente un broadcasting, o no podríamos enviar el mensaje en absoluto. En las redes IP, este objetivo se logra mediante la resolución de la dirección IP del destinatario (o siguiente salto) en su dirección única de capa 2 mediante ARP o un mecanismo similar. Por lo tanto, asegurarse de que el mensaje llegue al destino previsto, y solo a este, depende de la tecnología de red.

Algunas tecnologías no permiten enviar mensajes de una manera que impida que otros los vean. Por ejemplo, en las implementaciones de Ethernet con hubs o Wi-Fi, la transmisión siempre está visible para todos los nodos de la red. Si bien solo el destinatario previsto procesará de hecho el mensaje, los otros, no obstante, pueden verlo. Esto es similar a los paneles de mensajes en LinkedIn o Facebook, donde los mensajes, aunque estén dirigidos a un solo destinatario, pueden ser vistos por muchos usuarios o todos.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Diferentes tecnologías de redes sociales corresponden a diferentes tecnologías de red.
- Diferentes ID de usuario para una persona en particular, según la red social a la que está suscrita la persona, corresponden a un direccionamiento diferente de la capa 2 que utilizan distintas tecnologías de red.
- Las listas de contactos corresponden a las tablas donde están almacenadas las asignaciones de la capa 3 a la capa 2; por ejemplo, las tablas ARP en Ethernet o las tablas IP/DLCI en Frame Relay.
- Suscribirse a una red social corresponde al proceso de obtener un acceso a una red determinada y a la tecnología de red relacionada.
- Buscar una persona en la lista de contactos corresponde a las búsquedas en las tablas de asignación de la capa 3 a la capa 2.

Práctica de laboratorio: Visualización de direcciones MAC de dispositivos de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	No aplicable	No aplicable	No aplicable
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Establecer la topología e inicializar los dispositivos

- Configurar los equipos según la topología de la red.
- Inicializar y reiniciar el router y el switch, si es necesario.

Parte 2: Configurar dispositivos y verificar la conectividad

- Asignar una dirección IP estática a la NIC de la PC-A.
- Configurar la información básica en el R1.
- Asignar una dirección IP estática al R1.
- Verificar la conectividad de la red.

Parte 3: Mostrar, describir y analizar las direcciones MAC de Ethernet

- Analizar la dirección MAC para la PC-A.
- Analizar las direcciones MAC para el router R1.
- Visualizar la tabla de direcciones MAC en el switch S1.

Información básica/Situación

Cada dispositivo en una LAN Ethernet está identificado con una dirección MAC de la capa 2. Esta dirección se graba en la NIC. En esta práctica de laboratorio, se explorarán y analizarán los componentes que integran una dirección MAC, y cómo puede encontrar esta información en los diversos dispositivos de red, como un router, un switch y una PC.

Realizará el cableado de los equipos como se muestra en la topología. Luego, configurará el router y la PC según la tabla de direccionamiento. También probará la conectividad de red para verificar las configuraciones.

Una vez que los dispositivos estén configurados y que se haya verificado la conectividad de red, utilizará diferentes comandos para recuperar la información de los dispositivos y responder preguntas sobre los equipos de red.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: si utiliza routers distintos de los de las series 2900 o 1900, puede utilizar interfaces Fast Ethernet en lugar de interfaces Gigabit. Deberá ajustar los comandos **show** según corresponda.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red, borrará cualquier configuración, si fuera necesario, y configurará los parámetros básicos, como direcciones IP de la interfaz en el router y la PC.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

- a. Conecte los dispositivos que se muestran en la topología y realice el cableado según sea necesario.
- b. Encienda todos los dispositivos de la topología.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará la topología de la red y los parámetros básicos, como direcciones IP de la interfaz y el acceso a dispositivos. Para obtener información acerca de nombres y direcciones de dispositivos, consulte la topología y la tabla de direccionamiento.

Paso 1: Configurar la dirección IPv4 para la PC

- a. Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A.
- b. Haga ping a la dirección de gateway predeterminado del R1 desde el símbolo del sistema de la PC-A.
¿Tuvieron éxito los pings? ¿Por qué o por qué no?

No. La interfaz del router (gateway predeterminado) aún no se configuró y la interfaz G0/1 del router está inactiva.

Paso 2: Configurar el router.

- Acceda al router mediante el puerto de consola e introduzca el modo de configuración global.
- Asigne un nombre de host al router basado en la tabla de direccionamiento.
- Desactive la búsqueda del DNS.
- Configure y habilite la interfaz G0/1 en el router.

Paso 3: Verificar la conectividad de la red.

- Haga ping a la dirección de gateway predeterminado del R1 desde la PC-A.
¿Tuvieron éxito los pings?

Los pings deben tener éxito.

Parte 3: Mostrar, describir y analizar las direcciones MAC de Ethernet

Cada dispositivo en una LAN Ethernet tiene una dirección de control de acceso al medio (MAC) grabada en la tarjeta de interfaz de red (NIC). Las direcciones MAC de Ethernet tienen una longitud de 48 bits. Se muestran utilizando seis conjuntos de dígitos hexadecimales separados generalmente por guiones, dos puntos o puntos. En el siguiente ejemplo, se muestra la misma dirección MAC utilizando tres métodos de notación diferentes:

00-05-9A-3C-78-00

00:05:9A:3C:78:00

0005.9A3C.7800

Nota: las direcciones MAC también se denominan “direcciones físicas”, “direcciones de hardware” o “direcciones de hardware Ethernet”.

En la parte 3, emitirá comandos para mostrar las direcciones MAC en una PC, un router y un switch, y analizará las propiedades de cada uno.

Paso 1: Analizar la dirección MAC para la NIC de la PC-A

Antes de analizar la dirección MAC en la PC-A, veamos un ejemplo de una NIC de PC distinta. Puede emitir el comando **ipconfig /all** para ver la dirección MAC de las NIC. A continuación, se muestra un resultado en pantalla de ejemplo. Cuando utilice el comando **ipconfig /all**, tenga en cuenta que las direcciones MAC se denominan “direcciones físicas”. Si se lee la dirección MAC de izquierda a derecha, los primeros seis dígitos hexadecimales se refieren al proveedor (fabricante) de este dispositivo. Estos primeros seis dígitos hexadecimales (3 bytes) también se conocen como el “identificador único de organización” (OUI). La organización IEEE asigna este código de 3 bytes al proveedor. Para buscar al fabricante, puede utilizar una herramienta como www.macvendorlookup.com o ir al sitio Web de IEEE para buscar los códigos de proveedor OUI registrados. La dirección del sitio Web de IEEE para obtener información del OUI es <http://standards.ieee.org/develop/regauth/oui/public.html>. Los últimos seis dígitos corresponden al número de serie de la NIC asignados por el fabricante.

- a. Utilice el resultado del comando **ipconfig /all** para responder las siguientes preguntas.

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

¿Cuál es la porción del OUI de la dirección MAC para este dispositivo?

C8-0A-A9

¿Cuál es la porción del número de serie de la dirección MAC para este dispositivo?

FA-DE-0D

Utilice el ejemplo anterior para buscar el nombre del proveedor que fabricó esta NIC.

Quanta Computer Inc.

- b. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** e identifique la porción del OUI de la dirección MAC para la NIC de la PC-A.

Las respuestas varían según el fabricante.

Identifique la porción del número de serie de la dirección MAC para la NIC de la PC-A.

Las respuestas varían según código del número de serie del fabricante.

Identifique el nombre del proveedor que fabricó la NIC de la PC-A.

Las respuestas varían según el OUI del fabricante.

Paso 2: Analizar la dirección MAC para la interfaz G0/1 del R1

Puede utilizar una variedad de comandos para mostrar las direcciones MAC en el router.

- a. Acceda al R1 mediante el puerto de consola y utilice el comando **show interfaces g0/1** para buscar la información de la dirección MAC. A continuación, se presenta un ejemplo. Utilice los resultados que genera el router para contestar las preguntas.

```
R1> show interfaces g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 30f7.0da3.1821)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
Full Duplex, 100Mbps, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 3000 bits/sec, 4 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 15183 packets input, 971564 bytes, 0 no buffer
 Received 13559 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 301 multicast, 0 pause input
 1396 packets output, 126546 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
 195 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es la dirección MAC para la interfaz G0/1 en el R1?

Las respuestas variarán según el router que utilicen los estudiantes. Si se utiliza el resultado anterior, la respuesta sería 30f7.0da3.1821.

¿Cuál es el número de serie de la dirección MAC para G0/1?

Las respuestas variarán según el router que utilicen los estudiantes. Si se utiliza el resultado anterior, la respuesta sería a3-18-21.

¿Cuál es el OUI para G0/1?

Las respuestas varían según el router. Si se utiliza el resultado anterior, la respuesta sería 30-f7-0d.

Según este OUI, ¿cuál es el nombre del proveedor?

Cisco Systems

¿Qué significa BIA?

Dirección física

¿Por qué el resultado muestra la misma dirección MAC dos veces?

La dirección MAC puede cambiarse mediante un comando de software. La dirección real (BIA) aún estará presente y se muestra entre paréntesis.

- b. Otra forma de mostrar las direcciones MAC en el router es por medio del comando **show arp**. Utilice el comando **show arp** para mostrar la información de la dirección MAC. Este comando asigna la dirección de capa 2 a su correspondiente dirección de capa 3. A continuación, se presenta un ejemplo. Utilice los resultados que genera el router para contestar las preguntas.

```
R1> show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	30f7.0da3.1821	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	0	c80a.a9fa.de0d	ARPA	GigabitEthernet0/1

¿Qué direcciones de capa 2 se muestran en el R1?

Direcciones G0/1 del R1 y MAC de la PC-A Si el estudiante también registra direcciones MAC, las respuestas varían.

¿Qué direcciones de capa 3 se muestran en el R1?

Direcciones IP de R1 y PC-A

¿Por qué piensa que no se muestra información para el switch con el comando **show arp**?

El comando **show arp** asigna las direcciones de capa 2 a capa 3. El switch no tiene una dirección IP asignada.

Paso 3: Vea las direcciones MAC en el switch.

- a. Acceda al switch mediante el puerto de consola y utilice el comando **show interfaces** para los puertos 5 y 6 para mostrar la información de la dirección MAC. A continuación, se presenta un ejemplo. Utilice los resultados que genera el switch para contestar las preguntas.

```
Switch> show interfaces f0/5
```

```
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.7285 (bia 0cd9.96e8.7285)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:45, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    3362 packets input, 302915 bytes, 0 no buffer
    Received 265 broadcasts (241 multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 241 multicast, 0 pause input
```

```
0 input packets with dribble condition detected
38967 packets output, 2657748 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es la dirección MAC para la interfaz F0/5 en el switch?

Las respuestas varían. En el ejemplo anterior, la dirección MAC es 0cd9.96e8.7285.

Emita el mismo comando y anote la dirección MAC para F0/6.

Las respuestas varían.

¿Los OUI que se muestran en el switch son iguales a los que se mostraron en el router?

Las respuestas varían. Por lo general, la respuesta será negativa. Cisco Systems tiene muchos OUI registrados con la organización IEEE.

El switch rastrea los dispositivos mediante sus direcciones MAC de capa 2. En la topología, el switch conoce la dirección MAC del R1 y la dirección MAC de la PC-A.

- b. Emita el comando **show mac address-table** en el switch. A continuación, se presenta un ejemplo. Utilice los resultados que genera el switch para contestar las preguntas.

Nota para el instructor: El comando **show mac address-table** puede variar según el modelo de switch al que está conectado. Por ejemplo, la sintaxis en algunos switches es **show mac-address-table**.

```
Switch> show mac address-table
          Mac Address Table
-----
Vlan      Mac Address      Type      Ports
----      -
A11       0100.0ccc.cccc   STATIC    CPU
A11       0100.0ccc.cccd   STATIC    CPU
A11       0180.c200.0000   STATIC    CPU
A11       0180.c200.0001   STATIC    CPU
A11       0180.c200.0002   STATIC    CPU
A11       0180.c200.0003   STATIC    CPU
A11       0180.c200.0004   STATIC    CPU
A11       0180.c200.0005   STATIC    CPU
A11       0180.c200.0006   STATIC    CPU
A11       0180.c200.0007   STATIC    CPU
A11       0180.c200.0008   STATIC    CPU
A11       0180.c200.0009   STATIC    CPU
A11       0180.c200.000a   STATIC    CPU
A11       0180.c200.000b   STATIC    CPU
A11       0180.c200.000c   STATIC    CPU
A11       0180.c200.000d   STATIC    CPU
A11       0180.c200.000e   STATIC    CPU
```

```
All    0180.c200.000f    STATIC    CPU
All    0180.c200.0010    STATIC    CPU
All    ffff.ffff.ffff    STATIC    CPU
  1    30f7.0da3.1821    DYNAMIC    Fa0/5
  1    c80a.a9fa.de0d    DYNAMIC    Fa0/6
```

Total Mac Addresses for this criterion: 22

¿El switch mostró la dirección MAC de la PC-A? Si la respuesta fue afirmativa, ¿en qué puerto estaba?

Las respuestas variarán para la dirección MAC. En el ejemplo anterior, la dirección MAC sería c80a.a9fa.de0d. El puerto debe ser F0/6.

¿El switch mostró la dirección MAC del R1? Si la respuesta fue afirmativa, ¿en qué puerto estaba?

Las respuestas variarán para la dirección MAC. En el ejemplo anterior, la dirección MAC sería 30f7.0da3.1821. El puerto debe ser F0/5.

Reflexión

1. ¿Puede tener broadcasts en el nivel de capa 2? Si la respuesta es afirmativa, ¿cuál sería la dirección MAC?
-

Puede tener, y a menudo tiene, broadcasts en la capa 2. ARP utilizará los broadcasts para buscar la información de la dirección MAC. La dirección de broadcast es FF.FF.FF.FF.FF.FF.

2. ¿Por qué necesitaría saber la dirección MAC de un dispositivo?
-

Podría haber diversas razones. En una red grande, puede ser más sencillo identificar con precisión la ubicación y la identidad de un dispositivo mediante la dirección MAC en lugar de hacerlo mediante la dirección IP. El OUI de la dirección MAC indica el fabricante, lo que puede ayudar a restringir la búsqueda. Las medidas de seguridad se pueden aplicar en la capa 2, por lo que se necesita tener conocimiento de las direcciones MAC permitidas.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Configuración de dispositivos

Router R1

```
R1#sh run
Building configuration...

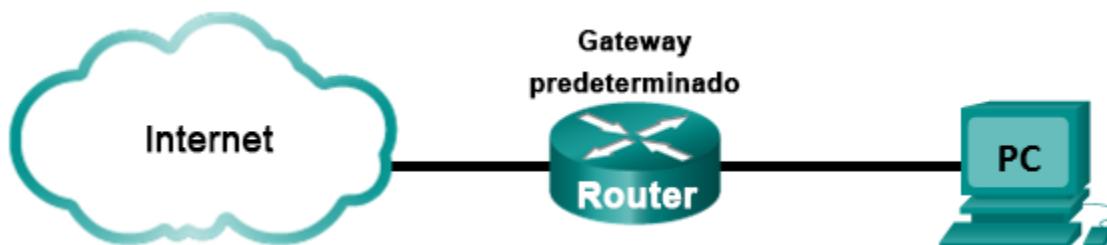
Current configuration : 1176 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ipv6 cef
!
no ip domain lookup
ip cef
multilink bundle-name authenticated
interface Embedded-Service-Engine0/0
no ip address
```

```
shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Práctica de laboratorio: Uso de Wireshark para examinar tramas de Ethernet (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Examinar los campos de encabezado en una trama de Ethernet II

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

Información básica/Situación

Cuando los protocolos de la capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas de interconexión de sistema abierto (OSI) y se encapsulan en la trama de la capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si los protocolos de capa superior son TCP e IP, y el acceso al medio es Ethernet, la encapsulación de la trama de la capa 2 será Ethernet II. Esto es típico de un entorno LAN.

Cuando se aprende sobre los conceptos de la capa 2, es útil analizar la información del encabezado de la trama. En la primera parte de esta práctica de laboratorio, revisará los campos incluidos en una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar los campos de encabezado de la trama de Ethernet II para el tráfico local y remoto.

Nota para el instructor: para esta práctica de laboratorio, se supone que el estudiante utiliza una PC con acceso a Internet. También se supone que Wireshark se instaló previamente en la PC. Las capturas de pantalla de esta práctica de laboratorio se tomaron de Wireshark v1.8.3 para Windows 7 (64 bits).

Recursos necesarios

- 1 PC (Windows 7, Vista o XP con acceso a Internet y Wireshark instalado)

Parte 1: Examinar los campos de encabezado en una trama de Ethernet II

En la parte 1, examinará los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de estos campos.

Paso 1: Revisar las descripciones y las longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Paso 2: Examinar la configuración de red de la PC

La dirección IP del host de esta PC es 10.20.164.22 y la dirección IP del gateway predeterminado es 10.20.164.17.

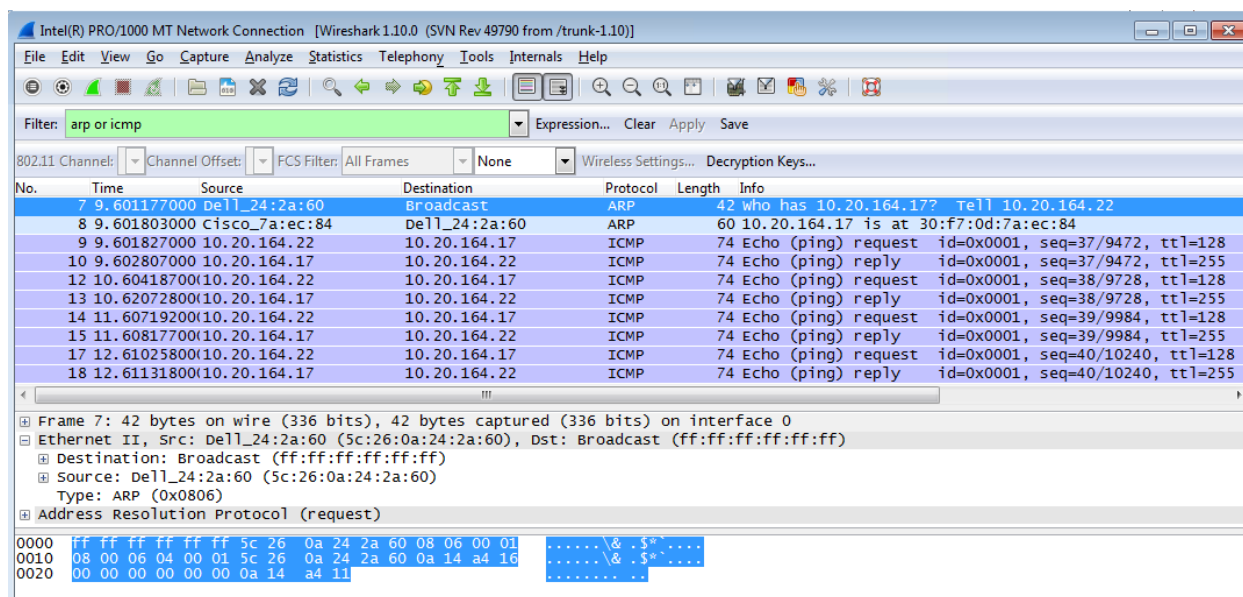
```

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . . : cisco.com
Vínculo: dirección IPv6 local. . . . . : fe80::b875:731b:3c7b:c0b1
Dirección IPv4. . . . . : 10.20.164.22
Máscara de subred . . . . . : 255.255.255.240
Puerta de enlace predeterminada . . . . . : 10.20.164.17
  
```

Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

En la siguiente captura de Wireshark, se muestran los paquetes que generó un ping que se emitió desde un host de la PC hasta su gateway predeterminado. Se aplicó un filtro a Wireshark para ver los protocolos ARP e ICMP únicamente. La sesión comienza con una consulta de ARP para la dirección MAC del router del gateway, seguida de cuatro solicitudes y respuestas de ping.



Paso 4: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP

En la tabla siguiente, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción						
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.						
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada como 12 dígitos hexadecimales, 0–9, A–F. Un formato común es 12:34:56:78:9A:BC. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC); los seis últimos números hexadecimales corresponden al número de serie de la NIC. La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast.						
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)							
Tipo de trama	0x0806	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior que admite Ethernet II. Dos tipos comunes de trama son: <table><tr><td>Valor</td><td>Descripción</td></tr><tr><td>0x0800</td><td>Protocolo IPv4</td></tr><tr><td>0x0806</td><td>Protocolo de resolución de direcciones (ARP)</td></tr></table>	Valor	Descripción	0x0800	Protocolo IPv4	0x0806	Protocolo de resolución de direcciones (ARP)
Valor	Descripción							
0x0800	Protocolo IPv4							
0x0806	Protocolo de resolución de direcciones (ARP)							
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 y 1,500 bytes.						
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica.						

¿Qué es importante acerca del contenido del campo de la dirección de destino?

Todos los hosts de la LAN recibirán esta trama de broadcast. El host con la dirección IP 10.20.164.17 (gateway predeterminado) enviará una respuesta unicast al origen (host de la PC). Esta respuesta contiene la dirección MAC de la NIC del gateway predeterminado.

¿Por qué la PC envía un broadcast de ARP antes de enviar la primera solicitud de ping?

Antes de que la PC pueda enviar una solicitud de ping a un host, necesita determinar la dirección MAC de destino para poder armar el encabezado de la trama para esa solicitud de ping. El broadcast de ARP se utiliza para solicitar la dirección MAC del host con la dirección IP incluida en el ARP.

¿Cuál es la dirección MAC del origen en la primera trama? 5c:26:0a:24:2a:60

¿Cuál es la ID de proveedor (OUI) de la NIC de origen? Dell

¿Qué parte de la dirección MAC es la OUI?

Los primeros tres octetos de la dirección MAC indican la OUI.

¿Cuál es el número de serie de la NIC de origen? 24:2a:60

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

En la parte 2, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego examinará la información incluida en los campos de encabezado de la trama.

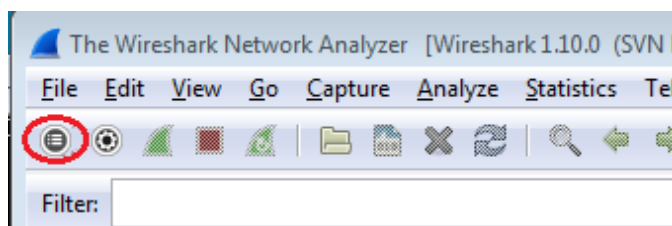
Paso 1: Determinar la dirección IP del gateway predeterminado en la PC

Abra una ventana del símbolo del sistema y emita el comando **ipconfig**.

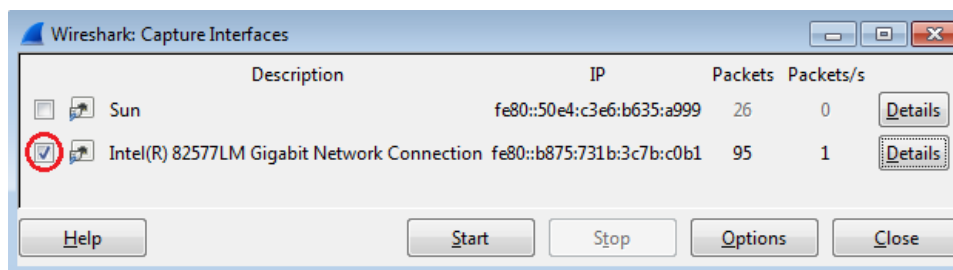
¿Cuál es la dirección IP del gateway predeterminado de la PC? Las respuestas varían.

Paso 2: Iniciar la captura de tráfico en la NIC de la PC

- Abra Wireshark.
- En la barra de herramientas de Wireshark Network Analyzer, haga clic en el ícono **Interface List** (Lista de interfaces).



- En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), seleccione la interfaz para iniciar la captura de tráfico haciendo clic en la casilla de verificación apropiada, y luego haga clic en **Start** (Comenzar). Si no está seguro de qué interfaz activar, haga clic en **Details** (Detalles) para obtener más información sobre cada interfaz enumerada.



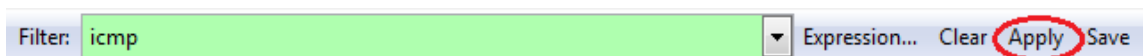
- Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).

Filter: Expression... Clear Apply Save									
802.11 Channels: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...									
No.	Time	Source	Destination	Protocol	Length	Info			
18	10.40268	10.20.164.22	10.20.164.22	ICMP	60	https > 62408 [ACK] Seq=1163 Ack=534 Win=16695 Len=0			
19	10.60449	10.20.164.22	10.20.164.22	TLSv1	587	Application Data			
20	10.80121	10.20.164.22	10.20.164.22	TCP	54	62408 > https [ACK] Seq=1163 Ack=534 Win=16695 Len=0			
21	11.04927	10.20.164.22	10.20.164.31	NBNS	92	Name query NB HP094B61<00>			
22	11.79926	10.20.164.22	10.20.164.31	NBNS	92	Name query NB HP094B61<00>			
23	12.03732	10.20.164.22	10.20.164.22	Spanning-tree-(for-br STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001			
24	12.06936	10.20.164.22	10.20.164.22	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.2			
25	14.03733	10.20.164.22	10.20.164.22	Spanning-tree-(for-br STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001			
26	16.03704	10.20.164.22	10.20.164.22	Spanning-tree-(for-br STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001			
27	18.03657	10.20.164.22	10.20.164.22	Spanning-tree-(for-br STP	60	Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001			
28	19.75046	10.20.164.22	70.42.228.171	TCP	66	62423 > https [SYN] Seq=0 win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1			
29	19.81045	10.20.164.22	70.42.228.171	TCP	66	https > 62423 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1260 SACK_PERM=1			
30	19.81054	10.20.164.22	70.42.228.171	TCP	54	62423 > https [ACK] Seq=1 Ack=1 win=66780 Len=0			

Paso 3: Filtrar Wireshark para mostrar solamente el tráfico de ICMP

Puede utilizar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra lo que se muestra en la pantalla. Por ahora, solo se debe ver el tráfico de ICMP.

En el cuadro **Filter** (Filtrar) de Wireshark, escriba **icmp**. Si escribió el filtro correctamente, el cuadro se volverá verde. Si el cuadro está de color verde, haga clic en **Apply** (Aplicar) para aplicar el filtro.

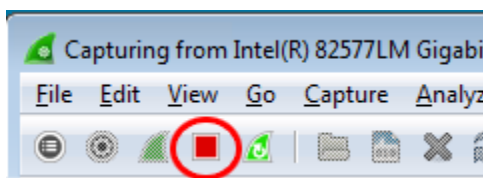


Paso 4: En la ventana del símbolo del sistema, haga ping al gateway predeterminado de la PC

En esta ventana, utilice la dirección IP que registró en el paso 1 para hacer ping al gateway predeterminado.

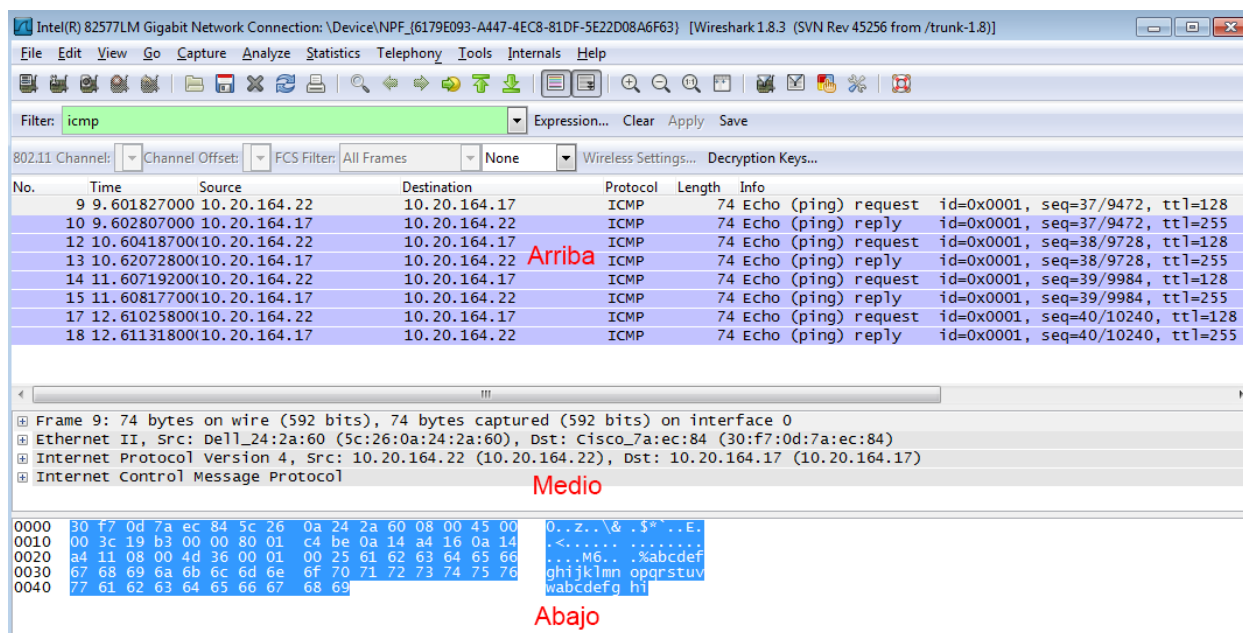
Paso 5: Detener la captura de tráfico en la NIC

Haga clic en el ícono **Stop Capture** (Detener captura) para detener la captura de tráfico.

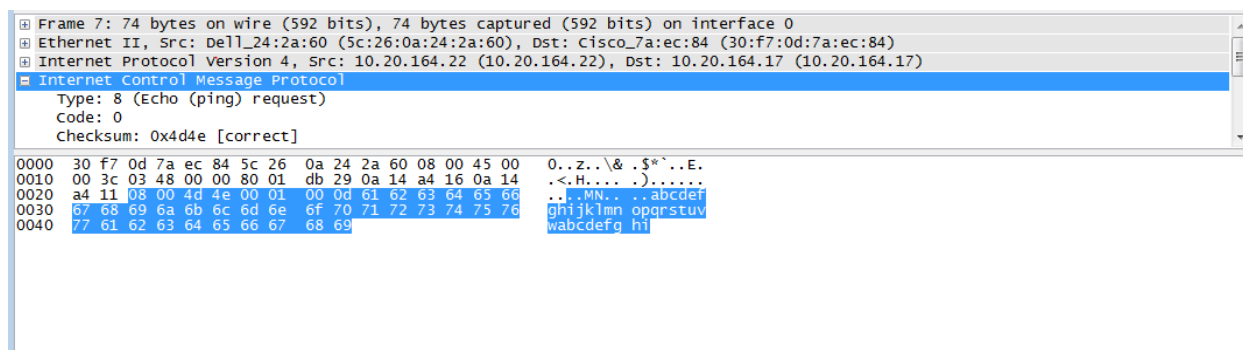


Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark

La ventana principal de Wireshark está dividida en tres secciones: el panel de la lista de paquetes (Arriba), el panel de detalles del paquete (Medio) y el panel de bytes del paquete (Abajo). Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark mostrará la información ICMP en el panel de la lista de paquetes de Wireshark, como se muestra en el ejemplo siguiente.



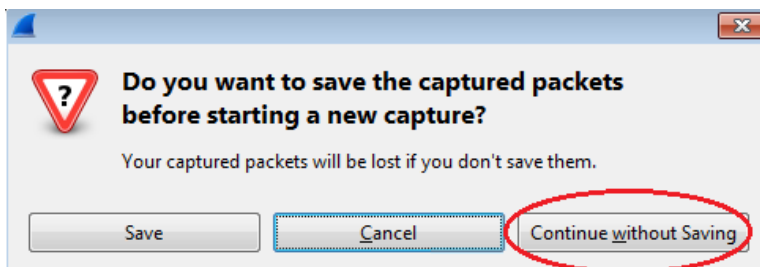
- En el panel de la lista de paquetes (sección superior), haga clic en la primera trama que se indica. Debería ver **Echo (ping) request** (Solicitud de eco [ping]) debajo del encabezado **Info** (Información). Esta acción debería resaltar la línea en color azul.
- Examine la primera línea del panel de detalles del paquete (sección media). En esta línea, se muestra la longitud de la trama; 74 bytes en este ejemplo.
- En la segunda línea del panel de detalles del paquete, se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y destino.
¿Cuál es la dirección MAC de la NIC de la PC? 5c:26:0a:24:2a:60 en el ejemplo.
¿Cuál es la dirección MAC del gateway predeterminado? 30:f7:0d:7a:ec:84 en el ejemplo.
- Puede hacer clic en el signo más (+) que se encuentra al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo más cambia al signo menos (-).
¿Qué tipo de trama se muestra? 0x0800 o un tipo de trama IPv4.
- Las dos últimas líneas que se muestran en la sección media proporcionan información sobre el campo de datos de la trama. Observe que los datos contienen la información de la dirección IPv4 de origen y destino.
¿Cuál es la dirección IP de origen? 10.20.164.22 en el ejemplo.
¿Cuál es la dirección IP de destino? 10.20.164.17 en el ejemplo.
- Puede hacer clic en cualquier línea de la sección media para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel de bytes del paquete (sección inferior). Haga clic en la línea **Internet Control Message Protocol** (Protocolo de mensajes de control de Internet) en la sección media y examine qué está resaltado en el panel de bytes del paquete.



- ¿Qué indican los dos últimos octetos resaltados? hi
- Haga clic en la trama siguiente de la sección superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y destino se invirtieron, porque esta trama se envió desde el router del gateway predeterminado como una respuesta al primer ping.
¿Qué dirección de dispositivo y dirección MAC se muestran como la dirección de destino?
La PC del host, 5c:26:0a:24:2a:60 en el ejemplo.

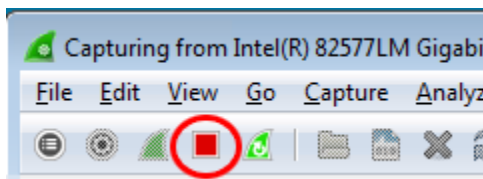
Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono **Start Capture** (Iniciar captura) para iniciar una nueva captura de Wireshark. Aparece una ventana emergente en la que se le pregunta si desea guardar los paquetes capturados anteriormente en un archivo antes de iniciar una nueva captura. Haga clic en **Continue without Saving** (Continuar sin guardar).



Paso 8: En la ventana del símbolo del sistema, hacer ping a www.cisco.com

Paso 9: Detener la captura de paquetes



Paso 10: Examinar los datos nuevos en el panel de la lista de paquetes de Wireshark

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y destino?

Origen: _____ Debería ser la dirección MAC de la PC.

Destino: _____ Debería ser la dirección MAC del gateway predeterminado.

¿Cuáles son las direcciones IP de origen y destino incluidas en el campo de datos de la trama?

Origen: _____ Sigue siendo la dirección IP de la PC.

Destino: _____ Es la dirección del servidor en www.cisco.com.

Compare estas direcciones con las direcciones que recibió en el paso 7. La única dirección que cambió es la dirección IP de destino. ¿Por qué la dirección IP de destino cambió y la dirección MAC de destino siguió siendo la misma?

Las tramas de la capa 2 nunca dejan la LAN. Cuando se emite un ping a un host remoto, el origen utiliza la dirección MAC del gateway predeterminado para el destino de la trama. El gateway predeterminado recibe el paquete, quita de este la información de la trama de la capa 2 y, a continuación, crea un nuevo encabezado de trama con una dirección MAC de siguiente salto. Este proceso continúa de router a router hasta que el paquete llega a la dirección IP de destino.

Reflexión

Wireshark no muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

El campo de preámbulo contiene siete octetos de secuencias 1010 alternas y un octeto que indica el comienzo de la trama, 10101011.

Práctica de laboratorio: Observación del protocolo ARP mediante la CLI de Windows, la CLI del IOS y Wireshark (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

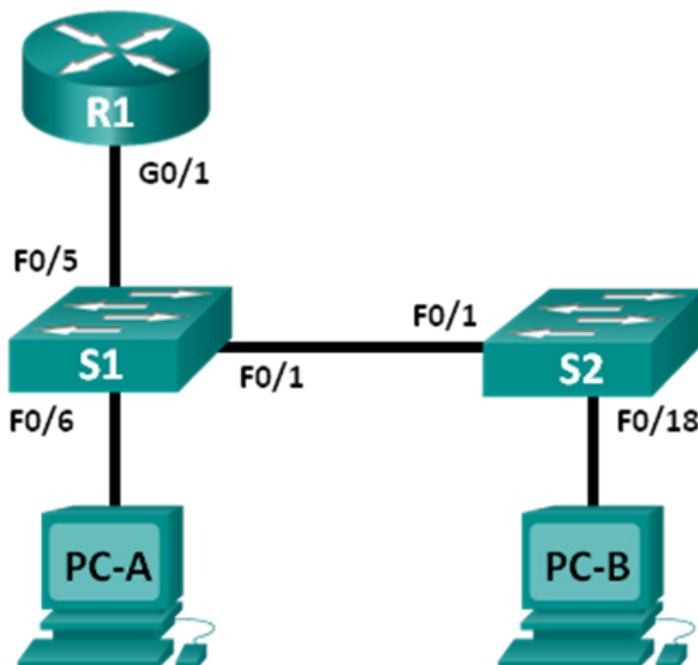


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Armar y configurar la red

Parte 2: Utilizar el comando ARP de Windows

Parte 3: Utilizar el comando show ARP del IOS

Parte 4: Utilizar Wireshark para examinar los intercambios ARP

Información básica/Situación

TCP/IP utiliza el protocolo de resolución de direcciones (ARP) para asignar una dirección IP de capa 3 a una dirección MAC de capa 2. Cuando se coloca una trama en la red, debe tener una dirección MAC de destino. Para descubrir dinámicamente la dirección MAC del dispositivo de destino, se transmite una solicitud de ARP en la LAN. El dispositivo que contiene la dirección IP de destino responde, y la dirección MAC se registra en la caché ARP. Cada dispositivo en la LAN mantiene su propio caché ARP, o un área pequeña en RAM que contiene los resultados ARP. Un cronómetro de caché de ARP elimina las entradas ARP que no se han usado por un determinado período de tiempo.

ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN. Por el contrario, los tiempos de espera ilimitados podrían provocar errores con dispositivos que dejan la red o cambian la dirección de la Capa 3.

Un administrador de red debe estar al tanto del ARP, pero es posible que no interactúe con el protocolo regularmente. ARP es un protocolo que permite que los dispositivos de red se comuniquen con el protocolo TCP/IP. Sin ARP no hay un método eficiente para construir el datagrama de la dirección de destino de la Capa 2. También, ARP es un riesgo de seguridad potencial. La suplantación de identidad de ARP, o envenenamiento de ARP, es una técnica usada por un atacante para inyectar una dirección MAC incorrecta asociada a una red. Un atacante falsifica la dirección MAC de un dispositivo y las tramas son enviadas a un destino equivocado. Configurar manualmente asociaciones ARP estáticas es una manera de impedir la suplantación de identidad de ARP. Por último, se puede configurar una lista de direcciones MAC autorizadas en los dispositivos Cisco para restringir el acceso a la red solo a los dispositivos aprobados.

En esta práctica de laboratorio, utilizará los comandos ARP tanto en los routers Windows como Cisco para visualizar la tabla ARP. También borrará la caché ARP y agregará entradas ARP estáticas.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbase9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: algunos de los comandos ARP en Windows Vista o en sistemas operativos posteriores requieren privilegios de administrador.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbase9 o comparable])
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal instalado, por ejemplo, Tera Term y Wireshark)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Fast Ethernet en los switches Cisco 2960 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre los switches S1 y S2. Si utiliza otro modelo de switch Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: Armar y configurar la red

Paso 1: Tender el cableado de red de acuerdo con la topología

Paso 2: Configurar las direcciones IP de los dispositivos de acuerdo con la tabla de direccionamiento

Paso 3: Verificar la conectividad de red haciendo ping a todos los dispositivos de la PC-B

Parte 2: Usar el comando ARP de Windows

El comando **arp** permite al usuario ver y modificar la caché ARP en Windows. A este comando se accede desde el símbolo del sistema de Windows.

Paso 1: Visualizar la caché ARP

- a. Abra una ventana de comandos en la PC-A y escriba **arp**.

```
C:\Users\User1> arp
```

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

```
ARP -s inet_addr eth_addr [if_addr]
```

```
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr] [-v]
```

-a Displays current ARP entries by interrogating the current protocol data. If `inet_addr` is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as **-a**.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.

`inet_addr` Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by `if_addr`.

-d Deletes the host specified by `inet_addr`. `inet_addr` may be wildcarded with `*` to delete all hosts.

-s Adds the host and associates the Internet address `inet_addr` with the Physical address `eth_addr`. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

`eth_addr` Specifies a physical address.

`if_addr` If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
```

```
> arp -a .... Displays the arp table.
```

- b. Observe el resultado.

¿Qué comando se usaría para mostrar todas las entradas en la caché ARP?

```
arp -a
```

¿Qué comando se usaría para eliminar todas las entradas de la caché ARP (purgar la caché ARP)?

```
arp -d *
```

¿Qué comando se usaría para eliminar la entrada de la caché ARP para 192.168.1.11?

```
arp -d 192.168.1.11
```

- c. Escriba **arp -a** para visualizar la tabla ARP.

```
C:\Users\User1> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
    Internet Address      Physical Address      Type
    192.168.1.1           d4-8c-b5-ce-a0-c1    dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
```

Nota: la tabla ARP está vacía si utiliza Windows XP (como se muestra a continuación).

```
C:\Documents and Settings\User1> arp -a
```

```
No ARP Entries Found.
```

- d. Haga ping de la PC-A a la PC-B para agregar dinámicamente entradas de la caché ARP.

```
C:\Documents and Settings\User1> ping 192.168.1.2
```

```
Interface: 192.168.1.3 --- 0xb
    Internet Address      Physical Address      Type
    192.168.1.2           00-50-56-be-f6-db    dynamic
```

¿Cuál es la dirección física para el host con dirección IP 192.168.1.2?

```
00-50-56-be-f6-db
```

Paso 2: Ajustar las entradas en la caché ARP manualmente

Para eliminar las entradas en la caché ARP, emita el comando **arp -d {inet-addr | *}**. Las direcciones se pueden eliminar de manera individual al especificar la dirección IP, o bien todas juntas con el wildcard *.

Verifique que la caché ARP contenga las entradas siguientes: el gateway predeterminado R1 G0/1 (192.168.1.1), la PC-B (192.168.1.2) y los dos switches (192.168.1.11 y 192.168.1.12).

- a. En la PC-A, haga ping a todas las direcciones de la tabla de direcciones.

- b. Verifique que todas las direcciones se hayan agregado a la caché ARP. Si la dirección no está en la caché ARP, haga ping a la dirección de destino y verifique que se haya agregado a la caché ARP.

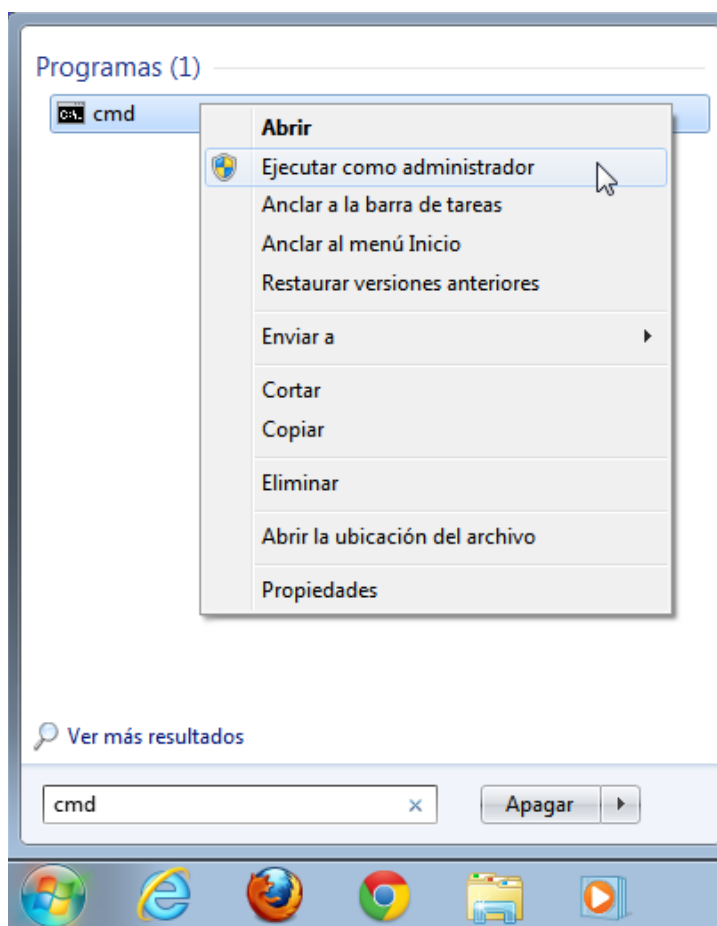
```
C:\Users\User1> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.1	d4-8c-b5-ce-a0-c1	dynamic
192.168.1.2	00-50-56-be-f6-db	dynamic
192.168.1.11	0c-d9-96-e8-8a-40	dynamic
192.168.1.12	0c-d9-96-d2-40-40	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

- c. Como administrador, acceda al símbolo del sistema. Haga clic en el ícono **Inicio** y, en el cuadro *Buscar programas y archivo*, escriba **cmd**. Cuando aparezca el ícono **cmd**, haga clic con el botón secundario en él y seleccione **Ejecutar como administrador**. Haga clic en **Sí** para permitir que este programa realice los cambios.

Nota: para los usuarios de Windows XP, no es necesario tener privilegios de administrador para modificar las entradas de la caché ARP.



- d. En la ventana del símbolo del sistema Administrador, escriba **arp -d ***. Este comando elimina todas las entradas de la caché ARP. Verifique que todas las entradas de la caché ARP se hayan eliminado; para eso, escriba **arp -a** en el símbolo del sistema.

```
C:\windows\system32> arp -d *
```

```
C:\windows\system32> arp -a
```

```
No ARP Entries Found.
```

- e. Espere unos minutos. El protocolo de descubrimiento de vecinos comienza a llenar la caché ARP nuevamente.

```
C:\Users\User1> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.255	ff-ff-ff-ff-ff-ff	static

Nota: el protocolo de descubrimiento de vecinos no está implementado en Windows XP.

- f. En la PC-A, haga ping a la PC-B (192.168.1.2) y a los switches (192.168.1.11 y 192.168.1.12) para agregar las entradas ARP. Verifique que las entradas ARP se hayan agregado a la caché.

```
C:\Users\User1> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.2	00-50-56-be-f6-db	dynamic
192.168.1.11	0c-d9-96-e8-8a-40	dynamic
192.168.1.12	0c-d9-96-d2-40-40	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static

- g. Registre la dirección física del switch S2.

Las respuestas varían. 0c-d9-96-d2-40-40 en este caso.

- h. Elimine una entrada de caché ARP específica escribiendo **arp -d inet-addr**. En el símbolo del sistema, escriba **arp -d 192.168.1.12** para eliminar la entrada ARP para el S2.

```
C:\windows\system32> arp -d 192.168.1.12
```

- i. Escriba **arp -a** para verificar que la entrada ARP para el S2 se eliminó de la caché ARP.

```
C:\Users\User1> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.2	00-50-56-be-f6-db	dynamic
192.168.1.11	0c-d9-96-e8-8a-40	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static

- j. Puede agregar una entrada de caché ARP específica escribiendo **arp -s inet_addr mac_addr**. En este ejemplo, se utilizará la dirección IP y la dirección MAC para el S2. Use la dirección MAC registrada en el paso g.

```
C:\windows\system32> arp -s 192.168.1.12 0c-d9-96-d2-40-40
```

- k. Verifique que la entrada ARP para el S2 se haya agregado a la caché.

Parte 3: Utilizar el comando show arp del IOS

Cisco IOS también puede mostrar la caché ARP en los routers y switches mediante el comando **show arp** o **show ip arp**.

Paso 1: Mostrar las entradas ARP del router R1

```
R1# show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	d48c.b5ce.a0c1	ARPA	GigabitEthernet0/1
Internet	192.168.1.2	0	0050.56be.f6db	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	0	0050.56be.768c	ARPA	GigabitEthernet0/1

```
R1#
```

Observe que no hay ningún valor de Age (-) para la primera entrada, la interfaz del router G0/1 (el gateway predeterminado de LAN). Age es la cantidad de minutos (min) que la entrada estuvo en la caché ARP y se incrementa para las otras entradas. El protocolo de descubrimiento de vecinos llena las entradas ARP de las direcciones IP y MAC de la PC-A y la PC-B.

Paso 2: Agregar entradas ARP del router R1

Puede agregar entradas ARP a la tabla ARP del router haciendo ping a otros dispositivos.

- a. Haga ping al switch S1.

```
R1# ping 192.168.1.11
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:

```
.!!!!
```

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

- b. Verifique que una entrada ARP para el switch S1 se haya agregado a la tabla ARP del R1.

```
R1# show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	d48c.b5ce.a0c1	ARPA	GigabitEthernet0/1
Internet	192.168.1.2	6	0050.56be.f6db	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	6	0050.56be.768c	ARPA	GigabitEthernet0/1
Internet	192.168.1.11	0	0cd9.96e8.8a40	ARPA	GigabitEthernet0/1

```
R1#
```

Paso 3: Mostrar las entradas ARP del switch S1

```
S1# show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	46	d48c.b5ce.a0c1	ARPA	Vlan1
Internet	192.168.1.2	8	0050.56be.f6db	ARPA	Vlan1
Internet	192.168.1.3	8	0050.56be.768c	ARPA	Vlan1
Internet	192.168.1.11	-	0cd9.96e8.8a40	ARPA	Vlan1

```
S1#
```

Paso 4: Agregar entradas ARP en el switch S1

Al hacer ping a otros dispositivos, también se puede agregar entradas ARP a la tabla ARP del switch.

- a. En el switch S1, haga ping al switch S2.

```
S1# ping 192.168.1.12
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:

```
.!!!!
```

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms

- b. Verifique que la entrada ARP para el switch S2 se haya agregado a la tabla ARP del S1.

S1# **show ip arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	5	d48c.b5ce.a0c1	ARPA	Vlan1
Internet	192.168.1.2	11	0050.56be.f6db	ARPA	Vlan1
Internet	192.168.1.3	11	0050.56be.768c	ARPA	Vlan1
Internet	192.168.1.11	-	0cd9.96e8.8a40	ARPA	Vlan1
Internet	192.168.1.12	2	0cd9.96d2.4040	ARPA	Vlan1

S1#

Parte 4: Utilizar Wireshark para examinar los intercambios ARP

En la parte 4, examinará los intercambios ARP mediante Wireshark para capturar y evaluar el intercambio ARP. También examinará la latencia de red que causan los intercambios ARP entre los dispositivos.

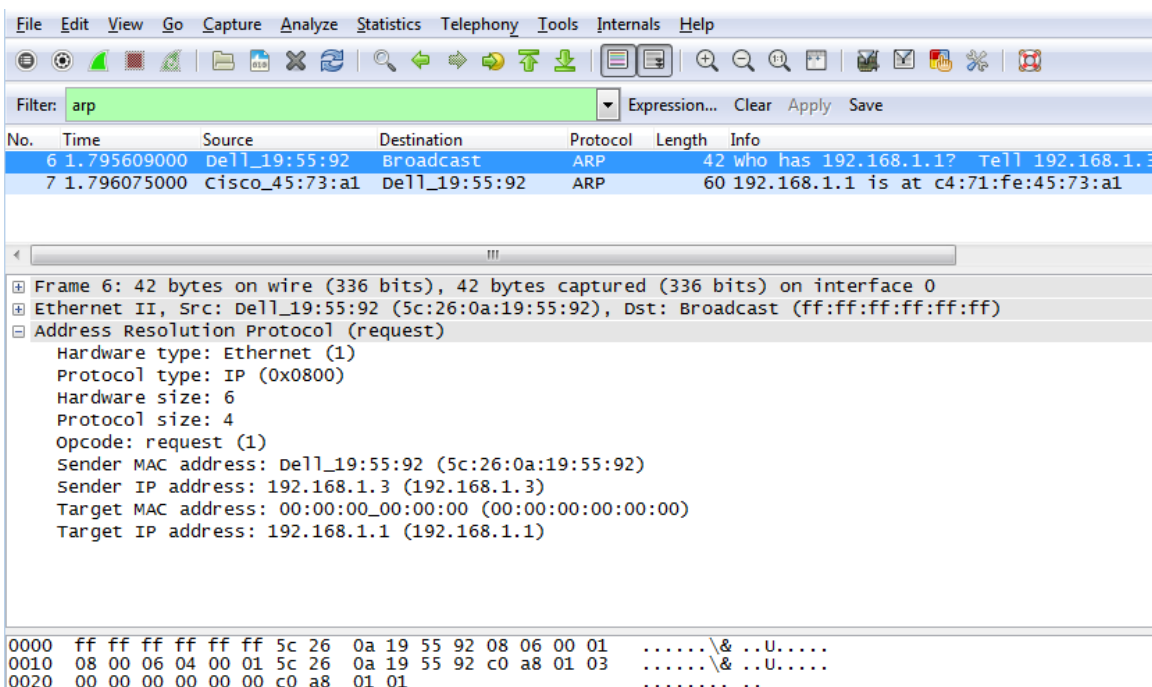
Paso 1: Configurar Wireshark para las capturas de paquetes

- Inicie Wireshark.
- Elija la interfaz de red que desea usar para capturar los intercambios ARP.

Paso 2: Capturar y evaluar las comunicaciones del ARP

- Inicie la captura de paquetes en Wireshark. Utilice el filtro para mostrar solamente los paquetes ARP.
- Purgue la caché ARP; para eso, escriba el comando **arp -d *** en el símbolo del sistema.
- Verifique que la caché ARP se haya borrado.
- Envíe un ping al gateway predeterminado mediante el comando **ping 192.168.1.1**.
- Después de hacer ping al gateway predeterminado, detenga la captura de Wireshark.
- Examine las capturas de Wireshark para los intercambios ARP en el panel de detalles del paquete.

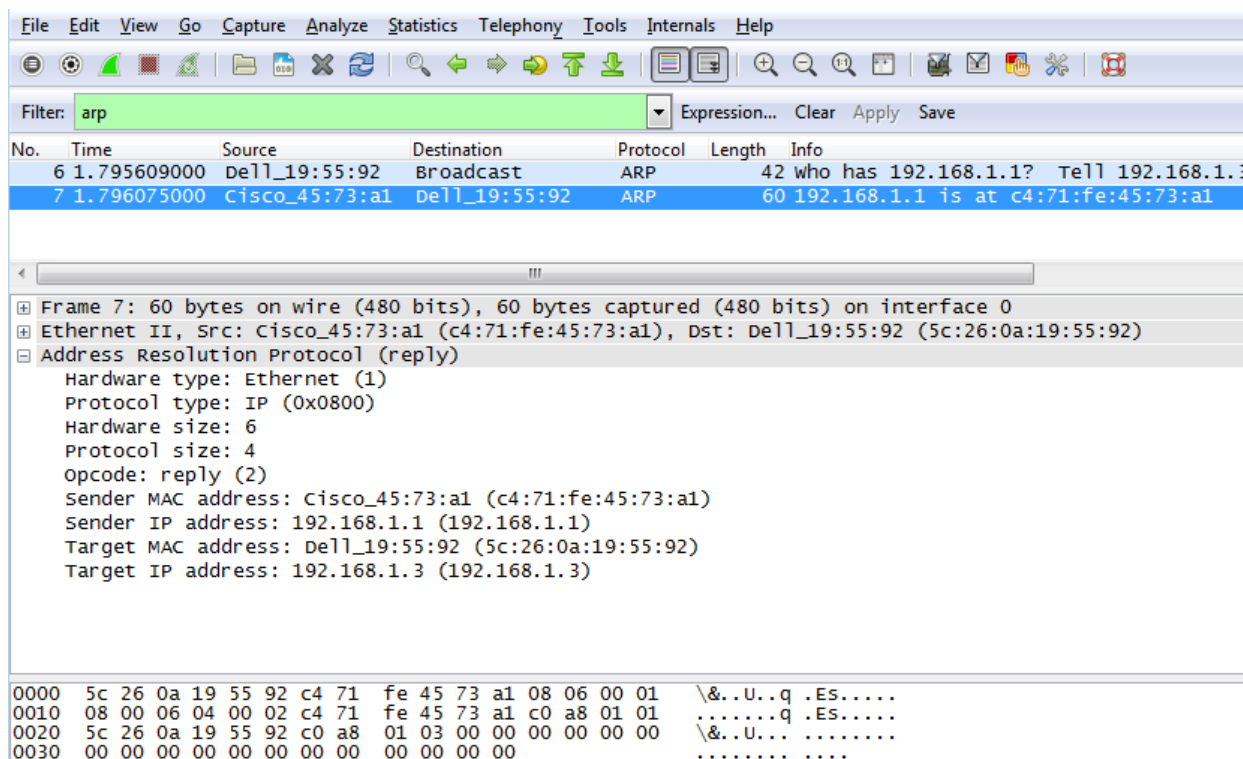
¿Cuál fue el primer paquete de ARP? _____ Solicitud de ARP



Complete la siguiente tabla con información sobre el primer paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	5C:26:0A:19:55:92 - Las respuestas varían.
Dirección IP del emisor	192.168.1.3
Dirección MAC de destino	00:00:00:00:00:00
Dirección IP de destino	192.168.1.1

¿Cuál fue el segundo paquete de ARP? Respuesta de ARP



Complete la siguiente tabla con información sobre el segundo paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	C4:71:FE:45:73:A1. Las respuestas varían.
Dirección IP del emisor	192.168.1.1
Dirección MAC de destino	5C:26:0A:19:55:92 - Las respuestas varían.
Dirección IP de destino	192.168.1.3

Paso 3: Examinar la latencia de red que causa el ARP

- Borre las entradas ARP de la PC-A.
- Inicie una captura de Wireshark.

- c. Haga ping al switch S2 (192.168.1.12). El ping debe ser correcto después de la primera solicitud de eco.

Nota: si todos los pings son correctos, el S1 debe volver a cargarse para observar la latencia de red con el ARP.

```
C:\Users\User1> ping 192.168.1.12
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

- d. Una vez finalizado el ping, detenga la captura de Wireshark. Utilice el filtro de Wireshark para mostrar solamente los resultados de ARP e ICMP. En Wireshark, escriba **arp o icmp** en el área de entrada **Filter:** (Filtro:).
- e. Examine la captura de Wireshark. En este ejemplo, la trama 10 es la primera solicitud de ICMP que se envía de la PC-A al S1. Dado que no hay una entrada ARP para el S1, se envió una solicitud de ARP a la dirección IP de administración del S1 en la que se solicita la dirección MAC. Durante los intercambios ARP, la solicitud de eco no recibió una respuesta antes de agotarse el tiempo de espera de la solicitud. (Tramas 8 a 12)

Después de que la entrada ARP para el S1 se agregó a la caché ARP, los últimos tres intercambios ICMP fueron correctos, como se muestra en las tramas 26, 27 y 30-33.

Como se muestra en la captura de Wireshark, ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN.

No.	Time	Source	Destination	Protocol	Length	Info
8	1.649929000	Dell_19:55:92	Broadcast	ARP	42	who has 192.168.1.12? Tell 192.168.1.3
9	1.651202000	Cisco_59:91:c0	Dell_19:55:92	ARP	60	192.168.1.12 is at 00:23:5d:59:91:c0
10	1.651489000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1873
11	1.653790000	Cisco_59:91:c0	Broadcast	ARP	60	who has 192.168.1.3? Tell 192.168.1.12
12	1.653999000	Dell_19:55:92	Cisco_59:91:c0	ARP	42	192.168.1.3 is at 5c:26:0a:19:55:92
26	6.562409000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1874
27	6.564426000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1874
30	7.560977000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1875
31	7.563586000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1875
32	8.559352000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1876
33	8.560466000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1876

Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Dell_19:55:92 (5c:26:0a:19:55:92), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Dell_19:55:92 (5c:26:0a:19:55:92)

Sender IP address: 192.168.1.3 (192.168.1.3)

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.1.12 (192.168.1.12)

0000	ff ff ff ff ff ff	5c 26 0a 19 55 92	08 06 00 01	\& ..U.....
0010	08 00 06 04 00 01	5c 26 0a 19 55 92	c0 a8 01 03	\& ..U.....
0020	00 00 00 00 00 00	c0 a8 01 0c		

Reflexión

- ¿Cómo y cuándo se quitan las entradas ARP estáticas?

Se eliminan manualmente.

- ¿Por qué desea agregar entradas ARP estáticas en la caché?

Una entrada ARP estática puede mitigar el envenenamiento o la suplantación ARP en la red.

- Si las solicitudes ARP pueden causar latencia de red, ¿por qué no es conveniente tener tiempos de espera ilimitados para las entradas ARP?

Los tiempos de espera ilimitados podrían provocar errores con dispositivos que dejan la red o cambian la dirección de capa 3.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos

Router R1

```
R1#show run
Building configuration...

Current configuration : 1165 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 15
!
!
```

```
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
no ip address  
shutdown  
clock rate 2000000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!
```

```
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login  
  transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

Switch S1

```
S1#show run  
Building configuration...  
  
Current configuration : 1305 bytes  
!  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
system mtu routing 1500  
!  
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip http server
 ip http secure-server
!
!
!
line con 0
line vty 5 15
!
end
```

Switch S2

```
S2#show run
Building configuration...

Current configuration : 1313 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
```

```
!  
no aaa new-model  
system mtu routing 1500  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!
```

```
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.12 255.255.255.0
!
ip http server
ip http secure-server
!
!
line con 0
line vty 5 15
!
end
```


Práctica de laboratorio: Uso de la CLI del IOS con las tablas de direcciones MAC del switch (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

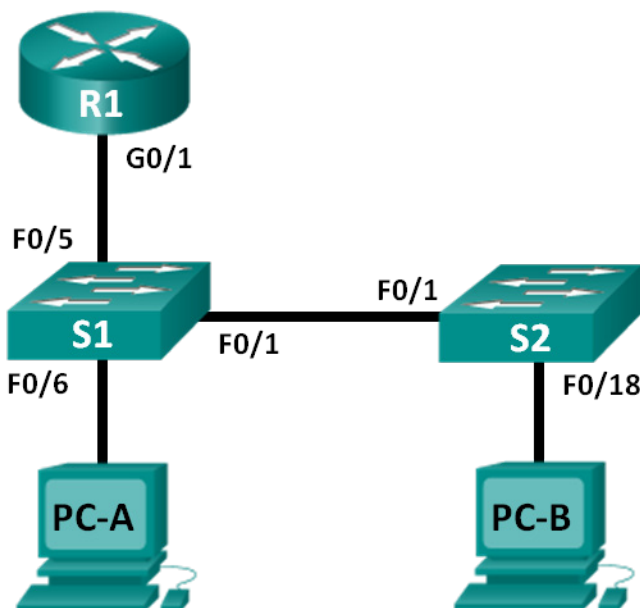


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Armar y configurar la red

- Tender el cableado de red de acuerdo con el diagrama de topología.
- Configurar los dispositivos de red de acuerdo con la tabla de direccionamiento.

Parte 2: Examinar la tabla de direcciones MAC del switch

- Utilizar los comandos **show** para observar el proceso para crear la tabla de direcciones MAC del switch.

Información básica/Situación

El propósito de un switch LAN de capa 2 es enviar tramas de Ethernet a dispositivos host en la red local. El switch registra las direcciones MAC del host que pueden verse en la red y asigna esas direcciones MAC a sus propios puertos del switch Ethernet. Este proceso se denomina “creación de la tabla de direcciones MAC”. Cuando un switch recibe una trama de una PC, examina las direcciones MAC de origen y destino de la trama. La dirección MAC de origen se registra y se asigna al puerto del switch de donde provino. Luego, se busca la dirección MAC de destino en la tabla de direcciones MAC. Si la dirección MAC de destino es una dirección conocida, entonces la trama se reenvía fuera del puerto del switch correspondiente de la dirección MAC. Si la dirección MAC es desconocida, entonces la trama se transmite fuera de todos los puertos del switch, excepto del que provino. Es importante observar y comprender la función de un switch y la forma en que entrega los datos en la red. La forma en que un switch actúa tiene consecuencias para los administradores de red cuya tarea es garantizar una comunicación de red segura y uniforme.

Los switches se utilizan para interconectar PC y entregar información a estas en las redes de área local. Los switches proporcionan las tramas de Ethernet a los dispositivos host identificados por las direcciones MAC de la tarjeta de interfaz de red.

En la parte 1, armará una topología de varios routers y varios switches con un enlace troncal que une los dos switches. En la parte 2, hará ping a diversos dispositivos y observará la forma en que los dos switches construyen las tablas de direcciones MAC.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: antes de iniciar la práctica de laboratorio, debe descargar el programa Wireshark e instalarlo en la PC-B. Wireshark se puede descargar de <http://www.wireshark.org>.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Fast Ethernet en los switches Cisco 2960 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre los switches S1 y S2. Si utiliza otro modelo de switch Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: Armar y configurar la red

Paso 1: Tender el cableado de red de acuerdo con la topología

Paso 2: Configurar los hosts de la PC

Paso 3: Inicializar y recargar los routers y switches según sea necesario

Paso 4: Configurar los parámetros básicos para cada switch

- Configure el nombre del dispositivo como se muestra en la topología.
- Configure la dirección IP y el gateway predeterminado como se indica en la tabla de direccionamiento.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña de EXEC privilegiado.

Paso 5: Configurar los parámetros básicos del router

- Desactive la búsqueda del DNS.
- Configure la dirección IP del router como se indica en la tabla de direccionamiento.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña de EXEC privilegiado.

Parte 2: Examinar la tabla de direcciones MAC del switch

A medida que los dispositivos de red inician la comunicación en la red, un switch aprende las direcciones MAC y crea la tabla de direcciones MAC.

Paso 1: Registrar las direcciones MAC del dispositivo de red

- Abra el símbolo del sistema en la PC-A y la PC-B y escriba **ipconfig /all**. ¿Cuáles son las direcciones físicas del adaptador Ethernet?

Dirección MAC de la PC-A: _____

Dirección MAC de la PC-B: _____

Las respuestas varían.

- Acceda al router R1 mediante el puerto de consola e introduzca el comando **show interface G0/1**. ¿Cuál es la dirección de hardware?

Dirección MAC Gigabit Ethernet 0/1 del R1: _____

Las respuestas varían, pero en el resultado del ejemplo que se muestra a continuación, la dirección MAC G0/1 es 30f7.0da3.17c1.

```
R1# show interface G0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.17c1 (bia 30f7.0da3.17c1)
  Internet address is 192.168.1.1/24
<output omitted>
R1#
```

- c. Acceda a los switches S1 y S2 mediante el puerto de consola e introduzca el comando **show interface F0/1** en cada switch. En la segunda línea del resultado del comando, ¿cuáles son las direcciones de hardware (o la dirección física [bia])?

Dirección MAC Fast Ethernet 0/1 del S1: _____

Dirección MAC Fast Ethernet 0/1 del S2: _____

Las respuestas varían, pero en el resultado del ejemplo que se muestra a continuación, la dirección MAC F0/1 del S1 es 0cd9.96d2.3d81 y la dirección MAC F0/1 del S2 es 0cd9.96d2.4581.

```
S1# show interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96d2.3d81 (bia 0cd9.96d2.3d81)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
S1#
```

```
S2# show interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96d2.4581 (bia 0cd9.96d2.4581)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
S2#
```

Paso 2: Visualizar la tabla de direcciones MAC del switch

Acceda al switch S2 mediante el puerto de consola y vea la tabla de direcciones MAC, antes y después de ejecutar pruebas de comunicación de red con ping.

- Establezca una conexión de consola al S2 e ingrese al modo EXEC privilegiado.
- En el modo EXEC privilegiado, escriba el comando **show mac address-table** y presione Entrar.

```
S2# show mac address-table
```

Aunque no se haya iniciado la comunicación de red a través de la red (es decir, sin uso de ping), es posible que el switch haya aprendido las direcciones MAC de su conexión a la PC y al otro switch.

¿Hay direcciones MAC registradas en la tabla de direcciones MAC?

El switch puede tener una o más direcciones MAC en la tabla; según si los estudiantes introdujeron un comando ping, o no, cuando configuraron la red. Lo más probable es que el switch haya aprendido las direcciones MAC a través del puerto de switch F0/1 del S1. El switch registra varias direcciones MAC de hosts que aprendió a través de la conexión al otro switch en F0/1.

```
S2# show mac address-table
          Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
A11     0100.0ccc.cccc   STATIC    CPU
A11     0100.0ccc.cccd   STATIC    CPU
A11     0180.c200.0000   STATIC    CPU
A11     0180.c200.0001   STATIC    CPU
A11     0180.c200.0002   STATIC    CPU
```

```
A11 0180.c200.0003 STATIC CPU
A11 0180.c200.0004 STATIC CPU
A11 0180.c200.0005 STATIC CPU
A11 0180.c200.0006 STATIC CPU
A11 0180.c200.0007 STATIC CPU
A11 0180.c200.0008 STATIC CPU
A11 0180.c200.0009 STATIC CPU
A11 0180.c200.000a STATIC CPU
A11 0180.c200.000b STATIC CPU
A11 0180.c200.000c STATIC CPU
A11 0180.c200.000d STATIC CPU
A11 0180.c200.000e STATIC CPU
A11 0180.c200.000f STATIC CPU
A11 0180.c200.0010 STATIC CPU
A11 ffff.ffff.ffff STATIC CPU
  1 0cd9.96d2.3d81 DYNAMIC Fa0/1
  1 1cc1.de91.c35d DYNAMIC Fa0/1
```

Total Mac Addresses for this criterion: 22

S2#

¿Qué direcciones MAC se registran en la tabla? ¿A qué puertos de switch están asignadas y a qué dispositivos pertenecen? Omita las direcciones MAC que corresponden a la CPU.

Puede haber varias direcciones MAC registradas en la tabla de direcciones MAC, en particular las direcciones MAC aprendidas a través del puerto de switch F0/1 del S1. En el resultado del ejemplo anterior, la dirección MAC F0/1 del S1 y la dirección MAC de la PC-A corresponden al F0/1 del S2.

Si anteriormente, en el paso 1, no registró direcciones MAC de los dispositivos de red, ¿cómo podría saber a qué dispositivos pertenecen las direcciones MAC utilizando solo el resultado del comando **show mac address-table**? ¿Esto funciona en todas las situaciones?

El resultado del comando **show mac address-table** muestra el puerto en el que se aprendió la dirección MAC. En la mayoría de los casos, esto identifica el dispositivo de red al que pertenece la dirección MAC, excepto en el caso de varias direcciones MAC asociadas al mismo puerto. Esto sucede cuando los switches están conectados a otros switches y registran todas las direcciones MAC para los dispositivos conectados al otro switch.

Paso 3: Borre la tabla de direcciones MAC del S2 y vuelva a visualizar la tabla de direcciones MAC.

- En el modo EXEC privilegiado, escriba el comando **clear mac address-table dynamic** y presione Entrar.

S2# **clear mac address-table dynamic**

- Vuelva a escribir rápidamente el comando **show mac address-table**. ¿La tabla de direcciones MAC contiene alguna dirección para VLAN 1? ¿Hay otras direcciones MAC en la lista?

No. Es muy probable que el estudiante descubra que la dirección MAC para el puerto de switch F0/1 del otro switch se reinsertó rápidamente en la tabla de direcciones MAC.

S2# **show mac address-table**

Mac Address Table

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	0cd9.96d2.3d81	DYNAMIC	Fa0/1

Total Mac Addresses for this criterion: 21

S2#

Espere 10 segundos, escriba el comando **show mac address-table** y presione Entrar. ¿Hay nuevas direcciones en la tabla de direcciones MAC? _____ Las respuestas varían. Es posible.

Paso 4: En la PC-B, haga ping a los dispositivos en la red y observe la tabla de direcciones MAC del switch.

- En la PC-B, abra el símbolo del sistema y escriba **arp -a**. Sin incluir direcciones multicast o de broadcast, ¿cuántos pares de direcciones IP a MAC del dispositivo aprendió el ARP?

Las respuestas varían. Es posible que la caché ARP no tenga ninguna entrada, o puede ser que tenga la asignación de direcciones IP del gateway a direcciones MAC.

C:\Users\PC-B> **arp -a**

Interface: 192.168.1.2 --- 0xb

Internet Address	Physical Address	Type
192.168.1.1	30-f7-0d-a3-17-c1	dynamic

C:\Users\PC-B>

- b. En el símbolo del sistema de la PC-B, haga ping al router/gateway R1, PC-A, S1 y S2. ¿Todos los dispositivos tuvieron respuestas exitosas? Si la respuesta es negativa, revise el cableado y las configuraciones IP.

Si la red estaba conectada y configurada correctamente, la respuesta debería ser afirmativa.

- c. En una conexión de consola al S2, introduzca el comando **show mac address-table**. ¿El switch agregó más direcciones MAC a la tabla de direcciones MAC? Si es así, ¿qué direcciones y dispositivos?

Es posible que solo se haya agregado una asignación de dirección MAC adicional a la tabla; lo más probable es que sea la dirección MAC de la PC-A.

```
S2# show mac address-table
```

```
Mac Address Table
```

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	0021.700c.050c	DYNAMIC	Fa0/18
1	0cd9.96d2.3d81	DYNAMIC	Fa0/1
1	0cd9.96d2.3dc0	DYNAMIC	Fa0/1
1	1cc1.de91.c35d	DYNAMIC	Fa0/1
1	30f7.0da3.17c1	DYNAMIC	Fa0/1

```
Total Mac Addresses for this criterion: 25
```

```
S2#
```

En la PC-B, abra el símbolo del sistema y vuelva a escribir **arp -a**. ¿La caché ARP de la PC-B tiene entradas adicionales para todos los dispositivos de red a los que se enviaron pings?

Las respuestas pueden variar, pero la caché ARP en la PC-B debería tener más entradas.

```
C:\Users\PC-B> arp -a
Interface: 192.168.1.2 --- 0xb

    Internet Address      Physical Address      Type
    192.168.1.1           30-f7-0d-a3-17-c1    dynamic
    192.168.1.3           1c-c1-de-91-c3-5d    dynamic
    192.168.1.11          0c-d9-96-d2-3d-c0    dynamic
    192.168.1.12          0c-d9-96-d2-45-c0    dynamic
C:\Users\PC-B>
```

Reflexión

En las redes Ethernet, los datos se entregan a los dispositivos por medio de las direcciones MAC. Para que esto suceda, los switches y las PC crean cachés ARP y tablas de direcciones MAC en forma dinámica. Con solo algunas PC en la red, este proceso parece bastante fácil. ¿Cuáles podrían ser algunos de los desafíos en las redes más grandes?

Los broadcasts ARP podrían causar tormentas de broadcast. Dado que las tablas MAC de ARP y de los switches no pueden autenticar ni validar las direcciones IP para las direcciones MAC, sería fácil suplantar un dispositivo en la red.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos

Router R1

```
R1#show running-config
Building configuration...

Current configuration : 1128 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
no ipv6 cef
!
!
!
!
!
ip cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!  
interface GigabitEthernet0/1  
 ip address 192.168.1.1 255.255.255.0  
 duplex auto  
 speed auto  
!  
interface Serial0/0/0  
 no ip address  
 shutdown  
 clock rate 2000000  
!  
interface Serial0/0/1  
 no ip address  
 shutdown  
 clock rate 2000000  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
 no activation-character  
 no exec  
 transport preferred none  
 transport input all  
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
 stopbits 1  
line vty 0 4  
 login  
 transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

Switch S1

```
S1#show running-config  
Building configuration...
```

```
Current configuration : 1355 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
!
!
no aaa new-model
system mtu routing 1500
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
```

```
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
 line con 0
 line vty 0 4
  password cisco
  login
```

```
line vty 5 15
login
!
end
```

Switch S2

```
S2#show running-config
Building configuration...

Current configuration : 1355 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
!
!
no aaa new-model
system mtu routing 1500
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

```
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.1.12 255.255.255.0  
!  
ip default-gateway 192.168.1.1
```

```
ip http server
ip http secure-server
!
line con 0
line vty 0 4
password cisco
login
line vty 5 15
login
!
end
```

MAC y Ethernet... (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar conceptos básicos de conmutación.

Los estudiantes indicarán su conocimiento de la tecnología Ethernet comparando correctamente los estándares antiguos con los vigentes. También especularán sobre posibles estándares de tecnología Ethernet futuros. Asimismo, explicarán por qué las direcciones MAC y los formatos de entramado permanecieron básicamente iguales, a fin de ayudar en la transmisión de datos, durante la evolución de Ethernet.

Información básica/Situación

Nota: conviene realizar esta actividad en grupos de dos a tres estudiantes.

Mire el video The History of Ethernet en el enlace siguiente:

<http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet>

Los temas que se tratan en el video incluyen no solo hasta dónde llegó el desarrollo de Ethernet, sino hacia dónde se dirige la tecnología Ethernet.

Después de ver el video y de comparar su contenido con el capítulo 10, acceda a la Web y busque información sobre Ethernet:

- ¿Cómo se utilizaba Ethernet cuando se desarrolló por primera vez?
- ¿En qué aspectos Ethernet permaneció sin alteraciones durante alrededor de los últimos 25 años?
¿Qué cambios se están realizando para que sea más útil o se adapte mejor a los métodos actuales de transmisión de datos?

Reúna tres imágenes de dispositivos y medios físicos Ethernet antiguos, actuales y futuros posibles. Centre su búsqueda en los switches, si es posible. Comparta estas imágenes con la clase y analicen lo siguiente:

- ¿En qué aspectos cambiaron los medios físicos de Ethernet y los dispositivos intermediarios?
- ¿En qué aspectos permanecieron sin alteraciones los medios físicos de Ethernet y los dispositivos intermediarios?
- ¿Cómo piensa que Ethernet cambiará en el futuro? ¿Cuáles son los factores que podrían influir en estos cambios?

Notas para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la forma en que Ethernet se desarrolló conforme a los estándares vigentes, incluido su uso en redes LAN y WAN para la transmisión de tramas. La facilitación del debate debe incluir conversaciones entre los estudiantes sobre el trabajo de cada uno.

Recursos necesarios

- Acceso a Internet para ver el video History of Ethernet que se encuentra en el enlace:
<http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet>
- Copias impresas o electrónicas para registrar las respuestas a las preguntas y compartirlas en clase

Reflexión

1. ¿Cómo se utilizaba Ethernet cuando se desarrolló por primera vez?

Los estudiantes pueden mencionar que, en principio, Ethernet se desarrolló para usarse con impresoras (información del video).

2. ¿En qué aspectos Ethernet permaneció sin alteraciones durante alrededor de los últimos 25 años?
¿Qué cambios se están realizando para que sea más útil o se adapte mejor a los métodos actuales de transmisión de datos?

Ethernet aún emplea la transmisión inalámbrica y por cable de cobre, mientras que la velocidad y la distancia de las transmisiones evolucionaron para responder a los métodos de transmisión de datos actuales y futuros.

3. ¿En qué aspectos cambiaron los medios físicos de Ethernet y los dispositivos intermediarios?

La velocidad y la distancia de las comunicaciones de datos aumentaron exponencialmente: se diseñaron dispositivos intermediarios para utilizar diferentes tipos de terminales de cableado para admitir este aumento de velocidad y distancia.

4. ¿En qué aspectos permanecieron sin alteraciones los medios físicos de Ethernet y los dispositivos intermediarios?

Los switches aún se encargan de la mayoría de las transmisiones de Ethernet, ya sea de la capa 2 o la capa 3, pero el entramado es básicamente el mismo, con modificaciones menores a las secciones introductorias de las tramas, que indican qué tipo de trama se transmite, etc.

5. ¿Cómo piensa que Ethernet cambiará en el futuro? ¿Cuáles son los factores que podrían influir en estos cambios?

Las conexiones de los dispositivos y los desarrollos en la velocidad y la distancia cambiarán la forma en que las redes accederán a otras redes, pero la tecnología subyacente de Ethernet y el entramado de las transmisiones de Ethernet probablemente permanecerán iguales. Un ejemplo es la tecnología inalámbrica. Es antigua y actual o futurista.

Realidad

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Ethernet es una idea basada en tecnología con cableado y velocidad; todos los métodos de señalización implican decidir qué método de Ethernet se debe usar en una red.
- Los switches emplean la tecnología Ethernet en ambos lados de una red: LAN y WAN.
- Si bien Ethernet es antigua en cuanto a su origen, se mantiene completamente vigente en lo que respecta a la aplicación en las redes actuales, en especial en formatos de entramado con leves modificaciones.

La ruta menos transitada... ¿realmente lo es?

(Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que los dispositivos de red utilizan tablas de enrutamiento para dirigir los paquetes a una red de destino.

- Los estudiantes visualizarán la forma en que un paradigma de enrutamiento de salto por salto con la selección correcta de rutas en cada salto deriva en una entrega de paquetes correcta. Reconocerán que cada router de la ruta debe tener el conocimiento adecuado acerca de la red de destino, y la ruta hacia esa red, a fin de entregar los paquetes a través de la ruta más corta.

Información básica/Situación

Decidió que el próximo fin de semana irá a visitar a un compañero de curso que está en su casa debido a una enfermedad. Tiene la dirección de su compañero, pero nunca fue a la ciudad donde vive.

En lugar de buscar la dirección en el mapa, decide simplificar las cosas y pedir indicaciones a los residentes del lugar después de bajar del tren.

Los residentes a los que pide ayuda son muy amables. Sin embargo, todos tienen una costumbre interesante. En lugar de explicar por completo el camino que debe tomar para llegar a destino, todos le dicen: "vaya por esta calle y, en cuanto llegue al cruce más cercano, vuelva a preguntar a alguien allí".

Confundido por esta situación claramente curiosa, sigue estas instrucciones y finalmente llega a la casa de su compañero pasando cruce por cruce y calle por calle.

Responda las siguientes preguntas:

1. ¿Habría sido muy diferente si, en lugar de que se le indicara que fuera hasta el cruce más cercano, se le hubiera indicado el camino completo o una parte del camino más extensa?
2. ¿Habría sido más útil preguntar por la dirección específica o solo por la calle? ¿Qué ocurriría si la persona a la que solicita indicaciones no supiera dónde queda la calle de destino o le indicara un recorrido incorrecto?
3. Suponiendo que en su camino de regreso a casa decide preguntar nuevamente a los residentes cómo llegar. ¿Es seguro que le indicarían seguir el mismo camino que hizo para llegar a la casa de su amigo? Justifique su respuesta.
4. ¿Es necesario explicar de dónde parte cuando pide indicaciones para llegar a un destino deseado?

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la forma en que una red utiliza las rutas para enviar y recibir comunicaciones de datos. Como resultado de esta actividad, se facilitará el debate.

Reflexión

1. ¿Habría sido muy diferente si, en lugar de que se le indicara que fuera hasta el cruce más cercano, se le hubiera indicado el camino completo o una parte del camino más extensa?
-

Realmente, no habría sido diferente. El hecho clave que se debe recordar es que, para llegar a cualquier parte de la ruta detrás del cruce más cercano, primero debemos llegar a ese cruce. Si se puede asumir que los residentes en cada cruce conocen bien su ciudad, no es muy útil preguntarles qué hay más allá del primer cruce, ya que igualmente debemos llegar allí y, en cada cruce, se nos orientará adecuadamente. Sin embargo, los estudiantes deben tener en cuenta que la congestión también puede afectar el hecho de usar una ruta mejor que otra.

2. ¿Habría sido más útil preguntar por la dirección específica o solo por la calle?

Preguntar el nombre de la calle, y omitir el número de la casa, es suficiente. Una vez que llegamos a la calle de destino, podemos buscar fácilmente la casa nosotros mismos. Las personas que están en los cruces pueden darnos indicaciones incluso sin decirles el número exacto de la casa. No es necesario que conozcan cada casa de cada calle; es suficiente con que sepan las calles.

3. ¿Qué ocurriría si la persona a la que solicita indicaciones no supiera dónde queda la calle de destino o le indicara un recorrido incorrecto?

En ese caso, estaríamos en riesgo de desorientarnos y seguir una ruta más larga de lo necesario hacia el destino, o incluso podríamos terminar girando en círculos o perdiéndonos.

4. Suponiendo que en su camino de regreso a casa decide preguntar nuevamente a los residentes cómo llegar. ¿Está garantizado que lo guiarán por la misma ruta que la que tomó para llegar a la casa de su amigo? Justifique su respuesta.

No existe tal garantía. Cada persona en un cruce toma una decisión individual e independiente sobre el mejor camino. Es muy probable que, si los residentes no conocen o no tienen mucha idea de las rutas de su ciudad, usted vuelva a la estación de tren por una ruta diferente.

5. ¿Es necesario explicar de dónde parte cuando pide indicaciones para llegar a un destino deseado?

Describir de dónde partió no es útil cuando se elige la ruta hacia un destino. El destino mismo es lo que importa cuando se elige la mejor ruta hacia él.

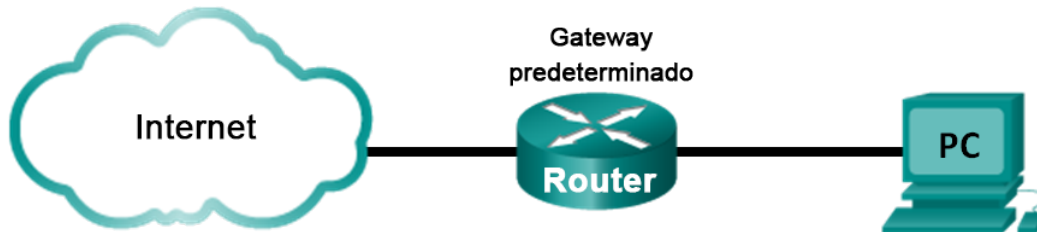
Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Cruces: corresponde a las paradas en el camino (routers).
- Caminos: corresponde a los enlaces de interfaz entre los routers.
- Calle: corresponde a una red.
- Irrelevancia del número de casa al preguntar por la ruta hacia la calle de destino: corresponde a los routers que tienen conocimiento de las redes; no de hosts individuales.
- Preguntar por la ruta al destino en cada cruce: corresponde a la selección de rutas realizada en cada router.
- La estación de tren, la casa del amigo: corresponden al origen y al destino.
- Importancia solo del destino al preguntar por una ruta: corresponde al enrutamiento basado en el destino.
- Diferentes rutas posibles hasta la casa del amigo y desde esta: corresponde al enrutamiento independiente hacia un destino y desde este.

Práctica de laboratorio: Visualización de tablas de enrutamiento de host (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Acceder a la tabla de enrutamiento de host

Parte 2: Examinar las entradas de la tabla de enrutamiento de host IPv4

Parte 3: Examinar las entradas de la tabla de enrutamiento de host IPv6

Información básica/Situación

Para acceder a un recurso en una red, el host determina la ruta hacia el host de destino mediante la tabla de enrutamiento. La tabla de enrutamiento de host es similar a la de un router, pero es específica del host local y mucho menos compleja. Para que un paquete llegue a un destino local, se requiere la tabla de enrutamiento del host local. Para llegar a un destino remoto, se requieren la tabla de enrutamiento del host local y la tabla de enrutamiento del router. Los comandos **netstat -r** y **route print** proporcionan detalles sobre la forma en que el host local enruta los paquetes al destino.

En esta práctica de laboratorio, mostrará y examinará la información en la tabla de enrutamiento de host de la PC utilizando los comandos **netstat -r** y **route print**. Asimismo, determinará la forma en que la PC enrutará paquetes según la dirección de destino.

Nota: esta práctica de laboratorio no se puede realizar utilizando Netlab. Para la realización de esta práctica de laboratorio, se da por sentado que tiene acceso a Internet.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con acceso a Internet y al símbolo del sistema)

Parte 1: Acceder a la tabla de enrutamiento de host

Paso 1: Registrar la información de la PC

En la PC, abra una ventana de símbolo del sistema y escriba el comando **ipconfig /all** para visualizar la siguiente información y registrarla:

Dirección IPv4	Las respuestas varían. En este ejemplo, 192.168.1.11.
Dirección MAC	Las respuestas varían. En este ejemplo, 90:4C:E5:BE:15:63.
Gateway predeterminado	Las respuestas varían. En este ejemplo, 192.168.1.1.

Paso 2: Mostrar las tablas de enrutamiento

En una ventana de símbolo del sistema, escriba el comando **netstat -r** (o **route print**) para visualizar la tabla de enrutamiento de host.

```
C:\Users\user1>netstat -r
=====
Interface List
13...90 4c e5 be 15 63 .....Atheros AR9285 802.11b/g/n WiFi Adapter
1.....Software Loopback Interface 1
25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.11     25
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.1.0                255.255.255.0    On-link          192.168.1.11     281
192.168.1.11              255.255.255.255  On-link          192.168.1.11     281
192.168.1.255              255.255.255.255  On-link          192.168.1.11     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.1.11     281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.1.11     281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
14      58 ::/0 On-link
1      306 ::1/128 On-link
14      58 2001::/32 On-link
14      306 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128 On-link
14      306 fe80::/64 On-link
14      306 fe80::1863:3bca:3f57:fef4/128 On-link
1      306 ff00::/8 On-link
14      306 ff00::/8 On-link
=====
Persistent Routes:
None
```

¿Cuáles son las tres secciones que se muestran en el resultado?

El resultado tiene tres secciones: Interface List (Lista de interfaces), IPv4 Route Table (Tabla de rutas IPv4) e IPv6 Route Table (Tabla de rutas IPv6).

Paso 3: Examinar la lista de interfaces

En la primera sección, Interface List, se muestran las direcciones de control de acceso al medio (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host.

```
=====
Interface List
13...90 4c e5 be 15 63 .....Atheros AR9285 802.11b/g/n WiFi Adapter
1.....Software Loopback Interface 1
25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====
```

La primera columna corresponde al número de interfaz. La segunda columna corresponde a la lista de direcciones MAC asociadas a las interfaces con capacidad de red en los hosts. Estas interfaces pueden incluir adaptadores Ethernet, Wi-Fi y Bluetooth. La tercera columna muestra el fabricante y una descripción de la interfaz.

En este ejemplo, la primera línea muestra la interfaz inalámbrica que está conectada a la red local.

Nota: si tiene una PC con una interfaz Ethernet y un adaptador inalámbrico habilitados, se incluirán las dos interfaces en la lista de interfaces.

¿Cuál es la dirección MAC de la interfaz conectada a la red local? ¿Cómo se compara la dirección MAC con la dirección MAC registrada en el paso 1?

Las respuestas varían. La dirección MAC en este ejemplo es 90:4C:E5:BE:15:63. La dirección MAC debe ser la misma que la registrada en el paso 1 mediante el comando `ipconfig /all`.

La segunda línea corresponde a la interfaz loopback. Cuando el protocolo de control de transmisión/protocolo de Internet (TCP/IP) se ejecuta en un host, a la interfaz loopback se le asigna automáticamente una dirección IP 127.0.0.1.

Las cuatro últimas líneas representan la tecnología de transición que permite la comunicación en un entorno mixto e incluye IPv4 e IPv6.

Parte 2: Examinar las entradas de la tabla de enrutamiento de host IPv4

En la parte 2, examinará la tabla de enrutamiento de host IPv4. Esta tabla se encuentra en la segunda sección como resultado del comando **netstat -r**. Enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, la red local y las rutas predeterminadas locales.

IPv4 Route Table					
=====					
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.11	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.1.0	255.255.255.0	255.255.255.0	On-link	192.168.1.11	281
192.168.1.11	255.255.255.255	255.255.255.255	On-link	192.168.1.11	281
192.168.1.255	255.255.255.255	255.255.255.255	On-link	192.168.1.11	281
224.0.0.0	240.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.1.11	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.1.11	281
=====					
Persistent Routes:					
None					

El resultado se divide en cinco columnas: Network Destination (Destino de red), Netmask (Máscara de red), Gateway, Interface (Interfaz) y Metric (Métrica).

- En la columna Network Destination, se indica la red con la que hay posibilidad de conexión. El destino de red se utiliza con la máscara de red para coincidir con la dirección IP de destino.
- En la columna Netmask, se indica la máscara de subred que el host utiliza para determinar las porciones de red y host de la dirección IP.
- En la columna Gateway, se indica la dirección que el host utiliza para enviar los paquetes a un destino de red remoto. Si un destino está conectado directamente, el gateway aparece como On-link (En enlace) en el resultado.
- En la columna Interface, se indica la dirección IP que está configurada en el adaptador de red local. Se utiliza para reenviar un paquete en la red.

- En la columna Metric, se indica el costo de usar una ruta. Se utiliza para calcular la mejor ruta a un destino. Una ruta preferida tiene un número de métrica menor que otras rutas de la lista.

El resultado muestra cinco tipos diferentes de rutas activas:

- La ruta predeterminada local 0.0.0.0 se utiliza cuando el paquete no coincide con otras instrucciones especificadas en la tabla de enrutamiento. El paquete se envía hacia el gateway desde la PC para un procesamiento adicional. En este ejemplo, el paquete se envía hacia 192.168.1.1 desde 192.168.1.11.
- Las direcciones de loopback, 127.0.0.0 – 127.255.255.255, están relacionadas con la conexión directa y prestan servicios al host local.
- Todas las direcciones para la subred, 192.168.1.0 – 192.168.1.255, están relacionadas con el host y la red local. Si el destino final del paquete está en la red local, el paquete sale de la interfaz 192.168.1.11.
 - La dirección de la ruta local 192.168.1.0 representa todos los dispositivos en la red 192.168.1.0/24.
 - La dirección del host local es 192.168.1.11.
 - La dirección de broadcast de la red 192.168.1.255 se utiliza para enviar mensajes a todos los hosts en la red local.
- Las direcciones multicast de clase D especiales 224.0.0.0 están reservadas para ser utilizadas a través de la interfaz loopback (127.0.0.1) o del host (192.168.1.11).
- La dirección de broadcast local 255.255.255.255 se puede utilizar a través de la interfaz loopback (127.0.0.1) o del host (192.168.1.11).

Según el contenido de la tabla de enrutamiento IPv4, si la PC deseara enviar un paquete a 192.168.1.15, ¿qué haría y adónde enviaría el paquete?

La PC consultaría la tabla de rutas IPv4 y haría coincidir la dirección IP de destino con la entrada 192.168.1.0 de Network Destination para mostrar que el host está en la misma red (On-link). Luego, la PC enviaría el paquete hacia el destino final mediante su interfaz local (192.168.1.11).

Si la PC deseara enviar un paquete a un host remoto ubicado en 172.16.20.23, ¿qué haría y adónde enviaría el paquete?

La PC consultaría la tabla de rutas IPv4 y encontraría que no hay una coincidencia exacta para la dirección IP de destino. Luego, elegiría la ruta predeterminada local (red 0.0.0.0, máscara de red 0.0.0.0) para revelar que debe reenviar el paquete a la dirección de gateway 192.168.1.1 (la dirección de un dispositivo de gateway, como una interfaz del router en la red local). Luego, la PC reenviaría el paquete hacia el gateway mediante su interfaz local (192.168.1.11). A continuación, el dispositivo de gateway determina la siguiente ruta que debe tomar el paquete para llegar a la dirección de destino final, 172.16.20.23.

Parte 3: Examinar las entradas de la tabla de enrutamiento de host IPv6

En la parte 3, examinará la tabla de enrutamiento IPv6. Esta tabla se encuentra en la tercera sección que se muestra en el resultado del comando **netstat -r**. Enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, la red local y las rutas predeterminadas locales.

```
IPv6 Route Table
=====
Active Routes:
  If Metric Network Destination      Gateway
  14     58  ::/0                On-link
  1     306  ::1/128             On-link
  14     58  2001::/32           On-link
  14     306  2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128
                                On-link
  14     306  fe80::/64           On-link
  14     306  fe80::1863:3bca:3f57:fef4/128
                                On-link
  1     306  ff00::/8            On-link
  14     306  ff00::/8            On-link
=====
Persistent Routes:
None
```

El resultado de la tabla de rutas IPv6 difiere en los encabezados de columna y en el formato, ya que las direcciones IPv6 son de 128 bits mientras que las direcciones IPv4 son solo de 32 bits. En la sección de la tabla de rutas IPv6, se muestran cuatro columnas:

- En la columna If (Si), se indican los números de interfaz de las interfaces de red con IPv6 de la sección Interface List del comando **netstat -r**.
- En la columna Metric, se indica el costo de cada ruta a un destino. El costo más bajo corresponde a la ruta preferida, y la métrica se utiliza para seleccionar entre varias rutas con el mismo prefijo.
- En la columna Network Destination, se indica el prefijo de dirección para la ruta.
- En la columna Gateway, se indica la dirección IPv6 del siguiente salto para llegar al destino. Como dirección del siguiente salto, se indica On-link, si está conectada directamente al host.

En este ejemplo, en la ilustración se muestra la sección de la tabla de rutas IPv6 que se genera con el comando **netstat -r** para mostrar los siguientes destinos de red:

- `::/0`: es el equivalente en IPv6 a la ruta predeterminada local. En la columna Gateway, se proporciona la dirección link-local del router predeterminado.
- `::1/128`: equivale a la dirección de loopback IPv4 y proporciona servicios al host local.
- `2001::/32`: es el prefijo de red unicast global.
- `2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128`: es la dirección IPv6 unicast global de la PC local.
- `fe80::/64`: es la dirección de la ruta de red de enlace local y representa a todas las PC en la red IPv6 de enlace local.
- `fe80::1863:3bca:3f57:fef4/128`: es la dirección IPv6 link-local de la PC local.
- `ff00::/8`: son direcciones multicast de clase D especiales y reservadas que equivalen a las direcciones IPv4 `224.x.x.x`.

La tabla de enrutamiento del host para IPv6 contiene información similar a la de la tabla de enrutamiento IPv4. ¿Cuál es la ruta predeterminada local para IPv4 y para IPv6?

Para IPv4, la ruta predeterminada local es `0.0.0.0 0.0.0.0` (quad zero) y, para IPv6, `::/0`.

¿Cuál es la dirección de loopback y la máscara de subred para IPv4? ¿Cuál es la dirección IP de loopback para IPv6?

Para IPv4, 127.0.0.1 0.0.0.0 0.0.0.0, y para IPv6, ::1/128.

¿Cuántas direcciones IPv6 se asignaron a esta PC?

Hay dos direcciones IP. La dirección link-local y la dirección unicast global.

¿Cuántas direcciones de broadcast tiene la tabla de enrutamiento IPv6?

Ninguna. IPv6 no utiliza direcciones de broadcast.

Reflexión

1. ¿Cómo es el número de bits para la red que se indica para IPv4? ¿Y cómo es para IPv6?

IPv4 utiliza una máscara de subred decimal punteada de 32 bits con la forma a.b.c.d. IPv6 utiliza un número con barra.

2. ¿Por qué hay información tanto de IPv4 como de IPv6 en las tablas de enrutamiento de host?

En la actualidad, las PC ejecutan ambos protocolos, y los ISP suelen asignar direcciones IPv4 e IPv6 para admitir el acceso a los servidores en Internet que ejecutan cualquiera de los dos protocolos.

Práctica de laboratorio: Exploración de las características físicas del router (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Examinar las características externas del router

- Identificar las diversas partes de un router Cisco, entre ellas:
 - Puertos de administración
 - Interfaces LAN
 - Interfaces WAN
 - Ranuras de expansión de módulo
 - Ranuras de expansión de memoria CompactFlash
 - Puertos USB
- Examinar las luces de actividad y de estado del router.

Parte 2: Examinar las características internas del router utilizando los comandos show

- Establecer una conexión de consola al router utilizando Tera Term.
- Identificar las características internas del router utilizando el comando **show version**.
- Identificar las características de la interfaz del router utilizando el comando **show interface**.

Información básica/Situación

En esta práctica de laboratorio, examinará el exterior del router para familiarizarse con sus características y componentes, como el interruptor de alimentación, los puertos de administración, las interfaces LAN y WAN, las luces indicadoras, las ranuras de expansión de red, las ranuras de expansión de memoria y los puertos USB.

También identificará los componentes internos y las características del IOS al acceder al router mediante el puerto de consola y emitir diversos comandos, como **show version** y **show interfaces**, desde la CLI.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Se pueden utilizar otros routers y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: asegúrese de que los routers se hayan eliminado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: según la disponibilidad del equipo, el instructor puede preferir utilizar la práctica de laboratorio como una disertación o demostración guiada para señalar las características del router y analizarlas con la clase.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola

Parte 1: Examinar las características externas del router

Utilice las imágenes que se muestran a continuación, así como su propia inspección directa del backplane de un router Cisco, para responder las siguientes preguntas. Siéntase libre para dibujar flechas y rodear con círculos las áreas de la imagen que identifican correctamente las partes.

Nota: el router que se muestra en las imágenes siguientes es un router Cisco 1941, que puede ser diferente en marca y modelo de los routers de su academia particular. Para obtener información sobre el dispositivo y especificaciones de los routers Cisco serie 1941, acceda al sitio Web [www.Cisco.com](http://www.cisco.com). En este enlace, encontrará información adicional e incluso las respuestas a muchas de las preguntas que se formulan más adelante:

http://www.cisco.com/en/US/prod/collateral/routers/ps10538/data_sheet_c78_556319.html

Paso 1: Identificar las diversas partes de un router Cisco

La imagen que se muestra en este paso corresponde al backplane de un ISR Cisco 1941. Utilícela para responder las preguntas de este paso. Asimismo, si examina un router de un modelo diferente, aquí se brinda un espacio para que dibuje el backplane e identifique los componentes y las interfaces como se especifica en las preguntas que siguen.





- a. Rodee con un círculo y rotule el interruptor de alimentación del router. ¿El interruptor de alimentación en el router se encuentra en la misma área que en el router que se muestra en la imagen?

Las respuestas pueden variar según los routers del laboratorio de la academia. Los estudiantes deben dibujar una línea alrededor del interruptor de encendido/apagado en la imagen.

- b. Rodee con un círculo y rotule los puertos de administración. ¿Cuáles son los puertos de administración incorporados? ¿Los puertos de administración son los mismos en su router? De lo contrario, ¿en qué se diferencian?

Las respuestas pueden variar según los routers del laboratorio de la academia. Los estudiantes deben rodear con un círculo el puerto de consola, el puerto auxiliar y el puerto de consola mini-USB en la imagen.

- c. Rodee con un círculo y rotule las interfaces LAN del router. ¿Cuántas interfaces LAN tiene el router en la imagen y cuál es el tipo de tecnología de la interfaz? ¿Las interfaces LAN son las mismas en su router? De lo contrario, ¿en qué se diferencian?

Las respuestas pueden variar según los routers del laboratorio de la academia. Los estudiantes deben rodear con un círculo las interfaces Gigabit Ethernet 0/0 y 0/1 en la imagen.

- d. Rodee con un círculo y rotule las interfaces WAN del router. ¿Cuántas interfaces WAN tiene el router en la imagen y cuál es el tipo de tecnología de la interfaz? ¿Las interfaces WAN son las mismas en su router? De lo contrario, ¿en qué se diferencian?

Las respuestas pueden variar según los routers del laboratorio de la academia. Los estudiantes deben rodear con un círculo las interfaces Serial 0 y Serial 1 en la imagen.

- e. El ISR Cisco 1941 es una plataforma modular e incluye ranuras de expansión de módulo que permiten satisfacer los diversos requisitos de conectividad de red. Rodee con un círculo y rotule las ranuras de módulo. ¿Cuántas ranuras de módulo hay? ¿Cuántas se utilizan? ¿Qué tipo de ranuras de expansión de módulo son? ¿Las ranuras de módulo son las mismas en su router? De lo contrario, ¿en qué se diferencian?

Las respuestas pueden variar según los routers del laboratorio de la academia. En la imagen, se muestra un ISR Cisco 1941 con dos ranuras de expansión de módulo para las tarjetas de interfaz WAN de alta velocidad mejoradas (EHWIC): EHWIC 0 y EHWIC 1. EHWIC 0 se ocupa con una tarjeta de interfaz WAN serial inteligente. EHWIC 1 admite una tarjeta de expansión de doble ancho. La ranura para

EHWIC sustituye la ranura para la tarjeta de interfaz WAN de alta velocidad (HWIC) y admite de manera nativa HWIC, tarjetas de interfaz WAN (WIC), tarjetas de interfaz de voz (VIC) y tarjetas de interfaz WAN y de voz (VWIC).

- f. El router Cisco 1941 incluye ranuras para memoria CompactFlash para el almacenamiento de alta velocidad. Rodee con un círculo y rotule las ranuras para memoria CompactFlash. ¿Cuántas ranuras de memoria hay? ¿Cuántas se utilizan? ¿Cuánta memoria pueden alojar? ¿Las ranuras de memoria son las mismas en su router? De lo contrario, ¿en qué se diferencian?

Las respuestas pueden variar según los routers del laboratorio de la academia. En la imagen, se muestra un ISR Cisco 1941 con dos ranuras para memoria CompactFlash: CF 0 y CF 1. CF 0 se ocupa con una tarjeta de memoria CompactFlash de 256 MB, que se utiliza para almacenar el archivo de imagen de sistema de Cisco IOS.

- g. El router Cisco 1941 incluye puertos USB 2.0. Los puertos USB incorporados admiten dispositivos eToken y memoria flash USB. La característica de dispositivo USB eToken proporciona la autenticación del dispositivo y la configuración segura de los routers Cisco. La característica de memoria flash USB proporciona la capacidad de almacenamiento secundario optativa y un dispositivo de arranque adicional. Rodee con un círculo y rotule los puertos USB. ¿Cuántos puertos USB hay? ¿Hay puertos USB en su router?

Las respuestas pueden variar según los routers del laboratorio de la academia. En la imagen, se muestra un ISR Cisco 1941 con dos puertos USB 2.0.

- h. El router Cisco 1941 también incluye un puerto de consola USB mini-B. Rodee con un círculo y rotule el puerto de consola USB mini-B.

Las respuestas pueden variar según los routers del laboratorio de la academia. En la imagen, se muestra un ISR Cisco 1941 con un puerto de consola mini-USB junto al puerto de consola habitual.

Paso 2: Examinar las luces de actividad y de estado del router.

En las imágenes siguientes, se destacan las luces de actividad y estado del panel frontal y el backplane de un ISR Cisco 1941 encendido y conectado.

Nota: algunas de las luces indicadoras están ocultas en la imagen del backplane del router Cisco 1941 que se muestra a continuación.





- a. En la imagen de más arriba, revise las luces indicadoras en el panel frontal del router. Las luces están rotuladas SYS, ACT y POE. ¿A qué se refieren estos rótulos? ¿Qué indican las luces en la imagen sobre el estado del router? Estos rótulos se podrían leer si no estuvieran encendidos.

Las luces SYS, ACT y POE se refieren al estado del sistema, la actividad de la red y la alimentación por Ethernet, respectivamente. Las luces en la imagen muestran que el sistema del router está encendido correctamente, que hay actividad en la red y que la alimentación por Ethernet no está activada.

- b. En la imagen del backplane anterior, examine las luces indicadoras en el router. Hay tres luces de actividad visibles, una por cada una de las interfaces conectadas y los puertos de administración. Examine las luces de interfaz en su router. ¿Cómo están rotuladas las luces y cuál es su significado?

Las luces en la imagen muestran que las interfaces Serial y Gigabit Ethernet están activas y que el puerto de administración de la consola está habilitado y activo. Cada una de las interfaces Gigabit Ethernet tiene dos luces: una con el rótulo S, de Send (Enviar), y la otra con el rótulo L, de Link (Enlace). El puerto de consola y el puerto de consola mini-USB tienen el rótulo EN, de Enabled (Habilitado). Las interfaces seriales tienen una luz con el rótulo Conn, de Connected (Conectado).

- c. Además de los puertos de administración y de las interfaces de red, ¿qué otras luces indicadoras se encuentran en el backplane del router y cuál sería su propósito?

En el backplane del router también se muestran las luces CF 0 y CF 1 para las ranuras de memoria CompactFlash, así como una luz con el rótulo ISM/WLAN, que indicaría la presencia de un módulo de servicios internos de Cisco (ISM) o una tarjeta LAN inalámbrica (WLAN).

Parte 2: Examinar las características internas del router utilizando los comandos show

Paso 1: Establecer una conexión de consola al router y utilizar el comando show version

- a. A través de Tera Term, acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando **enable**.

```
Router> enable
Router#
```

- b. Muestre la información sobre el router utilizando el comando **show version**. Utilice la barra espaciadora del teclado para avanzar por el resultado.

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
Router uptime is 1 day, 14 hours, 46 minutes
System returned to ROM by power-on
System restarted at 07:26:55 UTC Mon Dec 3 2012
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
Last reload type: Normal Reload
Last reload reason: power-on
```

<resultado omitido>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco CISC01941/K9 (revision 1.0) with 487424K/36864K bytes of memory.
Processor board ID FGL16082318
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
<resultado omitido>
```

```
Technology Package License Information for Module:'c1900'
```

```
-----
Technology      Technology-package      Technology-package
                Current      Type                Next reboot
```

```
-----  
ipbase      ipbasek9      Permanent      ipbasek9  
security    securityk9    Permanent      securityk9  
data        None        None           None
```

Configuration register is 0x2102

- c. En función del resultado del comando **show version**, responda las siguientes preguntas sobre el router. Si está examinando un router de otro modelo, incluya la información aquí.

1) ¿Cuál es la versión de Cisco IOS y cuál es el nombre de archivo de imagen de sistema?

IOS versión 15.2(4)M3, c1900-universalk9-mz.SPA.152-4.M3.bin

2) ¿Cuál es la versión del programa bootstrap en ROM BIOS?

System Bootstrap, versión 15.0(1r)M15.

3) ¿Cuánto tiempo estuvo en funcionamiento el router sin ser reiniciado (lo que también se conoce como su tiempo de actividad)?

1 día, 14 horas, 46 minutos.

4) ¿Cuánta memoria de acceso aleatorio dinámica (DRAM) tiene el router?

487 424 K/36 864 K = 512 MB en total.

5) ¿Cuál es el número de ID de la placa del procesador del router?

El número de ID de la placa del procesador es FGL16082318.

6) ¿Qué interfaces de red tiene el router?

2 interfaces Gigabit Ethernet y 2 interfaces seriales.

7) ¿Cuánta memoria CompactFlash hay para el almacenamiento del IOS?

250 880 K de memoria CompactFlash.

8) ¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) hay para el almacenamiento de archivos de configuración?

255 K de NVRAM.

9) ¿Cuál es la configuración del registro de configuración?

0x2102

Paso 2: Utilice el comando show interface para examinar las interfaces de red.

- a. Utilice el comando **show interface gigabitEthernet 0/0** para ver el estado de la interfaz Gigabit Ethernet 0/0.

Nota: después de escribir parte del comando, por ejemplo, **show interface g**, puede utilizar la tecla **Tabulación** del teclado para completar el parámetro del comando gigabitEthernet.

```
Router# show interface gigabitEthernet 0/0
GigabitEthernet0/0 is administratively down, line protocol is down
  Hardware is CN Gigabit Ethernet, address is 442b.031a.b9a0 (bia 442b.031a.b9a0)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    3 packets input, 276 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

- b. Dado el resultado del comando **show interface gigabitEthernet 0/0** que se muestra arriba, o utilizando el resultado de su router, responda las siguientes preguntas:

¿Cuál es el tipo de hardware y la dirección MAC de la interfaz Gigabit Ethernet?

El tipo de hardware es CN Gigabit Ethernet y la dirección física (bia) o la dirección MAC es 442b.031a.b9a0.

¿Cuál es el tipo de medios de la interfaz? ¿La interfaz está activa o inactiva?

De acuerdo con el resultado, el tipo de medios de la interfaz es RJ45, la interfaz Gigabit Ethernet se encuentra administrativamente inactiva y el protocolo de línea se encuentra inactivo.

- c. Utilice el comando **show interface serial 0/0/0** para ver el estado de la interfaz Serial 0/0/0.

```
Router# show interface serial 0/0/0
Serial0/0/0 is administratively down, line protocol is down
```

```
Hardware is WIC MBRD Serial
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 07:41:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    1 packets input, 24 bytes, 0 no buffer
    Received 1 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
    DCD=down   DSR=down   DTR=down   RTS=down   CTS=down
```

- d. Dado el resultado del comando que se muestra arriba, responda las siguientes preguntas:

¿Cuál es el tipo de encapsulación de la trama?

De acuerdo con el resultado de arriba, el tipo de encapsulación de la trama es HDLC.

¿Cuál es el tipo de hardware? ¿La interfaz está activa o inactiva?

El tipo de hardware es WIC MBRD, y la interfaz se encuentra administrativamente inactiva, al igual que el protocolo de línea.

Reflexión

1. ¿Por qué podría ser necesario utilizar una ranura de expansión EHWIC?

Las respuestas varían. Quizá necesite tener una conexión WAN a su ISP a través de una tecnología de interfaz WAN que no venga con el router de manera predeterminada.

2. ¿Por qué podría ser necesario actualizar la memoria flash?

Las respuestas varían. Quizá desee almacenar un archivo de imagen del IOS adicional o actualizar a una imagen del IOS más grande.

3. ¿Cuál es el propósito del puerto mini-USB?

El propósito del puerto mini-USB es proporcionar al usuario la capacidad de acceder al router mediante el puerto de consola, si no cuenta con un puerto serie COM en su computadora portátil o PC.

4. ¿Cuál es el propósito de la luz indicadora ISM/WLAN en el backplane del router? ¿A qué hace referencia?

El router Cisco 1941 puede admitir un módulo de servicios internos Cisco que puede mejorar la inteligencia y las capacidades del router para realizar actividades como el análisis de prevención de intrusiones. El router Cisco 1941 también puede contar con una tarjeta LAN inalámbrica para admitir redes de área local inalámbricas.

Práctica de laboratorio: Armado de una red de switch y router (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	No aplicable
	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	No aplicable	No aplicable	No aplicable
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objetivos

Parte 1: Establecer la topología e inicializar los dispositivos

- Configurar los equipos según la topología de la red.
- Inicializar y reiniciar el router y el switch.

Parte 2: Configurar dispositivos y verificar la conectividad

- Asignar información de IP estática a las interfaces de la PC.
- Configurar el router.
- Verificar la conectividad de la red.

Parte 3: Mostrar información del dispositivo

- Recuperar información del hardware y del software de los dispositivos de red.
- Interpretar el resultado de la tabla de enrutamiento.
- Mostrar información de la interfaz en el router.
- Mostrar una lista de resumen de las interfaces del router y del switch.

Información básica/Situación

Esta es una práctica de laboratorio exhaustiva para repasar los comandos del IOS que se abarcaron anteriormente. En esta práctica de laboratorio, conectará el equipo tal como se muestra en el diagrama de topología. Luego, configurará los dispositivos según la tabla de direccionamiento. Cuando se haya guardado la configuración, la verificará probando la conectividad de red.

Una vez que los dispositivos estén configurados y que se haya verificado la conectividad de red, utilizará los comandos del IOS para recuperar la información de los dispositivos y responder preguntas sobre los equipos de red.

En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos reales necesarios para configurar el router. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento intentando configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte Router Interface Summary Table al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice B para conocer el procedimiento para inicializar y volver a cargar un router y un switch.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Gigabit Ethernet en los routers Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: Establecer la topología e inicializar los dispositivos

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

- a. Conecte los dispositivos que se muestran en el diagrama de topología y tienda el cableado, según sea necesario.
- b. Encienda todos los dispositivos de la topología.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos. Para obtener información sobre cómo inicializar y volver a cargar estos dispositivos, consulte el apéndice B.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará la topología de la red y los parámetros básicos, como direcciones IP de la interfaz, el acceso a dispositivos y contraseñas. Consulte *Topology* y *Addressing Table* al principio de esta práctica de laboratorio para obtener información sobre nombres de dispositivos y direcciones.

Nota: en el apéndice A, se proporcionan detalles de configuración para los pasos de la parte 2. Antes de consultar el apéndice, intente completar la parte 2.

Paso 1: Asignar información de IP estática a las interfaces de la PC.

- Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.
- Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.
- Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.
¿Por qué los pings no fueron correctos?

Las interfaces del router (gateways predeterminados) aún no se configuraron, por lo que el tráfico de la capa 3 no se transmite entre las subredes.

Paso 2: Configurar el router.

- Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- Entre al modo de configuración.
- Asigne un nombre de dispositivo al router.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- Configure y active las dos interfaces en el router.
- Configure una descripción de interfaz para cada interfaz e indique qué dispositivo está conectado.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.
- Configure el reloj en el router.

Nota: utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar este comando.

- Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.
¿Tuvieron éxito los pings? ¿Por qué?
-
-
-

Sí. El router dirige el tráfico de ping a través de dos subredes. La configuración predeterminada para el switch 2960 activa automáticamente las interfaces que están conectadas a los dispositivos.

Parte 3: Mostrar información del dispositivo

En la parte 3, utilizará los comandos **show** para recuperar información del router y el switch.

Paso 1: Recuperar información del hardware y del software de los dispositivos de red.

- a. Utilice el comando **show version** para responder las siguientes preguntas sobre el router.

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R1 uptime is 10 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
Last reload type: Normal Reload
Last reload reason: power-on

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

License Info:

License UDI:

```
-----  
Device#          PID          SN  
-----  
*0              CISCO1941/K9      FTX1636848Z
```

Technology Package License Information for Module:'c1900'

```
-----  
Technology      Technology-package      Technology-package  
                Current      Type      Next reboot  
-----  
ipbase          ipbasek9      Permanent  ipbasek9  
security        None          None       None  
data            None          None       None
```

Configuration register is 0x2142 (will be 0x2102 at next reload)

¿Cuál es el nombre de la imagen del IOS que el router está ejecutando?

La versión de imagen puede variar, pero las respuestas deberían ser algo así como c1900-universalk9-mz.SPA.152-4.M3.bin.

¿Cuánta memoria DRAM tiene el router?

Las respuestas pueden variar, pero la configuración de la memoria DRAM predeterminada en un router 1941 es de 512 MB o 524 288 KB. El total se puede calcular sumando los dos números de DRAM del resultado del comando show version: Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.

¿Cuánta memoria NVRAM tiene el router?

Las respuestas pueden variar, pero el resultado del comando show version en el router 1941 es: 255K bytes of non-volatile configuration memory.

¿Cuánta memoria flash tiene el router?

Las respuestas pueden variar, pero el resultado del comando show version en el router 1941 es 250880K bytes of ATA System CompactFlash 0 (Read/Write).

- b. Utilice el comando **show version** para responder las siguientes preguntas sobre el switch.

```
Switch# show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE  
SOFTWARE (fcl)
```


Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fcl)

S1 uptime is 1 hour, 2 minutes

System returned to ROM by power-on

System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

```
Version ID           : V11
CLEI Code Number     : COM3L00BRF
Hardware Board Revision Number : 0x0A
```

```
Switch Ports Model          SW Version  SW Image
-----
*    1 26    WS-C2960-24TT-L  15.0(2)SE   C2960-LANBASEK9-M
```

```
Configuration register is 0xF
```

```
Switch#
```

¿Cuál es el nombre de la imagen del IOS que el switch está ejecutando?

La versión de la imagen puede variar, pero las respuestas serían algo así como c2960-lanbasek9-mz.150-2.SE.bin.

¿Cuánta memoria de acceso aleatorio dinámica (DRAM) tiene el switch?

Las respuestas pueden variar, pero la configuración de la memoria DRAM predeterminada en un switch 2960-24TT-L es 65 536 K de memoria.

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el switch?

Las respuestas pueden variar, pero la configuración de la memoria no volátil predeterminada en un switch 2960-24TT-L es 64 KB.

¿Cuál es el número de modelo del switch?

Las respuestas pueden variar, pero la respuesta debe aparecer de esta manera: WS-C2960-24TT-L.

Paso 2: Mostrar la tabla de enrutamiento en el router

Utilice el comando **show ip route** en el router para responder las preguntas siguientes.

```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0
```

```
L      192.168.0.1/32 is directly connected, GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

¿Qué código se utiliza en la tabla de enrutamiento para indicar una red conectada directamente? _____

La C designa una subred conectada directamente. Una L designa una interfaz local. Las dos respuestas son correctas.

¿Cuántas entradas de ruta están codificadas con un código C en la tabla de enrutamiento? _____ 2

¿Qué tipos de interfaces están asociadas a las rutas con código C?

Las respuestas pueden variar según el tipo de router, pero en el router 1941, la respuesta correcta es G0/0 y G0/1.

Paso 3: Mostrar información de la interfaz en el router.

Utilice el comando **show interface g0/1** para responder las preguntas siguientes.

```
R1# show interfaces g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    17 packets input, 5409 bytes, 0 no buffer
    Received 17 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 13 multicast, 0 pause input
    14 packets output, 1743 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    3 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es el estado operativo de la interfaz G0/1?

GigabitEthernet0/1 is up, line protocol is up

¿Cuál es la dirección de control de acceso al medio (MAC) de la interfaz G0/1?

Las respuestas varían, pero deben aparecer en la forma: xxxx.xxxx.xxxx, donde cada x se reemplazará por un número hexadecimal.

¿Cómo se muestra la dirección de Internet en este comando?

La dirección de Internet es 192.168.1.1/24.

Paso 4: Mostrar una lista de resumen de las interfaces del router y del switch.

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. Uno de los más útiles es el comando **show ip interface brief**. El resultado del comando muestra una lista resumida de las interfaces en el dispositivo e informa de inmediato el estado de cada interfaz.

- a. Introduzca el comando **show ip interface brief** en el router.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	192.168.0.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

```
R1#
```

- b. Introduzca el comando **show ip interface brief** en el switch.

```
Switch# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down

```
FastEthernet0/21      unassigned      YES unset  down      down
FastEthernet0/22      unassigned      YES unset  down      down
FastEthernet0/23      unassigned      YES unset  down      down
FastEthernet0/24      unassigned      YES unset  down      down
GigabitEthernet0/1    unassigned      YES unset  down      down
GigabitEthernet0/2    unassigned      YES unset  down      down
Switch#
```

Reflexión

- Si la interfaz G0/1 se mostrara administrativamente inactiva, ¿qué comando de configuración de interfaz usaría para activar la interfaz?

R1(config-if)# no shut

- ¿Qué ocurriría si hubiera configurado incorrectamente la interfaz G0/1 en el router con una dirección IP 192.168.1.2?
-

La PC-A no podría hacer ping a la PC-B. Esto se debe a que la PC-B está en una red diferente que la PC-A que requiere el router de gateway predeterminado para dirigir estos paquetes. La PC-A está configurada para utilizar la dirección IP 192.168.1.1 para el router de gateway predeterminado, pero esta dirección no está asignada a ningún dispositivo en la LAN. Cualquier paquete que deba enviarse al gateway predeterminado para su enrutamiento nunca llegará al destino.

Tabla de resumen de interfaces del router

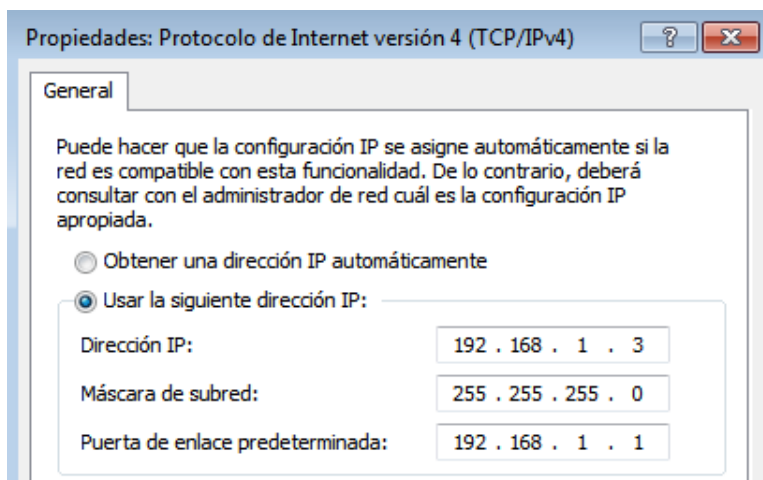
Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

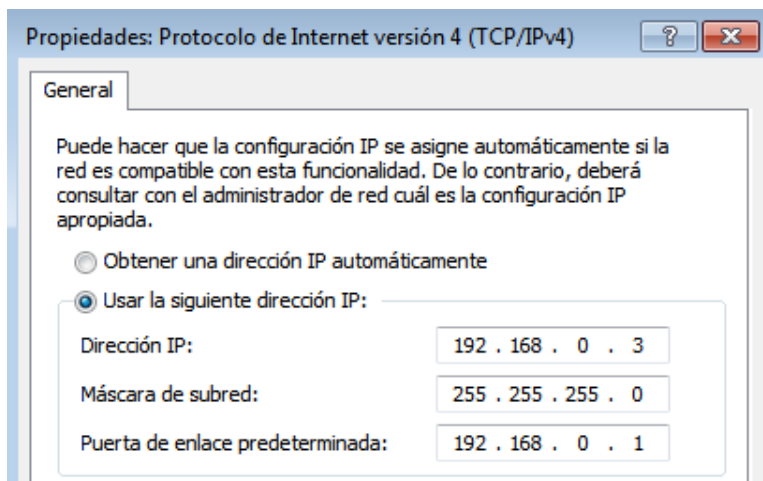
Apéndice A: Detalles de configuración para los pasos de la parte 2

Paso 1: Configure las interfaces de la PC.

- a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.



- b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.



- c. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\>
```

Paso 2: Configurar el router.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
Router#
```

- b. Entre al modo de configuración.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- c. Asigne un nombre de dispositivo al router.

```
Router(config)# hostname R1
```

- d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

```
R1(config)# no ip domain-lookup
```

- e. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

```
R1(config)# enable secret class
```

- f. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

- g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

- h. Encripte las contraseñas de texto no cifrado.

```
R1(config)# service password-encryption
```

- i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
  Unauthorized access prohibited!
#
R1(config)#
```

- j. Configure y active las dos interfaces en el router.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B.
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shut
```

```
R1(config-if)#
*Nov 29 23:49:44.195: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
down
*Nov 29 23:49:47.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
up
*Nov 29 23:49:48.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1.
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# exit
*Nov 29 23:50:15.283: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
*Nov 29 23:50:18.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Nov 29 23:50:19.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1#
```

- k. Guarde la configuración en ejecución en el archivo de inicio.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

- l. Configure el reloj en el router.

```
R1# clock set 17:00:00 29 Nov 2012
R1#
*Nov 29 17:00:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:55:46
UTC Thu Nov 29 2012 to 17:00:00 UTC Thu Nov 29 2012, configured from console by
console.
R1#
```

Nota: utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar este comando.

- m. Haga ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```


Apéndice B: Inicialización y recarga de un router y un switch

Parte 1: Inicializar el router y volver a cargar

Paso 1: Conéctese al router.

Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando **enable**.

```
Router> enable
Router#
```

Paso 2: Elimine el archivo de configuración de inicio de la NVRAM.

Escriba el comando **erase startup-config** para eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM, non-volatile random-access memory).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Paso 3: Recargue el router.

Emita el comando **reload** para eliminar una antigua configuración de la memoria. Cuando reciba el mensaje Proceed with reload (Continuar con la recarga), presione Entrar para confirmar la recarga. Si se presiona cualquier otra tecla, se anula la recarga.

```
Router# reload
Proceed with reload? [confirm]
```

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 4: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Paso 5: Finalice el programa de instalación automática.

Se le solicitará que finalice el programa de instalación automática. Responda **yes** (sí) y, luego, presione Entrar.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Parte 2: Inicializar el switch y volver a cargar

Paso 1: Conéctese al switch.

Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Paso 2: Determine si se crearon redes de área local virtuales (VLAN, Virtual Local-Area Networks).

Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
Switch# show flash

Directory of flash:/

   2  -rwx           1919   Mar 1 1993 00:06:33 +00:00  private-config.text
   3  -rwx           1632   Mar 1 1993 00:06:33 +00:00  config.text
   4  -rwx          13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
   5  -rwx         11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
   6  -rwx            616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Paso 3: Elimine el archivo VLAN.

- a. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Entrar si introdujo el nombre de manera correcta.

- b. Cuando se le pregunte sobre la eliminación de este archivo, presione Entrar para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Paso 4: Borre el archivo de configuración de inicio.

Utilice el comando **erase startup-config** para borrar el archivo de configuración de inicio de la NVRAM. Cuando se le pregunte sobre la eliminación del archivo de configuración, presione Entrar para confirmar el borrado. (Si se presiona cualquier otra tecla, se anula la operación).

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Paso 5: Recargar el switch.

Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Cuando se le pregunte sobre la recarga del switch, presione Entrar para continuar con la recarga. (Si se presiona cualquier otra tecla, se anula la recarga).

```
Switch# reload
Proceed with reload? [confirm]
```

Nota: es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Entrar.

```
System configuration has been modified. Save? [yes/no]: no
```

Paso 6: Omita el diálogo de configuración inicial.

Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Escriba **no** en la petición de entrada y presione Entrar.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Configuraciones de dispositivos

Router R1

```
R1#show run
Building configuration...

Current configuration : 1360 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
```

```
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  description Connection to PC-B.  
  ip address 192.168.0.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  description Connection to S1.  
  ip address 192.168.1.1 255.255.255.0 duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
banner motd ^C  
Unauthorized access prohibited!  
^C  
!  
line con 0  
  password 7 13061E010803
```

```
login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 070C285F4D06
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

¿Puede leer este mapa? (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que los dispositivos de red utilizan tablas de enrutamiento para dirigir los paquetes a una red de destino.

- Dada una situación, los estudiantes determinarán si se debe utilizar la mensajería de alta confiabilidad. Se centrarán en si el último mensaje estaba completo, era correcto y se entregó de manera oportuna.

Información básica/Situación

Nota: se sugiere que los estudiantes trabajen de a dos; no obstante, si así lo prefieren, pueden completar esta actividad individualmente.

El instructor le proporcionará los resultados generados por el comando show ip route de un router. Utilice Packet Tracer para armar un modelo de topología con esta información de enrutamiento.

Como mínimo, en el modelo de topología se deben utilizar los componentes siguientes:

- 1 switch Catalyst 2960
- 1 router serie 1941 de Cisco con una tarjeta modular de puerto de conmutación HWIC-4ESW y IOS versión 15.1 o superior
- 3 PC (pueden ser servidores, PC genéricas, computadoras portátiles, etcétera).

Utilice la herramienta de notas de Packet Tracer para indicar las direcciones de las interfaces del router y las posibles direcciones para los dispositivos finales que eligió para el modelo.

Rotule todos los dispositivos finales, los puertos y las direcciones que se establecieron a partir de la información de la tabla de enrutamiento y el resultado del comando show ip route en el archivo de Packet Tracer. Haga una copia impresa del trabajo o guarde una copia del archivo para compartirlo con la clase.

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la forma en que una red se configura y luego se revisa según la información de la tabla de enrutamiento.

Imprima o proyecte el gráfico de la tabla 1 que se encuentra en la sección Recursos necesarios de este documento. Los estudiantes deben poder ayudarse entre sí mientras leen la tabla de enrutamiento proporcionada y crean el modelo utilizando el software Packet Tracer. Como resultado de esta actividad, se facilitará un debate en grupos pequeños.

Nota para el instructor: se sugiere, aunque no es obligatorio, que los estudiantes trabajen de a dos para realizar esta actividad.

Recursos necesarios

- Programa de software Packet Tracer
- **Tabla de enrutamiento 1:** los estudiantes pueden utilizar la tabla para ayudarse entre sí mientras leen la información proporcionada y luego crean el modelo utilizando Packet Tracer.

Tabla 1

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

Reflexión

1. ¿Cuál fue la parte más difícil del diseño de este modelo de red? Justifique su respuesta.

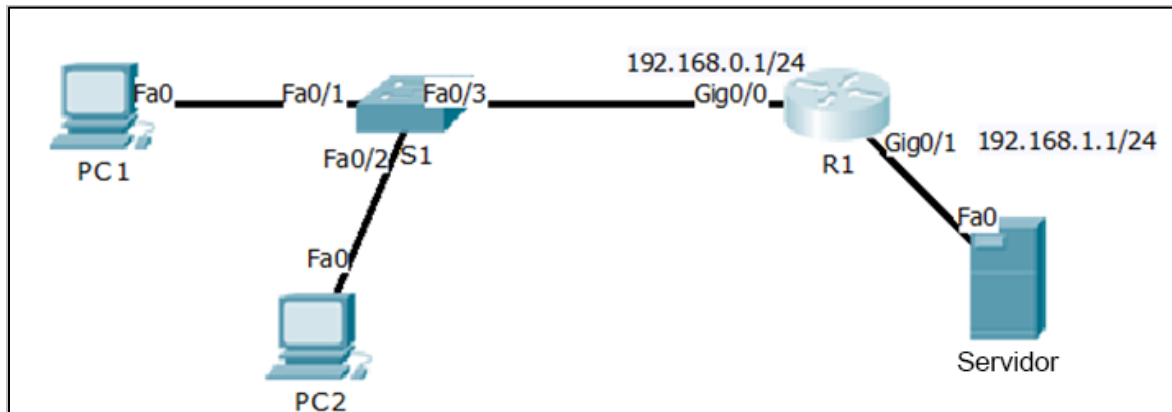
Las respuestas varían dentro de los grupos. Algunos estudiantes pueden mencionar los identificadores de origen y destino y otros pueden mencionar las direcciones IP reales que se citan en la tabla de enrutamiento. El concepto importante aquí es que puedan identificar cómodamente de dónde proviene la información incluida en la tabla de enrutamiento final según se detalla.

Las topologías varían según el grupo. Algunos estudiantes pueden colocar el switch fuera del puerto Gig0/1, etc.

Optativo: como **actividad de creación de modelos avanzada**, los estudiantes pueden crear una red simple de un router con cuatro interfaces Gigabit conectadas a dispositivos finales, configurar el router y las LAN con contraseñas, direcciones IP, anuncios, etc., y después crear una tabla de enrutamiento para respaldar la información de la red.

¿Puede leer este mapa?

La topología posible que creen los estudiantes podría verse así:



Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Al leer una tabla de enrutamiento, es posible verificar la forma en que una red se diseñó lógicamente.
- Una tabla de enrutamiento puede ayudar en la identificación de la topología física de la red.
- Una tabla de enrutamiento permite al lector identificar qué puertos están en funcionamiento y en qué redes.

Tenemos que hablar (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que los protocolos y servicios de capa de transporte admiten comunicaciones a través de las redes de datos.

- Los estudiantes determinarán si se deben utilizar métodos de entrega de comunicación de datos altos o bajos en contexto situacional.

Información básica/Situación

Nota: conviene realizar esta actividad en grupos medianos de seis a ocho estudiantes cada uno.

Este capítulo le permitirá comprender la forma en que los protocolos de la capa de transporte y los servicios admiten las comunicaciones de datos de la red.

El instructor susurrará un mensaje complejo al primer estudiante de un grupo. Por ejemplo, el mensaje puede ser: "El examen final se tomará el próximo martes 5 de febrero a las 14, en el aula 1151".

Ese estudiante le susurrará el mensaje al siguiente estudiante del grupo. Todos los grupos siguen este proceso hasta que todos los miembros de cada grupo hayan oído el mensaje susurrado. Las reglas que debe seguir son las siguientes:

- Puede susurrarle el mensaje al compañero junto a usted solo una vez.
- El mensaje se debe transmitir de una persona a otra sin saltar participantes. El instructor debe solicitarle a un estudiante que registre el tiempo total de transmisión del mensaje, desde el primero hasta el último participante. Se recomienda que tome el tiempo la primera o la última persona en recibir el mensaje.
- El último estudiante dirá en voz alta exactamente lo que escuchó.

A continuación, el instructor repetirá el mensaje original de modo que el grupo pueda compararlo con el mensaje provisto por el último estudiante del grupo.

Nota para el instructor: debe tener un mensaje complejo diferente para cada grupo de estudiantes. Inicie un debate acerca de lo que sucedió en la actividad. Céntrese en estas cinco preguntas:

1. ¿El mensaje estaba **completo** cuando llegó al último estudiante?
2. ¿El mensaje era **correcto** cuando se transmitió al último estudiante?
3. ¿Cuánto tardó el mensaje en llegar al último estudiante?
4. Si dependiera de este mensaje para organizar su agenda personal o empresarial, programa de estudio, etc., ¿el contenido de este mensaje debería ser totalmente correcto en el momento de recibirlo?
5. ¿El tiempo que lleva entregar el mensaje sería importante para el emisor y el destinatario?

Nota para el instructor: esta es una actividad de creación de modelos (MA). No tiene como fin ser una asignación con calificación. El objetivo es iniciar un debate entre los estudiantes acerca de su percepción sobre la forma en que los datos se transfieren de origen a destino, tanto en la práctica personal como corporativa. En este MA, se introduce a los alumnos a TCP/UDP, contenido de la capa de transporte.

Recursos necesarios

- Temporizador para el estudiante que lleva un registro de la duración de la conversación.

Reflexión

1. ¿El contenido de este mensaje debería ser totalmente correcto en el momento de recibirlo si dependiera de él para organizar su agenda personal o empresarial, programa de estudio, etc.?
2. ¿El tiempo que lleva entregar el mensaje sería un factor importante para el emisor y el destinatario?

En el debate iniciado como resultado de esta actividad, los estudiantes deben indicar lo siguiente:

- La importancia de los mensajes que se transmiten por completo del emisor al destinatario (TCP en comparación con UDP: ¿era el método de mensaje correcto para utilizar en esta situación?).
- La importancia de que los detalles del mensaje sean correctos del emisor al destinatario (entrega garantizada en comparación con entrega no garantizada: ¿el mensaje era correcto cuando llegó a la última persona?).
- La importancia de la temporización de un mensaje: para los detalles del mensaje y para la fecha y la hora necesarias para tomar medidas con respecto al mensaje (establecimiento del segmento y entrega en comparación con entrega del mensaje completo: ¿el mensaje tardó mucho en llegar al último estudiante?).

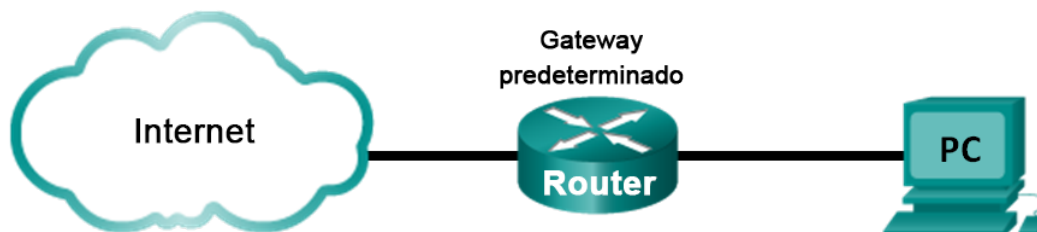
Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Los protocolos pueden establecer un método de envío y recepción de la información a través de una red (protocolos TCP/UDP).
- La calidad de la entrega de datos a través de una red puede verse afectada por el protocolo que se utiliza durante una conversación de la red (entrega de máximo esfuerzo).
- Los problemas y factores de temporización para la entrega de datos a través de un sistema de comunicaciones se ven afectados por la cantidad de datos que se envían en un momento y por el tipo de datos transportados (establecimiento y entrega del segmento: tanto TCP como UDP).

Práctica de laboratorio: Uso de Wireshark para observar el protocolo TCP de enlace de tres vías (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Preparar Wireshark para la captura de paquetes

- Seleccionar una interfaz NIC apropiada para capturar paquetes.

Parte 2: Capturar, localizar y examinar paquetes

- Capturar una sesión Web para www.google.com.
- Localizar paquetes apropiados para una sesión Web.
- Examinar la información de los paquetes, como direcciones IP, números de puerto TCP e indicadores de control TCP.

Información básica/Situación

En esta práctica de laboratorio, utilizará Wireshark para capturar y examinar paquetes que se generan entre el explorador de la PC mediante el protocolo de transferencia de hipertexto (HTTP) y un servidor Web, como www.google.com. Cuando una aplicación, como HTTP o el protocolo de transferencia de archivos (FTP), se inicia primero en un host, TCP utiliza el protocolo de enlace de tres vías para establecer una sesión TCP confiable entre los dos hosts. Por ejemplo, cuando una PC utiliza un explorador Web para navegar por Internet, se inicia un protocolo de enlace de tres vías y se establece una sesión entre el host de la PC y el servidor Web. Una PC puede tener varias sesiones TCP simultáneas activas con diversos sitios Web.

Nota: esta práctica de laboratorio no se puede realizar utilizando Netlab. Para la realización de esta práctica de laboratorio, se da por sentado que tiene acceso a Internet.

Nota para el instructor: el uso de un programa detector de paquetes como Wireshark se puede considerar una infracción de la política de seguridad del lugar de estudios. Se recomienda obtener permiso para realizar esta práctica de laboratorio antes de ejecutar Wireshark. Si el uso de un programa detector de paquetes como Wireshark constituye un problema, se sugiere que el instructor asigne la práctica de laboratorio como tarea para el hogar o realice una demostración explicativa.

Recursos necesarios

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

Parte 1: Preparar Wireshark para capturar paquetes

En la parte 1, inicia el programa Wireshark y selecciona la interfaz apropiada para comenzar a capturar paquetes.

Paso 1: Recuperar las direcciones de la interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

- a. Abra una ventana del símbolo del sistema, escriba **ipconfig /all** y luego presione Entrar.

```
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

- b. Anote las direcciones IP y MAC asociadas al adaptador Ethernet seleccionado, ya que esa es la dirección de origen que debe buscar al examinar los paquetes capturados.

Dirección IP del host de la PC: _____

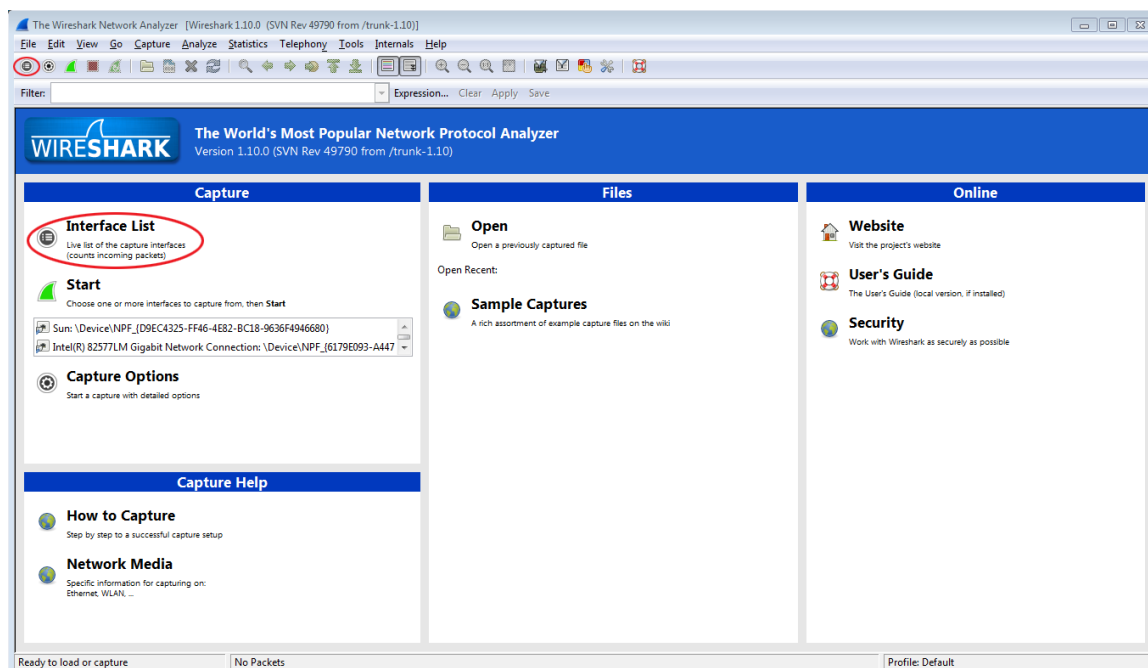
Las respuestas pueden variar. En este caso, 192.168.1.130.

Dirección MAC del host de la PC: _____

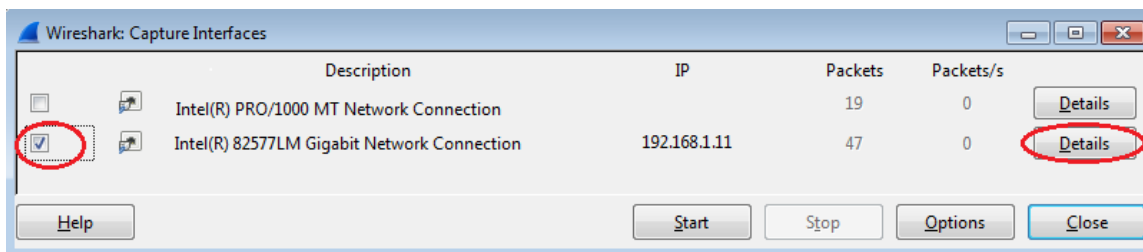
Las respuestas pueden variar. En este caso, C8:0A:A9:FA:DE:0D.

Paso 2: Iniciar Wireshark y seleccionar la interfaz apropiada

- a. Haga clic en el botón **Inicio** de Windows y, en el menú emergente, haga doble clic en **Wireshark**.
- b. Una vez que se inicia Wireshark, haga clic en **Interface List** (Lista de interfaces).



- c. En la ventana **Wireshark: Capture Interfaces** (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.



Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en **Details** (Detalles). Haga clic en la ficha **802.3 (Ethernet)** y verifique que la dirección MAC coincida con la que anotó en el paso 1b. Después de realizar esta verificación, cierre la ventana Interface Details (Detalles de la interfaz).

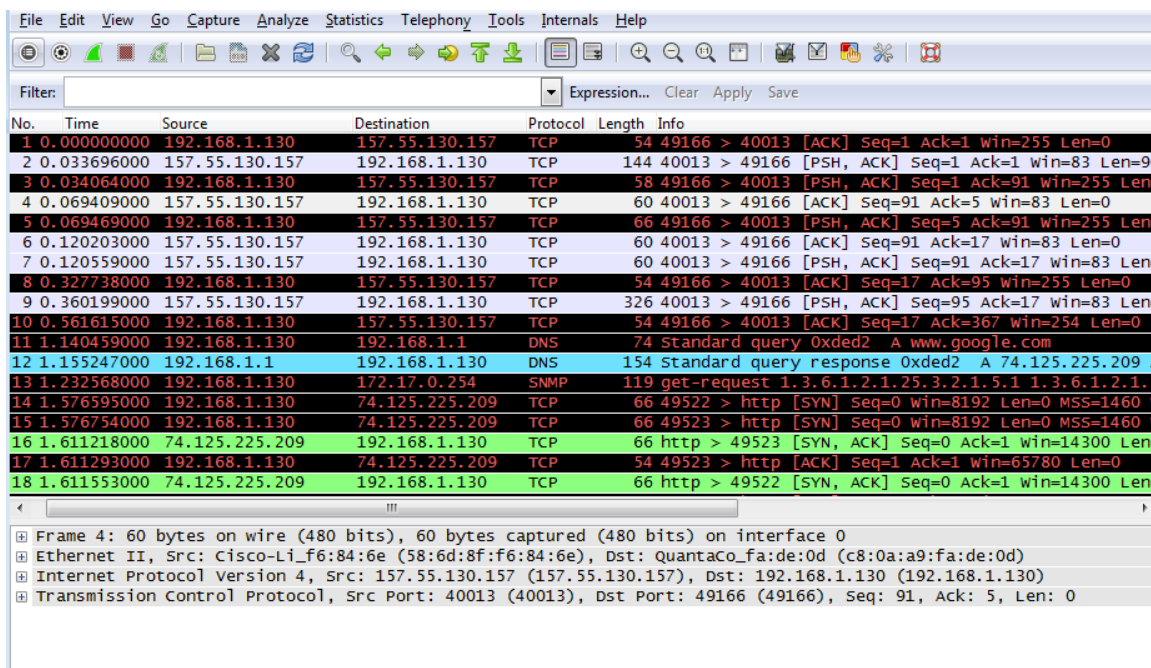
Parte 2: Capturar, localizar y examinar paquetes

Paso 1: Hacer clic en el botón Start (Comenzar) para iniciar la captura de datos

- a. Acceda a www.google.com. Minimice la ventana de Google y vuelva a Wireshark. Detenga la captura de datos. Debería ver tráfico capturado similar al que se muestra a continuación, en el paso b.

Nota: es posible que el instructor le proporcione un sitio Web diferente. En ese caso, introduzca el nombre del sitio Web o la dirección aquí:

- b. La ventana de captura ahora está activa. Ubique las columnas **Source** (Origen), **Destination** (Destino) y **Protocol** (Protocolo).



Paso 2: Localizar paquetes adecuados para la sesión Web

Si la PC se inició recientemente y no hubo actividad al acceder a Internet, puede ver todo el proceso en el resultado de la captura, incluido el protocolo de resolución de direcciones (ARP), el sistema de nombres de dominios (DNS) y el protocolo TCP de enlace de tres vías. La captura de pantalla de la parte 2, paso 1, muestra todos los paquetes que la PC debe obtener para `www.google.com`. En este caso, la PC ya tenía una entrada de ARP para el gateway predeterminado; por lo tanto, comenzó con la consulta DNS para resolver `www.google.com`.

- a. En la trama 11, se muestra la consulta DNS de la PC al servidor DNS, mediante la que se intenta resolver el nombre de dominio, `www.google.com`, a la dirección IP del servidor Web. La PC debe tener la dirección IP para poder enviar el primer paquete al servidor Web.

¿Cuál es la dirección IP del servidor DNS que consultó la PC? _____

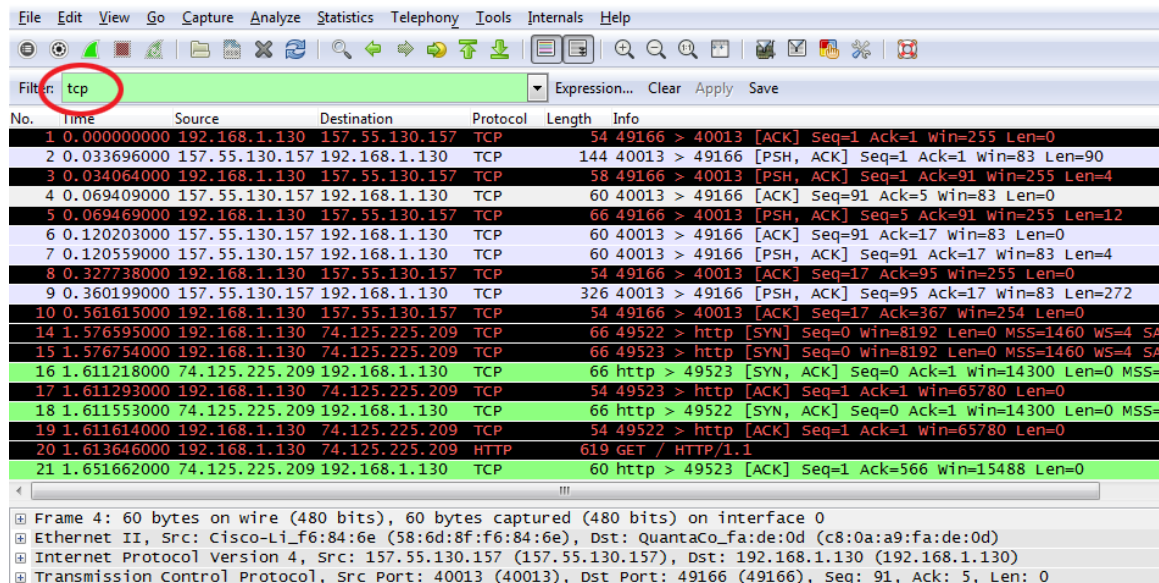
192.168.1.1

- b. La trama 12 es la respuesta del servidor DNS con la dirección IP de `www.google.com`.
- c. Busque el paquete apropiado para iniciar el protocolo de enlace de tres vías. En este ejemplo, la trama 15 es el inicio del protocolo TCP de enlace de tres vías.

¿Cuál es la dirección IP del servidor Web de Google? _____

En este ejemplo, 74.125.225.209.

- d. Si tiene muchos paquetes que no están relacionados con la conexión TCP, es posible que sea necesario usar la capacidad de filtro de Wireshark. Escriba `tcp` en el área de entrada de filtro de Wireshark y presione Entrar.

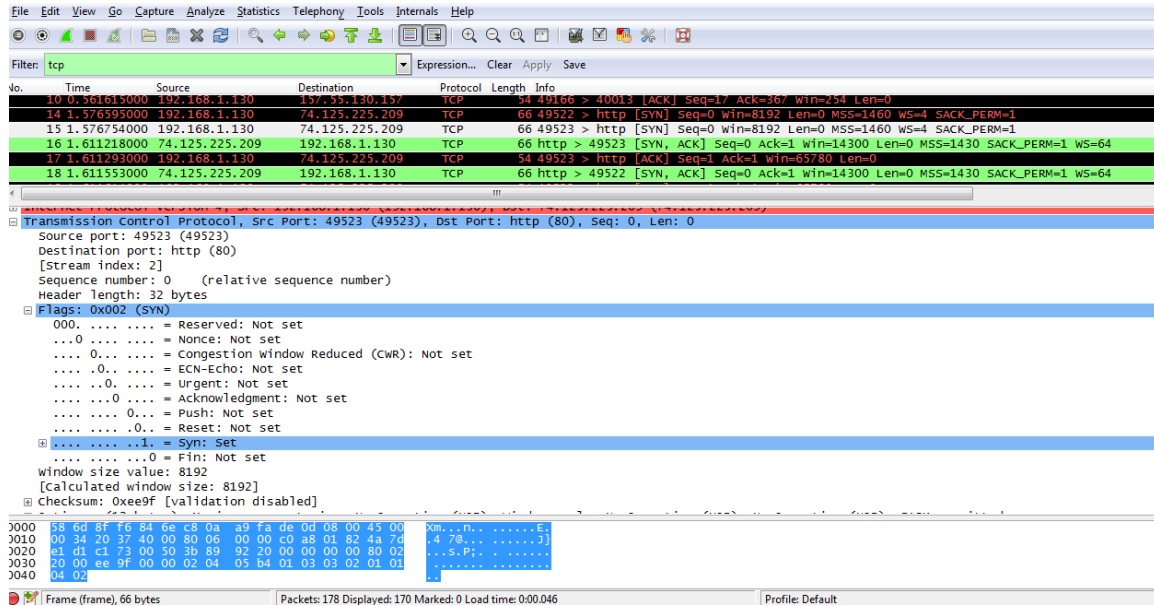


Paso 3: Examinar la información de los paquetes, como direcciones IP, números de puerto TCP e indicadores de control TCP

- a. En el ejemplo, la trama 15 es el inicio del protocolo de enlace de tres vías entre la PC y el servidor Web de Google. En el panel de la lista de paquetes (en la sección superior de la ventana principal), seleccione la trama. La línea se resalta, y en los dos paneles inferiores se muestra la información decodificada proveniente de ese paquete. Examine la información de TCP en el panel de detalles del paquete (sección media de la ventana principal).
- b. Haga clic en el ícono + que se encuentra a la izquierda del protocolo de control de transmisión (TCP) del panel de detalles del paquete para ampliar la vista de la información de TCP.

- c. Haga clic en el ícono **+** que está a la izquierda de los indicadores. Observe los puertos de origen y destino y los indicadores que están establecidos.

Nota: es posible que tenga que ajustar los tamaños de las ventanas superior y media de Wireshark para visualizar la información necesaria.



¿Cuál es el número de puerto de origen TCP? 49523 En este ejemplo, el puerto de origen es 49523. Las respuestas varían

¿Cómo clasificaría el puerto de origen? Dinámico o privado

¿Cuál es el número de puerto de destino TCP? 80

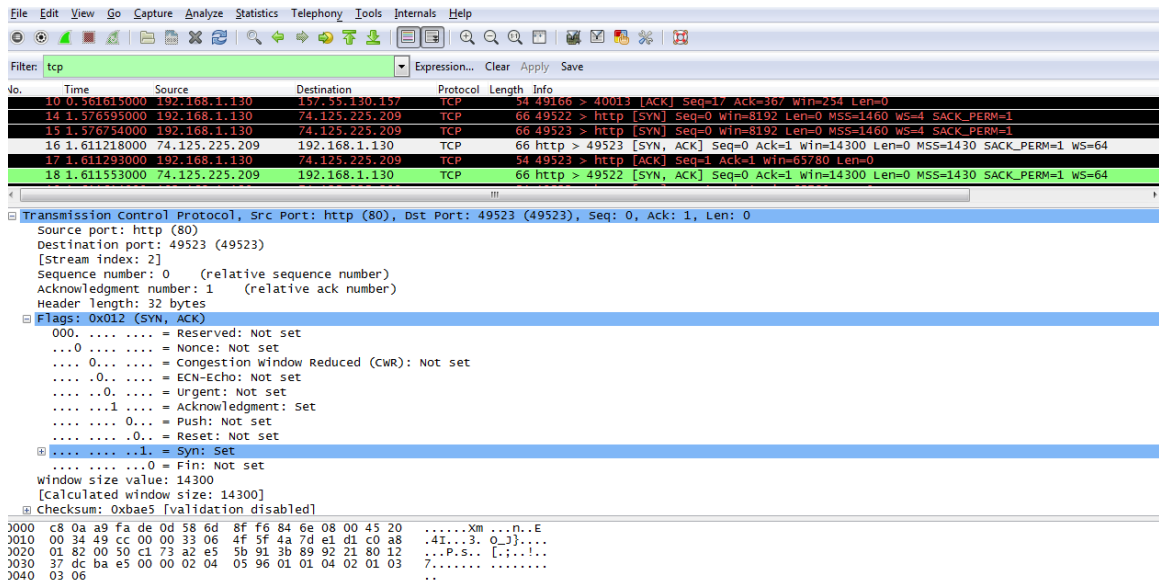
¿Cómo clasificaría el puerto de destino? Conocido, registrado (HTTP o protocolo Web)

¿Qué indicadores están establecidos? Indicador SYN

¿Cuál es el número de secuencia relativa establecido? 0

- d. Para seleccionar la próxima trama en le protocolo de enlace de tres vías, seleccione **Go** (Ir) en la barra de menús de Wireshark y, luego, **Next Packet in Conversation** (Siguiente paquete de la conversación). En este ejemplo, es la trama 16. Esta es la respuesta del servidor Web de Google a la solicitud inicial para iniciar una sesión.

Práctica de laboratorio: Uso de Wireshark para observar el protocolo TCP de enlace de tres vías



¿Cuáles son los valores de los puertos de origen y destino?

El puerto de origen ahora es 80 y el puerto de destino ahora es 49523.

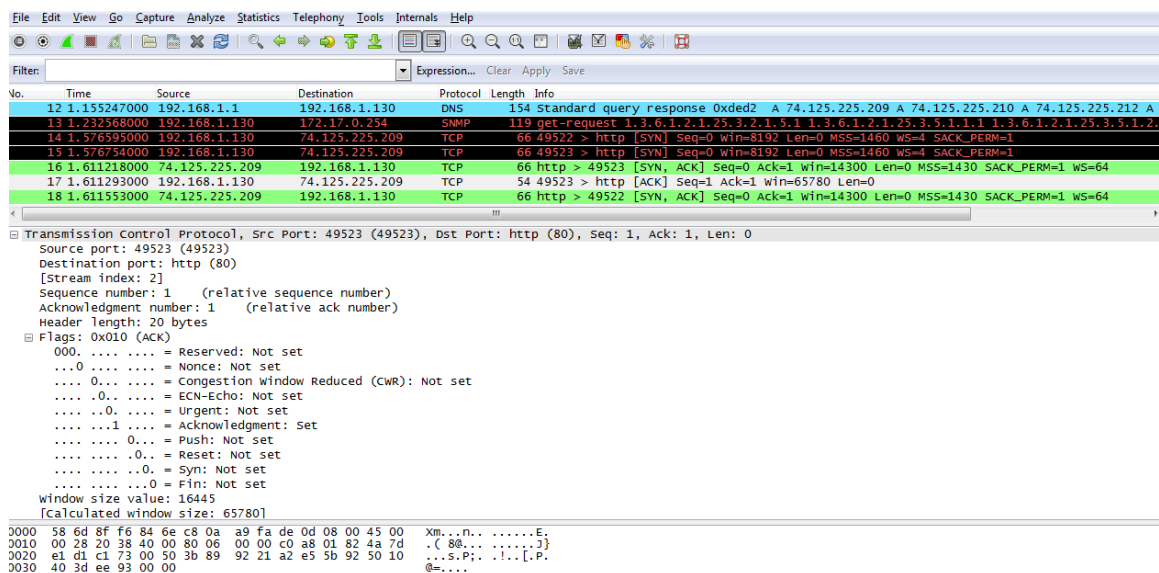
¿Qué indicadores están establecidos?

El indicador de acuse de recibo (ACK) y el indicador de sincronización (SYN).

¿Cuáles son los números de acuse de recibo y de secuencia relativa establecidos?

El número de secuencia relativa es 0 y el número de acuse de recibo es 1.

- e. Por último, examine el tercer paquete del protocolo de enlace de tres vías en el ejemplo. Al hacer clic en la trama 17 en la ventana superior, aparece la siguiente información en este ejemplo:



Examine el tercer y último paquete del protocolo de enlace.

¿Qué indicadores están establecidos?

Indicador de acuse de recibo (ACK)

Los números de acuse de recibo y de secuencia relativa están establecidos en 1 como punto de inicio. La conexión TCP ahora está establecida, y la comunicación entre la PC de origen y el servidor Web puede comenzar.

f. Cierre el programa Wireshark.

Reflexión

1. Hay cientos de filtros disponibles en Wireshark. Una red grande puede tener numerosos filtros y muchos tipos de tráfico diferentes. ¿Cuáles son los tres filtros de la lista que podrían ser los más útiles para un administrador de red?

Las respuestas varían, pero podrían incluir TCP, direcciones IP específicas (de origen o destino) y protocolos como HTTP.

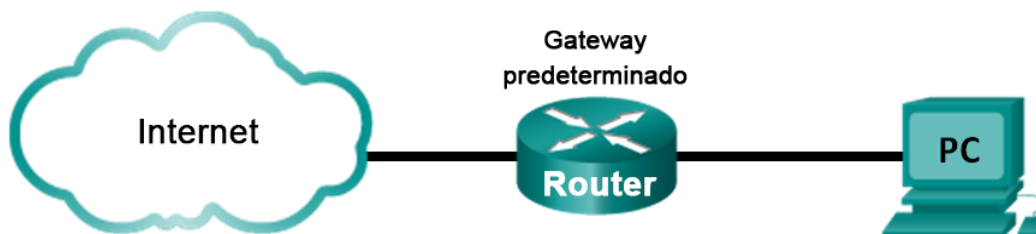
2. ¿De qué otras formas podría utilizarse Wireshark en una red de producción?

Wireshark suele utilizarse con fines de seguridad, para el análisis posterior del tráfico normal o después de un ataque de red. Es posible que se deban capturar nuevos protocolos o servicios para determinar qué puerto o puertos se utilizan.

Práctica de laboratorio: Uso de Wireshark para examinar una captura de UDP y DNS (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Registrar la información de configuración IP de una PC

Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

Parte 3: Analizar los paquetes DNS o UDP capturados

Información básica/Situación

Si alguna vez usó Internet, usó el Sistema de nombres de dominios (DNS). El DNS es una red distribuida de servidores que traduce nombres de dominio fáciles de usar, como www.google.com, en una dirección IP. Cuando escribe el URL de un sitio Web en el explorador, la PC realiza una consulta DNS a la dirección IP del servidor DNS. La consulta del servidor DNS de la PC y la respuesta del servidor DNS utilizan el protocolo de datagramas de usuario (UDP) como el protocolo de la capa de transporte. UDP opera sin conexión y no requiere una configuración de sesión como TCP. Las consultas y respuestas DNS son muy pequeñas y no requieren la sobrecarga de TCP.

En esta práctica de laboratorio, se comunicará con un servidor DNS enviando una consulta DNS mediante el protocolo de transporte UDP. Utilizará Wireshark para examinar los intercambios de consultas y respuestas DNS con el servidor de nombres.

Nota: esta práctica de laboratorio no se puede realizar utilizando Netlab. Para la realización de esta práctica de laboratorio, se da por sentado que tiene acceso a Internet.

Nota para el instructor: el uso de un programa detector de paquetes como Wireshark se puede considerar una infracción de la política de seguridad del lugar de estudios. Se recomienda obtener permiso para realizar esta práctica de laboratorio antes de ejecutar Wireshark. Si el uso de un programa detector de paquetes como Wireshark constituye un problema, se sugiere que el instructor asigne la práctica de laboratorio como tarea para el hogar o realice una demostración explicativa.

Recursos necesarios

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

Parte 1: Registrar la información de configuración IP de la PC

En la parte 1, utilizará el comando **ipconfig /all** en la PC local para buscar y registrar las direcciones MAC e IP de la tarjeta de interfaz de red (NIC) de la PC, la dirección IP del gateway predeterminado especificado y la dirección IP del servidor DNS especificada para la PC. Registre esta información en la tabla proporcionada. La información se utilizará en las partes siguientes de esta práctica de laboratorio con análisis de paquetes.

Dirección IP	Las respuestas varían. 192.168.1.11
Dirección MAC	Las respuestas varían. 90:4c:e5:be:15:63
Dirección IP de la puerta de enlace predeterminada	Las respuestas varían. 192.168.1.1
Dirección IP del servidor DNS	Las respuestas varían. 192.168.1.1

Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

En la parte 2, configurará Wireshark para capturar paquetes de consultas y respuestas DNS para demostrar el uso del protocolo de transporte UDP mientras se comunica con un servidor DNS.

- Haga clic en el botón **Inicio** de Windows y navegue hasta el programa Wireshark.
Nota: si Wireshark aún no está instalado, se puede descargar de <http://www.wireshark.org/download.html>.
- Seleccione una interfaz para que Wireshark capture paquetes. Utilice **Interface List** (Lista de interfaces) para elegir la interfaz asociada a las direcciones IP y de control de acceso al medio (MAC) registradas de la PC en la parte 1.
- Después de seleccionar la interfaz deseada, haga clic en **Start** (Comenzar) para capturar los paquetes.
- Abra un explorador Web y escriba **www.google.com**. Presione Entrar para continuar.
- Haga clic en **Stop** (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.

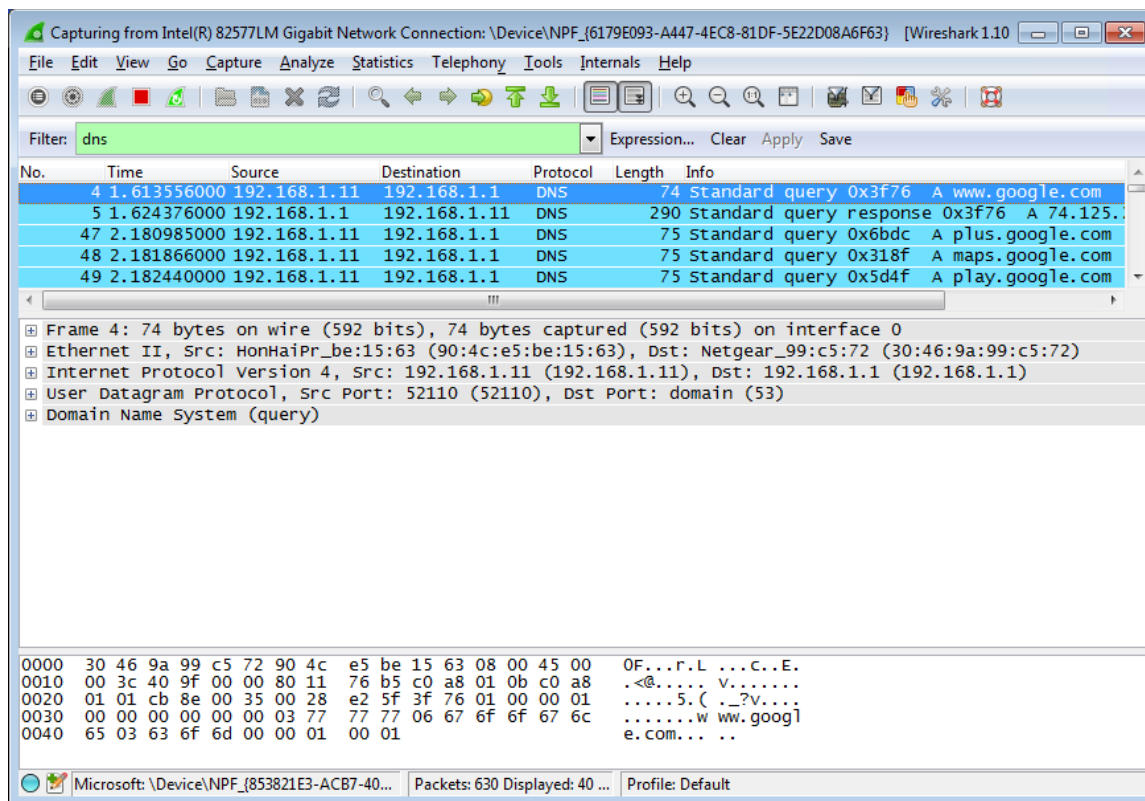
Parte 3: Analizar los paquetes DNS o UDP capturados

En la parte 3, examinará los paquetes UDP que se generaron al comunicarse con un servidor DNS para las direcciones IP para www.google.com.

Paso 1: Filtrar paquetes DNS

- En la ventana principal de Wireshark, escriba **dns** en el área de entrada de la barra de herramientas **Filter** (Filtrar). Haga clic en **Apply** (Aplicar) o presione Entrar.

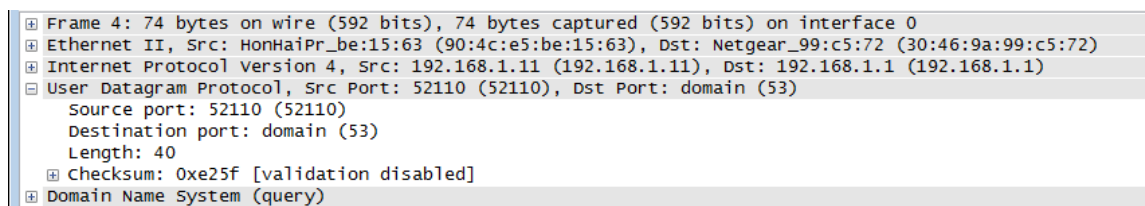
Nota: si no ve resultados después de aplicar el filtro DNS, cierre el explorador Web y, en la ventana del símbolo del sistema, escriba **ipconfig /flushdns** para eliminar todos los resultados anteriores del DNS. Reinicie la captura de Wireshark y repita las instrucciones de la parte 2b a la parte 2e. Si el problema no se resuelve, en la ventana del símbolo del sistema, puede escribir **nslookup www.google.com** como alternativa para el explorador Web.



- En el panel de la lista de paquetes (sección superior) de la ventana principal, ubique el paquete que incluye “standard query” (consulta estándar) y “A www.google.com”. Vea la trama 4, por ejemplo.

Paso 2: Examinar el segmento UDP mediante una consulta DNS

Examine UDP mediante una consulta DNS para www.google.com según lo capturado por Wireshark. En este ejemplo, está seleccionada la trama 4 de la captura de Wireshark en la lista de paquetes para su análisis. Los protocolos en esta consulta se muestran en el panel de detalles del paquete (sección media) de la ventana principal. Las entradas del protocolo están resaltadas en gris.



- En el panel de detalles del paquete, la trama 4 tenía 74 bytes de datos en el cable, tal como se muestra en la primera línea. Esta es la cantidad de bytes para enviar una consulta DNS a un servidor de nombres que solicita direcciones IP de www.google.com.
- En la línea Ethernet II, se muestran las direcciones MAC de origen y destino. La dirección MAC de origen proviene de la PC local, ya que esta originó la consulta DNS. La dirección MAC de destino proviene del gateway predeterminado, dado que esta es la última parada antes de que la consulta abandone la red local.
¿La dirección MAC de origen es la misma que la que se registró en la parte 1 para la PC local?

La respuesta debe ser afirmativa. De lo contrario, verifique que Wireshark esté utilizando la misma interfaz para capturar los paquetes.

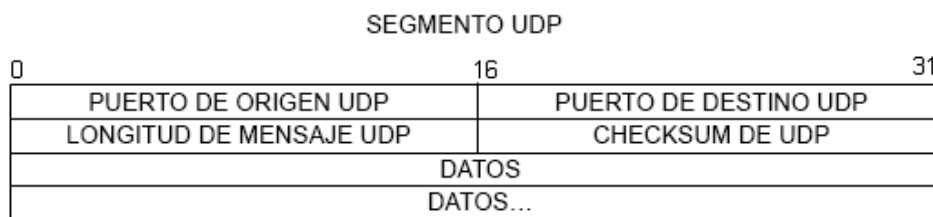
- c. En la línea Internet Protocol Version 4 (Protocolo de Internet versión 4), la captura de Wireshark de paquetes IP indica que la dirección IP de origen de esta consulta DNS es 192.168.1.11 y la dirección IP de destino es 192.168.1.1. En este ejemplo, la dirección de destino es el gateway predeterminado. El router es el gateway predeterminado en esta red.

¿Puede emparejar las direcciones IP y MAC para los dispositivos de origen y destino?

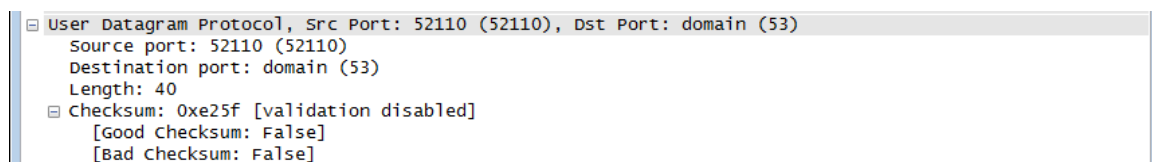
Dispositivo	Dirección IP	Dirección MAC
PC local	Las respuestas varían. 192.168.1.11	Las respuestas varían. 90:4c:e5:be:15:63
Gateway predeterminado	Las respuestas varían. 192.168.1.1	Las respuestas varían. 30:46:9a:99:c5:72

El paquete y el encabezado IP encapsulan el segmento UDP. El segmento UDP contiene la consulta DNS como los datos.

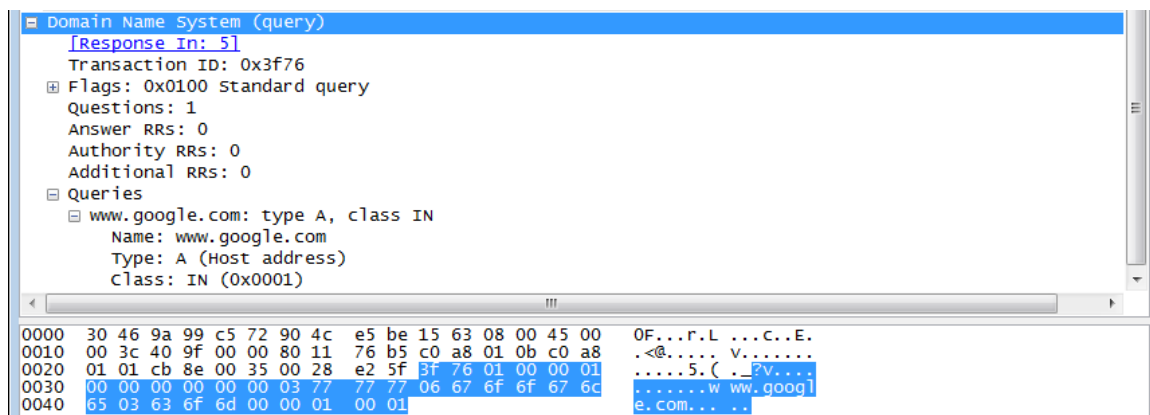
- d. Un encabezado UDP solo tiene cuatro campos: source port (puerto de origen), destination port (puerto de destino), length (longitud) y checksum. Cada campo en el encabezado UDP es de solo 16 bits, como se ilustra a continuación.



Amplíe el protocolo de datagramas de usuario en el panel de detalles del paquete haciendo clic en el signo más (+). Observe que hay solo cuatro campos. El número de puerto de origen en este ejemplo es 52110. La PC local generó el puerto de origen aleatoriamente utilizando los números de puerto que no están reservados. El puerto de destino es 53. El puerto 53 es un puerto conocido reservado para ser utilizado con DNS. En el puerto 53, los servidores DNS escuchan las consultas DNS de los clientes.



En este ejemplo, la longitud de este segmento UDP es de 40 bytes. De los 40 bytes, 8 bytes se utilizan como encabezado. Los otros 32 bytes los utilizan los datos de la consulta DNS. Estos 32 bytes están resaltados en la ilustración siguiente en el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.



El valor de checksum se usa para determinar la integridad del paquete después de haber atravesado Internet.

El encabezado UDP tiene una sobrecarga baja, porque UDP no tiene campos asociados con el protocolo de enlace de tres vías en TCP. Cualquier problema de confiabilidad de transferencia de datos que ocurra debe solucionarse en la capa de aplicación.

Registre los resultados de Wireshark en la tabla siguiente:

Tamaño de trama	
Dirección MAC de origen	
Dirección MAC de destino	
Dirección IP de origen	
Dirección IP de destino	
Puerto de origen	
Puerto de destino	

¿La dirección IP de origen es la misma que la dirección IP de la PC local registrada en la parte 1?

Sí

¿La dirección IP de destino es la misma que el gateway predeterminado que se registró en la parte 1?

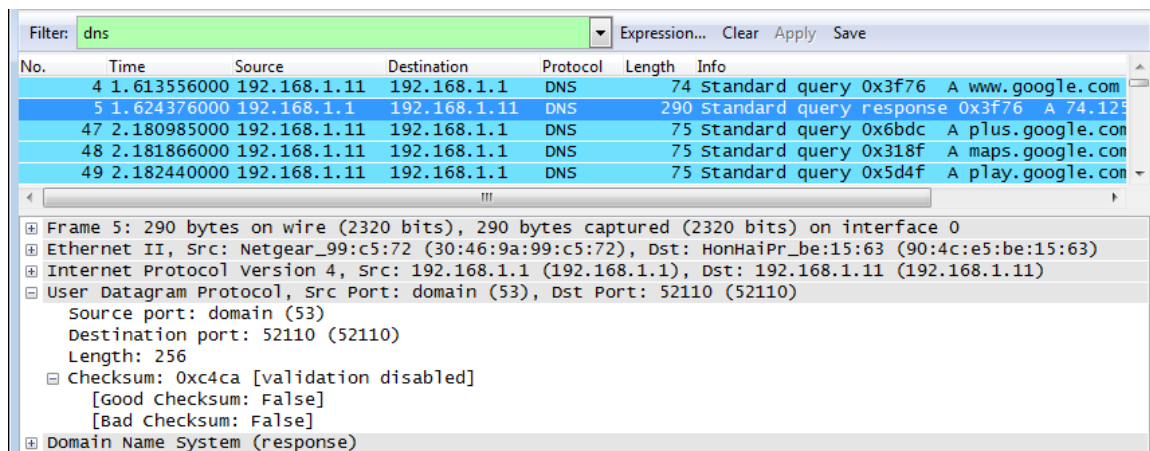
Sí

Sí, si el gateway predeterminado también ejecuta el DNS; de lo contrario, la respuesta es no.

Paso 3: Examinar el UDP usando la respuesta DNS

En este paso, examinará el paquete de respuesta DNS y verificará que este también utilice UDP.

- En este ejemplo, la trama 5 es el paquete de respuesta DNS correspondiente. Observe que la cantidad de bytes en el cable es 290 bytes. Es un paquete más grande con respecto al paquete de consulta DNS.



- b. En la trama Ethernet II para la respuesta DNS, ¿de qué dispositivo proviene la dirección MAC de origen y de qué dispositivo proviene la dirección MAC de destino?

La dirección MAC de origen es el gateway predeterminado y la dirección MAC de destino es el host local.

- c. Observe las direcciones IP de origen y destino en el paquete IP. ¿Cuál es la dirección IP de destino? ¿Cuál es la dirección IP de origen?

Dirección IP de destino: _____ Dirección IP de origen: _____

La respuesta varía. En este ejemplo, destino: 192.168.1.11; origen: 192.168.1.1

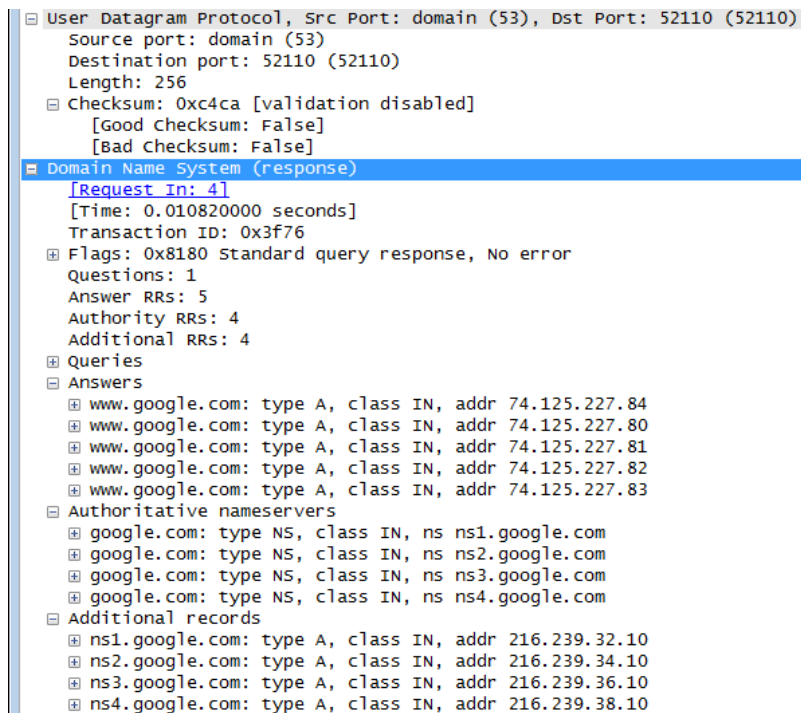
¿Qué ocurrió con los roles de origen y destino para el host local y el gateway predeterminado?

El host local y el gateway predeterminado invirtieron sus roles en los paquetes de consulta y respuesta DNS.

- d. En el segmento UDP, el rol de los números de puerto también se invirtió. El número de puerto de destino es 52110. El número de puerto 52110 es el mismo puerto que el que generó la PC local cuando se envió la consulta DNS al servidor DNS. La PC local escucha una respuesta DNS en este puerto.

El número de puerto de origen es 53. El servidor DNS escucha una consulta DNS en el puerto 53 y luego envía una respuesta DNS con un número de puerto de origen 53 de vuelta a quien originó la consulta DNS.

Cuando la respuesta DNS esté expandida, observe las direcciones IP resueltas para www.google.com en la sección **Answers** (Respuestas).



The image shows a Wireshark packet capture details pane for a User Datagram Protocol (UDP) packet. The packet is a Domain Name System (DNS) response. The details are as follows:

- User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)
 - Source port: domain (53)
 - Destination port: 52110 (52110)
 - Length: 256
 - Checksum: 0xc4ca [validation disabled]
 - [Good Checksum: False]
 - [Bad Checksum: False]
- Domain Name System (response)
 - [Request In: 4]
 - [Time: 0.010820000 seconds]
 - Transaction ID: 0x3f76
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 5
 - Authority RRs: 4
 - Additional RRs: 4
 - Queries
 - Answers
 - www.google.com: type A, class IN, addr 74.125.227.84
 - www.google.com: type A, class IN, addr 74.125.227.80
 - www.google.com: type A, class IN, addr 74.125.227.81
 - www.google.com: type A, class IN, addr 74.125.227.82
 - www.google.com: type A, class IN, addr 74.125.227.83
 - Authoritative nameservers
 - google.com: type NS, class IN, ns ns1.google.com
 - google.com: type NS, class IN, ns ns2.google.com
 - google.com: type NS, class IN, ns ns3.google.com
 - google.com: type NS, class IN, ns ns4.google.com
 - Additional records
 - ns1.google.com: type A, class IN, addr 216.239.32.10
 - ns2.google.com: type A, class IN, addr 216.239.34.10
 - ns3.google.com: type A, class IN, addr 216.239.36.10
 - ns4.google.com: type A, class IN, addr 216.239.38.10

Reflexión

¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para DNS?

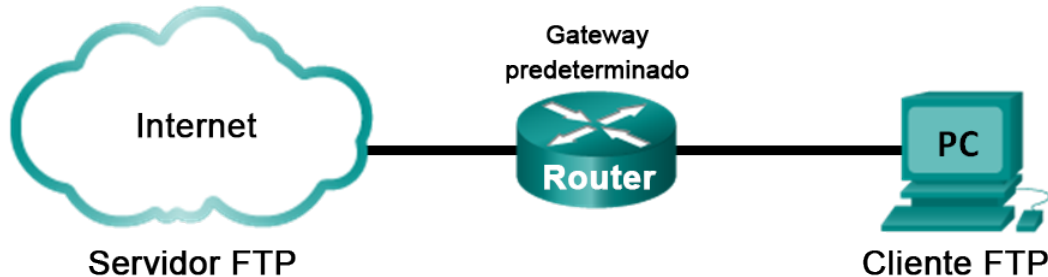
UDP como protocolo de transporte proporciona un rápido establecimiento de sesión, respuesta rápida, sobrecarga mínima, que no haya necesidad de reintentos, rearmado de segmentos y acuse de recibo de los paquetes recibidos.

Práctica de laboratorio: Uso de Wireshark para examinar capturas de FTP y TFTP (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología: parte 1 (FTP)

En la parte 1, se resaltará una captura de TCP de una sesión FTP. Esta topología consta de una PC con acceso a Internet.



Topología: parte 2 (TFTP)

En la parte 2, se resaltará una captura de UDP de una sesión TFTP. La PC debe tener tanto una conexión Ethernet como una conexión de consola para el switch S1.



Tabla de direccionamiento (parte 2)

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.1	255.255.255.0	No aplicable
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark

Parte 2: Identificar campos de encabezado y operación UDP mediante una captura de sesión TFTP de Wireshark

Información básica/Situación

Los dos protocolos en la capa de transporte TCP/IP son TCP, definido en RFC 761, y UDP, definido en RFC 768. Los dos protocolos admiten la comunicación de protocolos de la capa superior. Por ejemplo, TCP se utiliza para proporcionar soporte de la capa de transporte para los protocolos de transferencia de hipertexto (HTTP) y FTP, entre otros. UDP proporciona soporte de la capa de transporte para el Sistema de nombres de dominios (DNS) y TFTP, entre otros.

Nota: entender las partes de los encabezados y de la operación TCP y UDP es una aptitud fundamental con la que deben contar los ingenieros de red.

En la parte 1 de esta práctica de laboratorio, utilizará la herramienta de código abierto de Wireshark para capturar y analizar campos de encabezado del protocolo TCP para las transferencias de archivos FTP entre el equipo host y un servidor FTP anónimo. Para conectarse a un servidor FTP anónimo y descargar un archivo, se emplea la utilidad de línea de comandos de Windows. En la parte 2 de esta práctica de laboratorio, utilizará Wireshark para capturar y analizar campos de encabezado del protocolo UDP para las transferencias de archivos TFTP entre el equipo host y el switch S1.

Nota para el instructor: si la versión 1.8.3 o posterior de Wireshark no está cargada en la PC, se puede descargar del URL <http://www.wireshark.org/download.html>. Para la parte 2 de la práctica de laboratorio, si la versión 4.0 o posterior de tftpd32 no está cargada en la PC, se puede descargar del URL http://tftpd32.jounin.net/tftpd32_download.html.

Nota: el switch que se utiliza es Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: asegúrese de que el switch se haya borrado y de que no tenga configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: en la parte 1, se supone que la PC tiene acceso a Internet, y no se puede realizar utilizando Netlab. La parte 2 es compatible con Netlab.

Nota para el instructor: las instrucciones para borrar el switch se encuentran en el manual de prácticas de laboratorio.

Nota para el instructor: esta práctica de laboratorio se puede realizar en dos sesiones según la disponibilidad de tiempo y equipos. La secuencia de la parte 1 y de la parte 2 no es fundamental.

Nota para el instructor: el uso de un programa detector de paquetes como Wireshark se puede considerar una infracción de la política de seguridad del lugar de estudios. Se recomienda obtener permiso para realizar esta práctica de laboratorio antes de ejecutar Wireshark. Si el uso de un programa detector de paquetes como Wireshark constituye un problema, se sugiere que el instructor asigne la práctica de laboratorio como tarea para el hogar o realice una demostración explicativa.

Recursos necesarios: parte 1 (FTP)

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

Recursos necesarios: parte 2 (TFTP)

- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con Wireshark y un servidor TFTP, como tftpd32, instalados)
- Cable de consola para configurar los dispositivos Cisco IOS a través del puerto de consola
- Cable Ethernet como se muestra en la topología

Parte 1: Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark

En la parte 1, se utiliza Wireshark para capturar una sesión FTP e inspeccionar los campos de encabezado TCP.

Paso 1: Inicie una captura de Wireshark.

- Cierre todo el tráfico de la red innecesario, como el explorador Web, para limitar la cantidad de tráfico durante la captura de Wireshark.
- Inicie la captura de Wireshark.

Paso 2: Descargar el archivo Léame

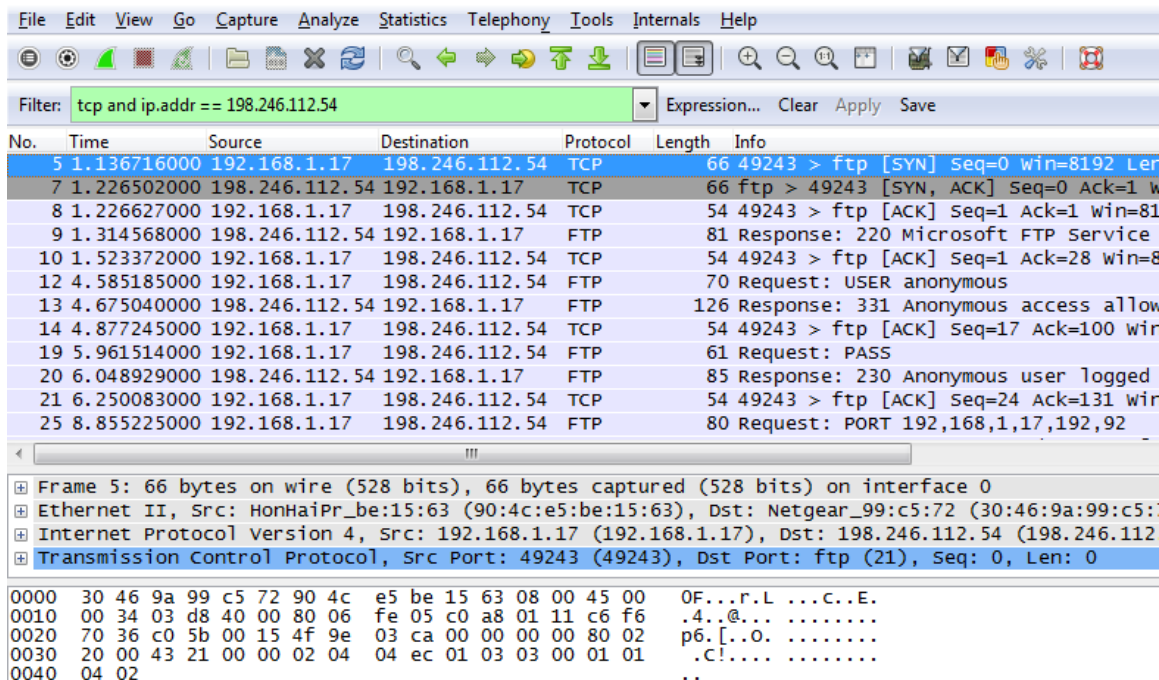
- En el símbolo del sistema, introduzca **ftp ftp.cdc.gov**.
- Conéctese al sitio FTP de Centros para el Control y la Prevención de Enfermedades (CDC) con el usuario **anonymous** y sin contraseña.
- Ubique y descargue el archivo Léame.

```
C:\Users\user1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
Siteinfo
up.htm
w3c
web.config
welcome.msg
226 Transfer complete.
ftp: 76 bytes received in 0.00Seconds 19.00Kbytes/sec.
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.01Seconds 204.00Kbytes/sec.
ftp> quit
221
```

Paso 3: Detener la captura de Wireshark

Paso 4: Ver la ventana principal de Wireshark

Wireshark capturó muchos paquetes durante la sesión FTP a ftp.cdc.gov. Para limitar la cantidad de datos para analizar, escriba **tcp and ip.addr == 198.246.112.54** en el área de entrada **Filter:** (Filtrar:) y haga clic en **Apply** (Aplicar). La dirección IP, 198.246.112.54, es la dirección para ftp.cdc.gov.



Paso 5: Analizar los campos TCP

Una vez aplicado el filtro TCP, las primeras tres tramas en el panel de la lista de paquetes (sección superior) muestran el protocolo de la capa de transporte TCP que crea una sesión confiable. La secuencia de [SYN], [SYN, ACK] y [ACK] ilustra el protocolo de enlace de tres vías.

5	1.136716000	192.168.1.17	198.246.112.54	TCP	66	49243 > ftp [SYN] Seq=0 win=8192 Len=0
7	1.226502000	198.246.112.54	192.168.1.17	TCP	66	ftp > 49243 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
8	1.226627000	192.168.1.17	198.246.112.54	TCP	54	49243 > ftp [ACK] Seq=1 Ack=1 win=8192

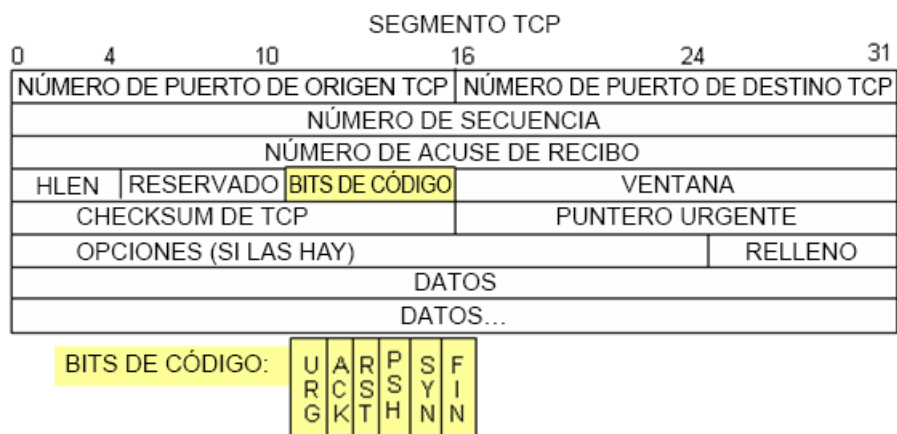
El TCP se utiliza en forma continua durante una sesión para controlar la entrega del datagrama, verificar la llegada del datagrama y administrar el tamaño de la ventana. Por cada intercambio de datos entre el cliente FTP y el servidor FTP, se inicia una nueva sesión TCP. Al término de la transferencia de datos, se cierra la sesión TCP. Por último, cuando la sesión FTP finaliza, TCP realiza un cierre y terminación ordenados.

En Wireshark, se encuentra disponible información detallada sobre TCP en el panel de detalles del paquete (sección media). Resalte el primer datagrama TCP del equipo host y expanda el registro TCP. El datagrama TCP expandido parece similar al panel de detalles del paquete que se muestra a continuación.

```

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.112.54 (198.246.112.54)
Transmission Control Protocol, Src Port: 49243 (49243), Dst Port: ftp (21), Seq: 0, Len: 0
  Source port: 49243 (49243)
  Destination port: ftp (21)
  [Stream index: 0]
  Sequence number: 0 (relative sequence number)
  Header length: 32 bytes
  Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (cwr): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...0 = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... ..... 0.. = Reset: Not set
    .... .... .1. = Syn: Set
    .... .... ...0 = Fin: Not set
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x4321 [validation disabled]
  Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), No

```



La imagen anterior es un diagrama del datagrama TCP. Se proporciona una explicación de cada campo para referencia:

- El **número de puerto de origen TCP** pertenece al host de la sesión TCP que inició una conexión. Generalmente el valor es un valor aleatorio superior a 1,023.
- El **número de puerto de destino TCP** se utiliza para identificar el protocolo de capa superior o la aplicación en el sitio remoto. Los valores en el intervalo de 0 a 1023 representan los “puertos bien conocidos” y están asociados a servicios y aplicaciones populares (como se describe en la RFC 1700, por ejemplo, Telnet, FTP, HTTP, etc.). La combinación de dirección IP de origen, puerto de origen, dirección IP de destino y puerto de destino identifica de manera exclusiva la sesión tanto para el emisor como para el receptor.

Nota: en la captura de Wireshark que se muestra a continuación, el puerto de destino es 21, que es FTP. Los servidores FTP escuchan las conexiones de cliente FTP en el puerto 21.

- El **número de secuencia** especifica el número del último octeto en un segmento.
- El **número de acuse de recibo** especifica el próximo octeto que espera el receptor.
- Los **bits de código** tienen un significado especial en la administración de sesión y en el tratamiento de los segmentos. Entre los valores interesantes se encuentran:

- ACK: acuse de recibo de un segmento.
- SYN: sincronizar; solo está configurado cuando se negocia una sesión TCP nueva durante el protocolo de enlace de tres vías.
- FIN: finalizar; solicitud para cerrar la sesión TCP.
- **Window size** (Tamaño de la ventana) es el valor de la ventana deslizante; determina cuántos octetos se pueden enviar antes de esperar un acuse de recibo.
- **Urgent pointer** (Indicador urgente) se utiliza solo con un indicador urgente (URG) cuando el emisor necesita enviar datos urgentes al receptor.
- En **Options** (Opciones), hay una sola opción actualmente, y se define como el tamaño máximo del segmento TCP (valor optativo).

Utilice la captura de Wireshark del inicio de la primera sesión TCP (bit SYN establecido en 1) para completar la información acerca del encabezado TCP:

De la PC al servidor CDC (solo el bit SYN está establecido en 1):

Dirección IP de origen:	192.168.1.17*
Dirección IP de destino:	198.246.112.54
Número de puerto de origen:	49243*
Número de puerto de destino:	21
Número de secuencia:	0 (relativo)
Número de acuse de recibo:	No es aplicable a esta captura
Longitud del encabezado:	32 bytes
Tamaño de la ventana:	8192

*Las respuestas de los estudiantes variarán.

En la segunda captura filtrada de Wireshark, el servidor FTP de CDC acusa recibo de la solicitud de la PC. Observe los valores de los bits SYN y ACK.

```
Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: HonHaiPr_be:15:63 (90:4c:e5:be:15:63)
Internet Protocol Version 4, Src: 198.246.112.54 (198.246.112.54), Dst: 192.168.1.17 (192.168.1.17)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49243 (49243), Seq: 0, Ack: 1, Len: 0
  Source port: ftp (21)
  Destination port: 49243 (49243)
  [Stream index: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header length: 32 bytes
  Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
  window size value: 64240
  [calculated window size: 64240]
  Checksum: 0x05bb [validation disabled]
  Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), N
  [SEQ/ACK analysis]
```

Complete la siguiente información con respecto al mensaje SYN-ACK.

Dirección IP de origen:	198.246.112.54
Dirección IP de destino:	192.168.1.17*
Número de puerto de origen:	21
Número de puerto de destino:	49243*
Número de secuencia:	0 (relativo)
Número de acuse de recibo:	1
Longitud del encabezado:	32 bytes
Tamaño de la ventana:	64240

*Las respuestas de los estudiantes variarán.

En la etapa final de la negociación para establecer las comunicaciones, la PC envía un mensaje de acuse de recibo al servidor. Observe que solo el bit ACK está establecido en 1, y el número de secuencia se incrementó a 1.

```
⊕ Frame 8: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊕ Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
⊕ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.112.54 (198.246.112.54)
⊖ Transmission Control Protocol, Src Port: 49243 (49243), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0
    Source port: 49243 (49243)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 1 (relative sequence number)
    Acknowledgment number: 1 (relative ack number)
    Header length: 20 bytes
    ⊖ Flags: 0x010 (ACK)
        000. .... = Reserved: Not set
        ...0 .... = Nonce: Not set
        .... 0... = Congestion Window Reduced (CWR): Not set
        .... .0.. = ECN-Echo: Not set
        .... ..0. = Urgent: Not set
        .... ...1 = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    window size value: 8192
    [Calculated window size: 8192]
    [window size scaling factor: 1]
    ⊕ Checksum: 0x2127 [validation disabled]
    ⊕ [SEQ/ACK analysis]
```


Complete la siguiente información con respecto al mensaje ACK.

Dirección IP de origen:	192.168.1.17*
Dirección IP de destino:	198.246.112.54
Número de puerto de origen:	49243*
Número de puerto de destino:	21
Número de secuencia:	1
Número de acuse de recibo:	1
Longitud del encabezado:	20
Tamaño de la ventana:	8192*

*Las respuestas de los estudiantes variarán.

¿Cuántos otros datagramas TCP contenían un bit SYN?

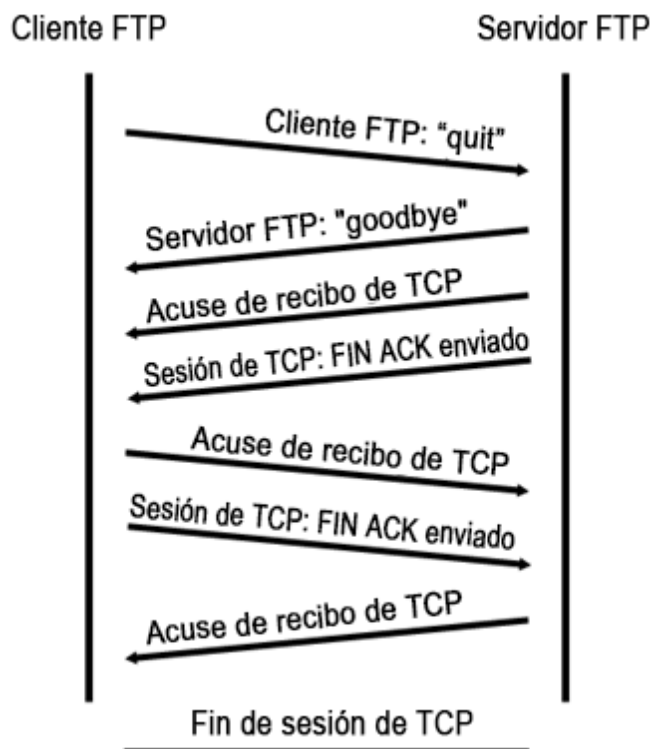
Uno. El primer paquete que envió el host al principio de una sesión TCP.

Una vez establecida una sesión TCP, puede haber tráfico FTP entre la PC y el servidor FTP. El cliente y el servidor FTP se comunican entre sí sin saber que TCP tiene el control y manejo de la sesión. Cuando el servidor FTP envía una Response: 220 (Respuesta: 220) al cliente FTP, la sesión TCP en el cliente FTP envía un acuse de recibo a la sesión TCP en el servidor. Esta secuencia se puede ver en la captura de Wireshark, a continuación.

9	1.314568000	198.246.112.54	192.168.1.17	FTP	81	Response: 220 Microsoft FTP Service
10	1.523372000	192.168.1.17	198.246.112.54	TCP	54	49243 > ftp [ACK] Seq=1 Ack=28 win=
12	4.585185000	192.168.1.17	198.246.112.54	FTP	70	Request: USER anonymous
13	4.675040000	198.246.112.54	192.168.1.17	FTP	126	Response: 331 Anonymous access allc

Frame 9: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: HonHaiPr_be:15:63 (90:4c:e5:be:15:63)
Internet Protocol Version 4, Src: 198.246.112.54 (198.246.112.54), Dst: 192.168.1.17 (192.168.1.17)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49243 (49243), Seq: 1, Ack: 1, Len: 27
File Transfer Protocol (FTP)
220 Microsoft FTP Service\r\n
Response code: Service ready for new user (220)
Response arg: Microsoft FTP Service

Cuando la sesión FTP terminó, el cliente FTP envía un comando para “salir”. El servidor FTP acusa recibo de la terminación FTP con una Response: 221 Goodbye (Respuesta: 221. Adiós). En este momento, la sesión TCP del servidor FTP envía un datagrama TCP al cliente FTP, en el que se anuncia la terminación de la sesión TCP. La sesión TCP del cliente FTP acusa recibo de la recepción del datagrama de terminación y luego envía su propia terminación de sesión TCP. Cuando quien originó la terminación TCP (servidor FTP) recibe una terminación duplicada, se envía un datagrama ACK para acusar recibo de la terminación y se cierra la sesión TCP. Esta secuencia se puede ver en el diagrama y la captura que se muestran a continuación.



Si se aplica un filtro **ftp**, puede examinarse la secuencia completa del tráfico FTP en Wireshark. Observe la secuencia de eventos durante esta sesión FTP. Para recuperar el archivo Léame, se utilizó el nombre de usuario anónimo. Una vez que se completó la transferencia de archivos, el usuario finalizó la sesión FTP.

No.	Time	Source	Destination	Protocol	Length	Info
9	1.314568000	198.246.112.54	192.168.1.17	FTP	81	Response: 220 Microsoft FTP Service
12	4.585185000	192.168.1.17	198.246.112.54	FTP	70	Request: USER anonymous
13	4.675040000	198.246.112.54	192.168.1.17	FTP	126	Response: 331 Anonymous access allowe
19	5.961514000	192.168.1.17	198.246.112.54	FTP	61	Request: PASS
20	6.048929000	198.246.112.54	192.168.1.17	FTP	85	Response: 230 Anonymous user logged i
25	8.855225000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,92
26	8.945530000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successfu
27	8.955549000	192.168.1.17	198.246.112.54	FTP	60	Request: NLST
29	9.053034000	198.246.112.54	192.168.1.17	FTP	109	Response: 150 opening ASCII mode data
39	9.347432000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
42	12.621720000	192.168.1.17	198.246.112.54	FTP	80	Request: PORT 192,168,1,17,192,93
43	12.709658000	198.246.112.54	192.168.1.17	FTP	84	Response: 200 PORT command successfu
44	12.722592000	192.168.1.17	198.246.112.54	FTP	67	Request: RETR Readme
45	12.811097000	198.246.112.54	192.168.1.17	FTP	118	Response: 150 opening ASCII mode data
58	13.107294000	198.246.112.54	192.168.1.17	FTP	78	Response: 226 Transfer complete.
61	15.514815000	192.168.1.17	198.246.112.54	FTP	60	Request: QUIT
62	15.601920000	198.246.112.54	192.168.1.17	FTP	61	Response: 221

Vuelva a aplicar el filtro TCP en Wireshark para examinar la terminación de la sesión TCP. Se transmiten cuatro paquetes para la terminación de la sesión TCP. Dado que la conexión TCP es full-duplex, cada dirección debe terminar independientemente. Examine las direcciones de origen y destino.

En este ejemplo, el servidor FTP no tiene más datos para enviar en el stream; envía un segmento con el conjunto de indicadores FIN en la trama 63. La PC envía un ACK para acusar recibo del FIN para terminar la sesión del servidor al cliente en la trama 64.

En la trama 65, la PC envía un FIN al servidor FTP para terminar la sesión TCP. El servidor FTP responde con un ACK para acusar recibo del FIN de la PC en la trama 67. Ahora, la sesión TCP terminó entre el servidor FTP y la PC.

61	15.514815000	192.168.1.17	198.246.112.54	FTP	60 Request: QUIT
62	15.601920000	198.246.112.54	192.168.1.17	FTP	61 Response: 221
63	15.602245000	198.246.112.54	192.168.1.17	TCP	54 ftp > 49243 [FIN, ACK] Seq=365 Ack=
64	15.602314000	192.168.1.17	198.246.112.54	TCP	54 49243 > ftp [ACK] Seq=101 Ack=366 v
65	15.605832000	192.168.1.17	198.246.112.54	TCP	54 49243 > ftp [FIN, ACK] Seq=101 Ack=
67	15.696497000	198.246.112.54	192.168.1.17	TCP	54 ftp > 49243 [ACK] Seq=366 Ack=102 v

+	Frame 63: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
+	Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: HonHaiPr_be:15:63 (90:4c:e5:be:15:63)
+	Internet Protocol Version 4, Src: 198.246.112.54 (198.246.112.54), Dst: 192.168.1.17 (192.168.1.17)
+	Transmission Control Protocol, Src Port: ftp (21), Dst Port: 49243 (49243), Seq: 365, Ack: 101, Len

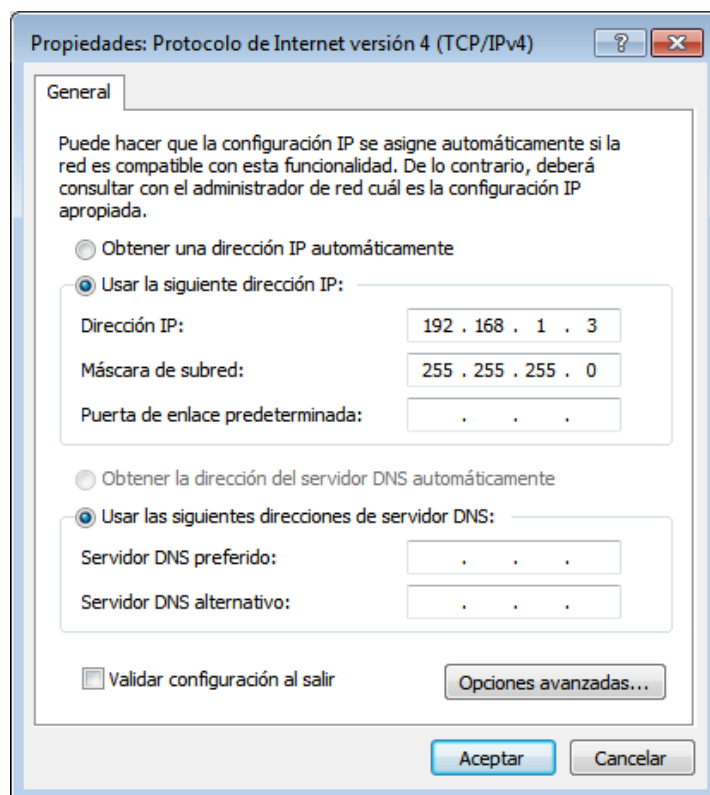
Parte 2: Identificar campos de encabezado y operación UDP mediante una captura de sesión TFTP de Wireshark

En la parte 2, se utiliza Wireshark para capturar una sesión TFTP e inspeccionar los campos de encabezado UDP.

Paso 1: Configurar esta topología física y prepararse para la captura de TFTP



- Establezca una consola y una conexión Ethernet entre la PC-A y el switch S1.
- Si aún no lo hizo, configure manualmente la dirección IP de la PC en 192.168.1.3. No se requiere configurar el gateway predeterminado.



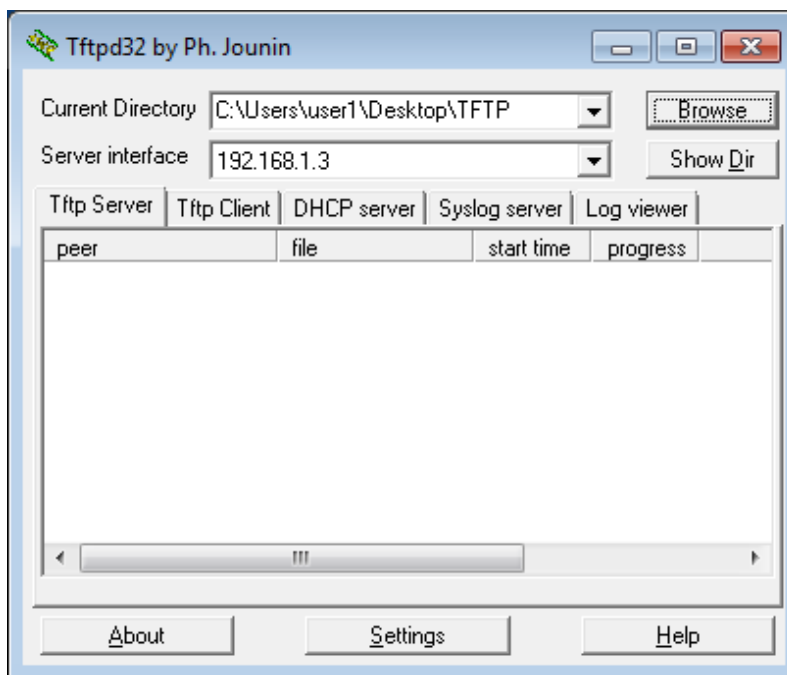
- c. Configure el switch. Asigne la dirección IP 192.168.1.1 a VLAN 1. Verifique la conectividad con la PC haciendo ping a 192.168.1.3. Resuelva cualquier problema que se presente.

```
Switch> enable
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# host S1
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shut
*Mar 1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar 1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

Paso 2: Preparar el servidor TFTP en la PC

- Si aún no existe, cree una carpeta en el escritorio de la PC con el nombre **TFTP**. Los archivos del switch se copiarán a esta ubicación.
- Inicie **tftpd32** en la PC.
- Haga clic en **Browse** (Buscar), cambie el directorio actual por **C:\Usuarios\usuario1\Escritorio\TFTP** y reemplace usuario1 con su nombre de usuario.

El servidor TFTP debería verse así:



Observe que, en Current Directory (Directorio actual), se indica la interfaz de usuario y servidor (PC-A) como la dirección IP **192.168.1.3**.

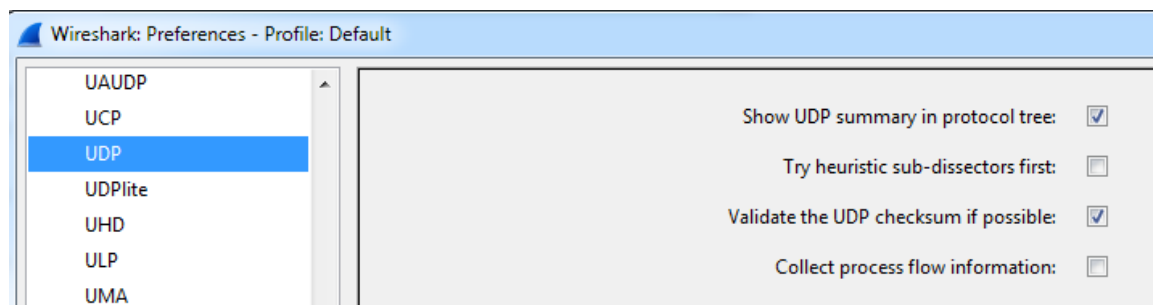
- d. Pruebe la capacidad de copiar un archivo del switch a la PC con TFTP. Resuelva cualquier problema que se presente.

```
S1# copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [s1-config]?
!!
1638 bytes copied in 0.026 secs (63000 bytes/sec)
```

Si ve que el archivo se copió (como en el resultado de arriba), entonces está listo para avanzar al siguiente paso. De lo contrario, resuelva el problema. Si recibe el mensaje de error `%Error opening tftp (Permission denied)` (Error al abrir tftp [permiso denegado]), primero asegúrese de que el firewall no esté bloqueando el TFTP y de que esté copiando a una ubicación donde su nombre de usuario tiene el permiso adecuado, como el escritorio.

Paso 3: Capturar una sesión TFTP en Wireshark

- a. Abra Wireshark. En el menú **Edit** (Editar), seleccione **Preferences** (Preferencias) y haga clic en el signo más (+) para expandir **Protocols** (Protocolos). Desplácese hacia abajo y seleccione **UDP**. Haga clic en la casilla de verificación **Validate the UDP checksum if possible** (Validar checksum UDP si es posible) y luego en **Apply** (Aplicar). A continuación, haga clic en **OK** (Aceptar).



Nota para el instructor: esto es un cambio de las versiones anteriores de esta práctica de laboratorio, porque la tecnología cambió. Busque “checksum offloading in Wireshark” (Descarga de checksum en Wireshark).

- b. Inicie una captura de Wireshark.
- c. Ejecute el comando `copy start tftp` en el switch.
- d. Detener la captura de Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
12	9.75564700	192.168.1.1	192.168.1.3	TFTP	60	Write Request, File: s1-config, Transfer type: octet
13	9.75668700	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 0
14	9.75794800	192.168.1.1	192.168.1.3	TFTP	558	Data Packet, Block: 1
15	9.75804400	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 1
16	9.75905100	192.168.1.1	192.168.1.3	TFTP	558	Data Packet, Block: 2
17	9.75911700	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 2
18	9.76013200	192.168.1.1	192.168.1.3	TFTP	558	Data Packet, Block: 3
19	9.76018700	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 3
20	9.76227300	192.168.1.1	192.168.1.3	TFTP	148	Data Packet, Block: 4 (last)
21	9.76240000	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 4

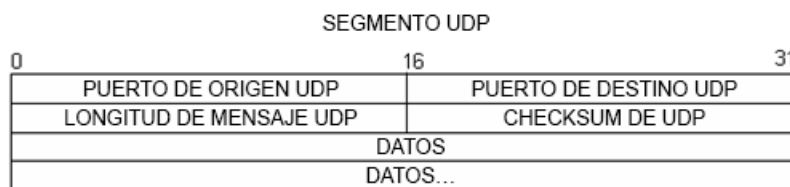
- e. Defina el filtro en **tftp**. El resultado debe ser similar al que se muestra más arriba. Esta transferencia TFTP se utiliza para analizar el funcionamiento de la capa de transporte UDP.

Nota para el instructor: si los estudiantes indican los acuses de recibo UDP, explique que el encabezado UDP no contiene un campo de acuse de recibo. En cambio, es responsabilidad del protocolo de capa superior, en este caso el TFTP, administrar la transferencia de datos y recibir la información. Esto se mostrará durante el examen del datagrama UDP.

En Wireshark, se encuentra disponible información detallada sobre UDP en el panel de detalles del paquete. Resalte el primer datagrama UDP del equipo host y mueva el puntero del mouse hacia el panel de detalles del paquete. Puede ser necesario ajustar el panel de detalles del paquete y expandir el registro UDP con un clic en la casilla de expansión de protocolo. El datagrama UDP expandido debe ser similar al diagrama siguiente.

Encabezado UDP	⊖ User Datagram Protocol, Src Port: 62513 (62513), Dst Port: tftp (69) - Source port: 62513 (62513) - Destination port: tftp (69) - Length: 25 ⊖ Checksum: 0x482c [correct]
UDP Data	⊖ Trivial File Transfer Protocol [DESTINATION File: s1-config] - Opcode: Write Request (2) - DESTINATION File: s1-config - Type: octet

En la siguiente ilustración, se muestra un diagrama de datagrama UDP. La información del encabezado está dispersa comparada con la del datagrama TCP. Al igual que TCP, cada datagrama UDP está identificado con el puerto de origen UDP y el puerto de destino UDP.



Utilice la captura Wireshark del primer datagrama UDP para completar la información acerca del encabezado UDP. El valor de la checksum es un valor hexadecimal (base 16) indicado por el código anterior 0x:

Dirección IP de origen:	192.168.1.1
Dirección IP de destino:	192.168.1.3
Número de puerto de origen:	62513*
Número de puerto de destino:	69
Longitud de mensaje UDP:	25 bytes*
Checksum de UDP:	0x482c [correcto]*

*La respuesta de los estudiantes variará.

¿Cómo verifica UDP la integridad del datagrama?

Se envía un valor de checksum en el datagrama UDP, y el valor de checksum del datagrama se vuelve a calcular al recibirlo. Si el valor de checksum calculado es idéntico al valor de checksum enviado, entonces se supone que el datagrama UDP está completo.

Examine la primera trama que devuelve el servidor tftpd. Complete la información sobre el encabezado UDP:

Dirección IP de origen:	192.168.1.3
Dirección IP de destino:	192.168.1.1
Número de puerto de origen:	58565*
Número de puerto de destino:	62513*
Longitud de mensaje UDP:	12 bytes*
Checksum de UDP:	Checksum: 0x8372 [incorrecto; debe ser 0xa385 (¿puede deberse a la "descarga de checksum UDP"?)]*

*La respuesta de los estudiantes variará.

- ▣ User Datagram Protocol, Src Port: 58565 (58565), Dst Port: 62513 (62513)
 - Source port: 58565 (58565)
 - Destination port: 62513 (62513)
 - Length: 12
- ▣ Checksum: 0x8372 [incorrect, should be 0xa385 (maybe caused by "UDP checksum offload"?)]
- ▣ Trivial File Transfer Protocol
 - [DESTINATION File: s1-config]
 - Opcode: Acknowledgement (4)
 - Block: 0

Observe que el datagrama UDP devuelto tiene un puerto de origen UDP diferente, pero este puerto de origen es utilizado para el resto de la transferencia TFTP. Dado que no hay una conexión confiable, para mantener la transferencia TFTP, se utiliza solo el puerto de origen que se empleó para iniciar la sesión TFTP.

También observe que el valor de checksum UDP es incorrecto. Lo más probable es que se deba a la descarga de checksum UDP. Para obtener más información acerca del motivo por el cual sucede esto, realice una búsqueda de "UDP checksum offload".

Reflexión

Esta práctica de laboratorio brindó a los estudiantes la oportunidad de analizar las operaciones de los protocolos UDP y TCP de las sesiones TFTP y FTP capturadas. ¿De qué manera TCP administra la comunicación distinto de como lo hace UDP?

TCP administra la comunicación de manera muy diferente que UDP, porque la confiabilidad y la entrega garantizada requieren mayor control sobre el canal de comunicación. UDP tiene menos sobrecarga y control, y el protocolo de capa superior debe proveer algún tipo de control de acuse de recibo. Sin embargo, ambos protocolos transportan datos entre clientes y servidores con el uso de los protocolos de la capa de Aplicación y son correctos para el protocolo de capa superior que cada uno admite.

Desafío

Debido a que ni FTP ni TFTP son protocolos seguros, todos los datos transferidos se envían en texto no cifrado. Esto incluye cualquier ID de usuario, contraseñas o contenido de archivo en texto no cifrado. Si analiza la sesión FTP de capa superior, identificará rápidamente la ID de usuario, la contraseña y las contraseñas de archivos de configuración. El examen de datos TFTP de capa superior es un poco más complicado, pero se puede examinar el campo de datos y extraer información sobre la ID de usuario de configuración y la contraseña.

Limpieza

Salvo que el instructor indique lo contrario:

- 1) Elimine los archivos que se copiaron a su PC.
- 2) Borre las configuraciones del switch **S1**.
- 3) Elimine la dirección IP manual de la PC y restaure la conectividad a Internet.

Configuraciones de dispositivos

Switch S1

```
S1#show run
Building configuration...

!
hostname S1
!
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
!
end
```

Tenemos que hablar nuevamente (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que los protocolos y servicios de capa de transporte admiten comunicaciones a través de las redes de datos.

- Dada una situación, los estudiantes determinarán si se debe utilizar la mensajería de alta confiabilidad. Se centrarán en si el último mensaje estaba completo, era correcto y se entregó de manera oportuna.

Información básica/Situación

(Nota: es importante que los estudiantes hayan completado la actividad de creación de modelos [MA] introductoria de este capítulo. Conviene realizar esta actividad en grupos medianos de seis a ocho estudiantes).

El instructor susurrará un mensaje complejo al primer estudiante de un grupo. Por ejemplo, el mensaje puede ser: “Se espera una tormenta de nieve mañana. Se espera que suceda por la mañana, por lo que el horario de clases se retrasará dos horas. Por lo tanto, traigan la tarea”.

Ese estudiante le susurrará el mensaje al siguiente estudiante del grupo. Todos los grupos siguen este proceso hasta que todos los miembros de cada grupo hayan oído el mensaje susurrado. Las reglas que debe seguir son las siguientes:

Las reglas que debe seguir son las siguientes:

- Puede susurrarle el mensaje al compañero junto a usted por partes Y TAMBIÉN puede repetir las partes del mensaje después de verificar que ese compañero escuchó el mensaje correctamente.
- Se pueden verificar y repetir partes del mensaje (hacia la derecha O hacia la izquierda para asegurar la precisión de las partes del mensaje) en susurros. A un estudiante se le asignará la tarea de medir el tiempo total de la actividad.
- Cuando se haya transmitido el mensaje a todo el grupo, el último estudiante que escuchó el mensaje lo dirá en voz alta. Las pequeñas partes del mensaje se pueden repetir (es decir, se pueden reenviar) y el proceso se puede volver a iniciar para asegurarse de que TODAS las partes del mensaje se hayan entregado en forma completa y correcta.
- El instructor repetirá el mensaje original para comprobar que el mensaje se haya entregado correctamente.

Nota para el instructor: inicie un debate acerca de lo que sucedió en la actividad. Céntrese en estas tres preguntas:

1. ¿El mensaje estaba completo cuando llegó al último estudiante?
2. ¿El mensaje era correcto cuando se transmitió a la última persona?
3. ¿El mensaje tardó mucho en llegar al último estudiante?

Si dependiera de este mensaje para organizar su agenda personal o empresarial, programa de estudio, etc., ¿el contenido de este mensaje debería ser totalmente claro y correcto en el momento de recibirlo?

¿El tiempo que lleva entregar el mensaje sería importante para el emisor y el destinatario?

Compare la MA introductoria de este capítulo con la MA de revisión (esta actividad). ¿Qué diferencias advierte con respecto a la entrega de los mensajes?

Recuerde a los estudiantes que los protocolos TCP e UDP aseguran que:

- Las comunicaciones de red con niveles diferentes de importancia se envían o se reciben según su nivel de importancia.
- El tipo de datos determina si se utiliza el método de entrega TCP o UDP.
- El tiempo en el cual el mensaje debe entregarse influye en si TCP o UDP se usan como método de entrega.

Reflexión

1. ¿El contenido de este mensaje debería ser totalmente claro y correcto en el momento de recibirlo si dependiera de él para organizar su agenda personal o empresarial, programa de estudio, etc.?

Importancia de entregar mensajes completos del emisor al destinatario: TCP asegura la entrega completa.

2. ¿El tiempo que lleva entregar el mensaje sería un factor importante para el emisor y el destinatario?

Importancia de la **temporización**: la temporización es relevante para los detalles del mensaje y la fecha y la hora necesarias para tomar medidas con respecto a este; es importante para todas las facetas de la transmisión de datos. El control del flujo mediante mecanismo ventana y el desplazamiento de ventanas se ocupan de esto en TCP; no así en UDP.

3. Compare el MA introductorio de este capítulo con esta actividad. ¿Qué diferencias advierte con respecto a la entrega de los mensajes?

Las respuestas representativas (para el debate) pueden ser similares a las siguientes:

El mensaje demoró mucho más en llegar desde quien lo originó hasta el último destinatario.

- La mayor parte del mensaje (si no todo) llegó, y el contenido fue probablemente mejor (si es que no fue completamente exacto).

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- El establecimiento de un método para transmitir información a través de una red es importante para obtener la entrega completa de los datos de red (el TCP está garantizado, pero el UDP no).
- El aseguramiento de la calidad de la entrega de datos a través de una red se ve afectado por el tipo de transporte que se utiliza. TCP verificará que no haya errores de checksum, acusará recibo y sincronizará cada segmento. Por el contrario, UDP no cuenta con un mecanismo de corrección de errores.
- La selección de TCP o UDP según un factor de tiempo para la entrega de datos a través de un sistema de comunicaciones. Si se detecta congestión en la red, las ventanas se configuran y ajustan en TCP; en tanto que UDP continúa la transmisión.
- Si bien no es confiable, UDP tiene su valor: el mensaje en la primera actividad se desarrolló mucho más rápido que en la segunda. Si el mensaje fuera más simple (por ejemplo, un mensaje que conste de un solo dígito), el primer método de transporte (UDP) podría ser mucho mejor que el segundo (TCP).

Internet de todo (IdT) (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que los dispositivos de red utilizan tablas de enrutamiento para dirigir los paquetes a una red de destino.

IPv6 es importante para ayudar a administrar la identificación del tráfico de datos, que será necesaria en el futuro. Muchas direcciones ayudan en este esfuerzo, e IPv6 permite aliviar esta necesidad.

Información básica/Situación

En la actualidad, más del 99% del mundo está desconectado. En el futuro, estaremos conectados a casi todo. Para 2020, unos 37 000 millones de dispositivos estarán conectados a Internet. Desde los árboles hasta el agua y los vehículos, todo lo orgánico y lo digital trabajarán en conjunto para lograr un mundo más inteligente y conectado. Este futuro de las redes se conoce como “Internet de todo”, o “IdT”.

Si el tráfico, el transporte, las redes y la exploración espacial dependen del intercambio de información digital, ¿de qué forma se identifica dicha información de origen a destino?

En esta actividad, comenzará a pensar no solo en lo que se identificará en el mundo de IdT, sino también en cómo se direccionarán todos esos aspectos en ese mundo.

Instrucciones de la actividad para la clase y estudiantes individuales:

1. Lea el blog o la fuente de noticias “Internet of Everything: Fueling an Amazing Future #TomorrowStartsHere”, de John Chambers, con respecto a Internet de todos (IdT). Este blog se encuentra en <http://blogs.cisco.com/news/internet-of-everything-2>.
2. Luego, mire el video “Cisco Commercial: Tomorrow Starts Here” que se encuentra en la mitad de la página.
3. A continuación, navegue hasta la página principal de IdT, ubicada en <http://www.cisco.com/web/tomorrow-starts-here/index.html>. Haga clic en una categoría que le interese del collage gráfico.
4. Luego, vea el video o lea el blog o el archivo .pdf que pertenece a la categoría de IdT de su interés.
5. Escriba cinco preguntas o comentarios sobre lo que vio o leyó. Prepárese para compartirlo con la clase.

Nota para el instructor: esta es una actividad de creación de modelos (MA) para realizar en forma individual o en clase. No tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes para que reflexionen acerca de su percepción respecto de las redes y la forma en que se identificarán en el futuro. IPv6 es necesario para respaldar el concepto Internet de todo.

Recursos necesarios

- Conectividad a Internet para investigar en el sitio cisco.com. También puede ser útil contar con auriculares si los estudiantes se dividen en grupos, pero completan esta actividad en forma individual.
- Capacidades de registro (papel, tablet PC, etc.) para comentarios o preguntas con respecto a videos, blogs y archivos .pdf leídos o vistos en el paso 3.

Reflexión

1. ¿Por qué piensa que hay necesidad de ocuparse de los árboles? ¿Molinos de viento? ¿Automóviles? ¿Refrigeradores? ¿Por qué prácticamente cualquier cosa podrá utilizar una dirección IP?

La investigación de esta situación será variada. Entre los conceptos que cabe mencionar o analizar, se incluyen los siguientes:

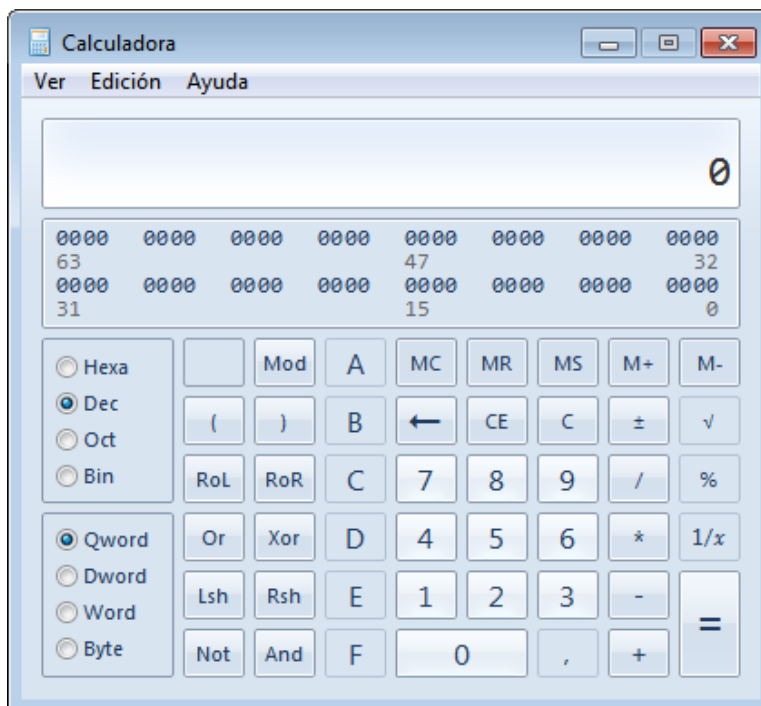
- Para admitir nuevos conceptos o implementaciones de IdT y el creciente número de dispositivos que se conectan a Internet, se necesitará una cantidad exponencial de direcciones. Quizá sea necesario analizar brevemente LA FORMA en que los árboles pueden conectarse a Internet (es decir, distintos tipos de sensores que transmiten datos; consulte http://www.ericsson.com/article/connected_tree_2045546582_c).
- Saber cómo utilizar el direccionamiento IPv6 será importante para los administradores de red, ISP y TSP, y el público en general, ya que evolucionamos a cada vez más tipos o clasificaciones de redes.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Tipos de red (subredes, etc.)
- Identificación de red y host en relación con tipos de red
- Calidad de las transmisiones de red en relación con la identificación de la red

Práctica de laboratorio: Uso de la calculadora de Windows con direcciones de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.



Objetivos

Parte 1: Acceder a la calculadora de Windows

Parte 2: Convertir entre sistemas de numeración

Parte 3: Convertir direcciones de host y máscaras de subred IPv4 al sistema binario

Parte 4: Determinar la cantidad de hosts en una red mediante potencias de 2

Parte 5: Convertir direcciones MAC y direcciones IPv6 al sistema binario

Información básica/Situación

Los técnicos de red usan números binarios, decimales y hexadecimales cuando trabajan con PC y dispositivos de red. Microsoft proporciona la aplicación Calculadora incorporada como parte del sistema operativo. La versión de Windows 7 de la calculadora incluye una vista estándar que se puede utilizar para realizar tareas básicas de aritmética, como suma, resta, multiplicación y división. La aplicación Calculadora también tiene capacidades avanzadas de programación, calculadora científica y estadística.

En esta práctica de laboratorio, utilizará la vista Programador de la aplicación Calculadora de Windows 7 para la conversión entre sistemas numéricos binarios, decimales y hexadecimales. También usará la función de potencia de la vista Científica para determinar la cantidad de hosts que se pueden asignar según la cantidad de bits disponibles.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP)

Nota: si se utiliza un sistema operativo distinto de Windows 7, las vistas de la aplicación Calculadora y las funciones disponibles pueden variar de las que se muestran en esta práctica de laboratorio. No obstante, debería poder realizar los cálculos.

Parte 1: Acceder a la calculadora de Windows.

En la parte 1, se familiarizará con la aplicación Calculadora incorporada de Microsoft Windows y verá los modos disponibles.

Paso 1: Haga clic en el botón Inicio de Windows y seleccione Todos los programas.

Paso 2: Haga clic en la carpeta Accesorios y seleccione Calculadora.

Paso 3: Una vez que se abra la calculadora, haga clic en el menú Ver.

¿Cuáles son los cuatro modos disponibles?

Estándar, Científica, Programador y Estadística

Nota: en esta práctica de laboratorio, se utilizan los modos Programador y Científica.

Parte 2: Convertir entre sistemas de numeración

En la vista Programador de la calculadora de Windows, se encuentran disponibles varios modos de sistemas de numeración: Hex (hexadecimal o de base 16), Dec (decimal o de base 10), Oct (octal o de base 8) y Bin (binario o de base 2).

Estamos acostumbrados a usar el sistema de numeración decimal que emplea los dígitos del 0 al 9. El sistema de numeración decimal se utiliza en la vida diaria para todas las transacciones contables, de dinero y financieras. Las PC y otros dispositivos electrónicos utilizan el sistema de numeración binario con los dígitos 0 y 1 únicamente para el almacenamiento de datos, la transmisión de datos y los cálculos numéricos. Todos los cálculos de las PC se realizan, en última instancia, internamente en forma binaria (digital), independientemente de cómo aparecen.

Una desventaja de los números binarios es que el equivalente en números binarios de un número decimal grande puede ser muy largo. Esto dificulta su lectura y escritura. Una manera de solucionar este problema es ordenar los números binarios en grupos de cuatro, como números hexadecimales. Los números hexadecimales son de base 16, y se usa una combinación de números del 0 al 9 y de letras de la A a la F para representar el equivalente binario o decimal. Los caracteres hexadecimales se utilizan cuando se escriben o se muestran direcciones IPv6 y MAC.

El sistema de numeración octal es muy similar en principio al hexadecimal. Los números octales representan números binarios en grupos de tres. Este sistema de numeración utiliza los dígitos del 0 al 7. Usar números octales también es una manera práctica de representar un número binario grande en grupos más pequeños, pero este sistema de numeración no es muy común.

En esta práctica de laboratorio, se utiliza la calculadora de Windows 7 para realizar conversiones entre distintos sistemas de numeración en el modo Programador.

a. Haga clic en el menú **Ver** y seleccione **Programador** para cambiar al modo de programador.

Nota: en Windows XP y Windows Vista, solo hay dos modos disponibles: Estándar y Científica. Si utiliza uno de estos sistemas operativos, puede utilizar el modo Científica para realizar esta práctica de laboratorio.

¿Qué sistema numérico está activo? _____ Dec (Decimal).

¿Qué números del teclado numérico están activos en el modo decimal? _____ Del 0 al 9

- b. Haga clic en el botón de opción **Bin** (Binario). ¿Qué números están activos ahora en el teclado numérico?

0 y 1

¿Por qué considera que los otros números se muestran en color gris?

Porque los únicos dígitos que se utilizan en el sistema binario (de base 2) son 0 y 1.

- c. Haga clic en el botón de opción **Hex** (Hexadecimal). ¿Qué caracteres están activos ahora en el teclado numérico?

Del 0 al 9 y A, B, C, D, E y F. El sistema hexadecimal (de base 16) tiene 16 valores posibles.

- d. Haga clic en el botón de opción **Dec** (Decimal). Con el mouse, haga clic en el número **1** y luego en el número **5** del teclado numérico. Se introdujo el número decimal 15.

Nota: también se pueden usar los números y las letras del teclado para introducir los valores. Si utiliza el teclado numérico, escriba el número **15**. Si el número no se introduce en la calculadora, presione la tecla **Bloq Num** para habilitar el teclado numérico.

Haga clic en el botón de opción **Bin** (Binario). ¿Qué sucedió con el número 15?

Se convirtió en el número binario 1111. Este número binario 1111 representa el número decimal 15.

- e. Los números se convierten de un sistema de numeración a otro al seleccionar el modo de numeración deseado. Vuelva a hacer clic en el botón de opción **Dec**. El número vuelve a convertirse a decimal.
- f. Haga clic en el botón de opción **Hex** para cambiar al modo hexadecimal. ¿Qué carácter hexadecimal (del 0 al 9 o de la A a la F) representa el 15 decimal? **F**
- g. Al cambiar entre los sistemas de numeración, es posible que haya observado que el número binario 1111 se mostraba durante la conversión. Esto lo ayuda a relacionar los dígitos binarios con otros valores del sistema de numeración. Cada conjunto de 4 bits representa un carácter hexadecimal o varios caracteres decimales potencialmente.

15							
0000	0000	0000	0000	0000	0000	0000	0000
63				47			32
0000	0000	0000	0000	0000	0000	0000	1111
31				15			0

- h. Haga clic en la **C** que está encima del número 9 en el teclado de la calculadora para borrar los valores de la ventana. Convierta los siguientes números entre los sistemas de numeración binario, decimal y hexadecimal.

Decimal	Binario	Hexadecimal
86	0101 0110	56
175	1010 1111	AF
204	1100 1100	CC
19	0001 0011	13
77	0100 1101	4D
42	0010 1010	2A
56	0011 1000	38
147	1001 0011	93
228	1110 0100	E4

- i. A medida que registra los valores en la tabla anterior, ¿observa un patrón entre los números binarios y hexadecimales?

Cada dígito hexadecimal se puede convertir a cuatro números binarios por separado. Por ejemplo, el hexadecimal 0A es 1010 en el sistema binario.

Parte 3: Convertir direcciones de host y máscaras de subred IPv4 al sistema binario

Las direcciones del protocolo de Internet versión 4 (IPv4) y las máscaras de subred se representan en un formato decimal punteado (cuatro octetos), por ejemplo, 192.168.1.10 y 255.255.255.0, respectivamente. Esto permite que estas direcciones sean más fáciles de leer para los usuarios. Cada uno de los octetos decimales de la dirección o de una máscara se puede convertir en 8 bits binarios. Un octeto equivale siempre a 8 bits binarios. Si los 4 octetos se convirtieran al sistema binario, ¿cuántos bits habría?

32

- a. Utilice la aplicación Calculadora de Windows para convertir la dirección IP 192.168.1.10 a número binario y registre los números binarios en la tabla siguiente:

Decimal	Binario
192	1100 0000
168	1010 1000
1	0000 0001
10	0000 1010

- b. Las máscaras de subred, como 255.255.255.0, también están representadas en formato decimal punteado. Una máscara de subred siempre consta de cuatro octetos de 8 bits, cada uno representado como un número decimal. Con la calculadora de Windows, convierta los 8 valores posibles de octetos de la máscara de subred decimal a números binarios y registre dichos números en la tabla siguiente:

Decimal	Binario
0	0000 0000
128	1000 0000
192	1100 0000
224	1110 0000
240	1111 0000
248	1111 1000
252	1111 1100
254	1111 1110
255	1111 1111

- c. Con la combinación de la dirección IPv4 y la máscara de subred, se puede determinar la porción de red y también se puede calcular la cantidad de hosts disponibles en una subred IPv4 determinada. El proceso se examina en la parte 4.

Parte 4: Determinar la cantidad de hosts en una red mediante potencias de 2

Dada una dirección de red IPv4 y una máscara de subred, se puede determinar la porción de red junto con la cantidad de hosts disponibles en la red.

- a. Para calcular la cantidad de hosts en una red, debe determinar la porción de red y de host de la dirección.

Si se aplica el ejemplo de 192.168.1.10 con una subred 255.255.248.0, la dirección y la máscara de subred se convierten a números binarios. Alinee los bits a medida que registra las conversiones a números binarios.

Dirección IP y máscara de subred decimales	Dirección IP y máscara de subred binarias
192.168.1.10	11000000.10101000.00000001.00001010
255.255.248.0	11111111.11111111.11111000.00000000

Dado que los primeros 21 bits en la máscara de subred son números 1 consecutivos, los primeros 21 bits correspondientes en la dirección IP en sistema binario son 11000000101010000000, que representan la porción de red de la dirección. Los 11 bits restantes son 00100001010 y representan la porción de host de la dirección.

¿Cuál es el número de red decimal y binario para esta dirección?

Decimal: 192.168.0.0 Binario: 11000000.10101000.00000000.00000000

¿Cuál es la porción de host decimal y binaria para esta dirección?

Decimal: 1.10 Binaria: 00000000.00000000.00000001.00001010

Dado que el número de red y la dirección de broadcast utilizan dos direcciones fuera de la subred, la fórmula para determinar la cantidad de hosts disponibles en una subred IPv4 es el número 2 elevado a la cantidad de bits de hosts disponibles, menos 2:

$$\text{Cantidad de hosts disponibles} = 2^{(\text{cantidad de bits de hosts})} - 2$$

- Con la aplicación Calculadora de Windows, cambie al modo Científica; para eso, haga clic en el menú **Ver** y, a continuación, seleccione **Científica**.
- Introduzca **2**. Haga clic en la tecla **x^y**. Esta tecla eleva un número a una potencia.
- Introduzca **11**. Haga clic en **=** o presione Entrar en el teclado para obtener la respuesta.
- Utilice la calculadora, si lo desea, para restar **2** a la respuesta.
- En este ejemplo, hay 2046 hosts disponibles en esta red ($2^{11} - 2$).
- Dada la cantidad de bits de hosts, determine la cantidad de hosts disponibles y registre el número en la tabla siguiente.

Cantidad de bits de host disponibles	Cantidad de hosts disponibles
5	30
14	16382
24	16777214
10	1022

- Para una máscara de subred dada, determine la cantidad de hosts disponibles y registre la respuesta en la tabla siguiente.

Máscara de subred	Máscara de subred binaria	Cantidad de bits de host disponibles	Cantidad de hosts disponibles
255.255.255.0	11111111.11111111.11111111.00000000	8	254
255.255.240.0	11111111.11111111.11110000.00000000	12	4094
255.255.255.128	11111111.11111111.11111111.10000000	7	126
255.255.255.252	11111111.11111111.11111111.11111100	2	2
255.255.0.0	11111111.11111111.00000000.00000000	16	65534

Parte 5: Convertir direcciones MAC y direcciones IPv6 al sistema binario

Tanto las direcciones de control de acceso al medio (MAC) y del protocolo de Internet versión 6 (IPv6) se representan como dígitos hexadecimales para facilitar la lectura. Sin embargo, las PC solo comprenden los dígitos binarios y los utilizan para los cálculos. En esta parte, convertirá estas direcciones hexadecimales a direcciones binarias.

Paso 1: Convertir direcciones MAC a dígitos binarios

- La dirección MAC o física normalmente se representa como 12 caracteres hexadecimales, agrupados en pares y separados por guiones (-). Las direcciones físicas en un equipo Windows se muestran en un formato xx-xx-xx-xx-xx-xx, donde cada x es un número del 0 al 9 o una letra de la A a la F. Cada uno de los caracteres hexadecimales en la dirección puede convertirse en 4 bits binarios, que es lo que la PC comprende. Si los 12 caracteres hexadecimales se convirtieran al sistema binario, ¿cuántos bits habría?

La dirección MAC es 48 bits, 12 caracteres hexadecimales y 4 bits por carácter.

- b. Registre la dirección MAC de la PC.

Las respuestas varían según la PC. Ejemplo: CC-12-DE-4A-BD-88

- c. Convierta la dirección MAC a dígitos binarios mediante la aplicación Calculadora de Windows.

Las respuestas varían. Por ejemplo: CC (11001100), 12 (0001 0010), DE (1101 1110) 4A (0100 1010), BD (1011 1101), 88 (1000 1000)

Paso 2: Convertir una dirección IPv6 a dígitos binarios

Las direcciones IPv6 también se escriben en caracteres hexadecimales por cuestiones de practicidad. Estas direcciones IPv6 pueden convertirse a números binarios para el uso de la PC.

- a. Las direcciones IPv6 son números binarios representados en notaciones legibles para los usuarios: 2001:0DB8:ACAD:0001:0000:0000:0000:0001 o en un formato más corto: 2001:DB8:ACAD:1::1.
- b. Las direcciones IPv6 tienen una longitud de 128 bits. Utilice la aplicación Calculadora de Windows para convertir la dirección IPv6 del ejemplo a números binarios y regístrela en la tabla siguiente.

Hexadecimal	Binario
2001	0010 0000 0000 0001
0DB8	0000 1101 1011 1000
ACAD	1010 1100 1010 1101
0001	0000 0000 0000 0001
0000	0000 0000 0000 0000
0000	0000 0000 0000 0000
0000	0000 0000 0000 0000
0001	0000 0000 0000 0001

Reflexión

1. ¿Puede realizar todas las conversiones sin la ayuda de la calculadora? ¿Qué puede hacer para lograrlo?

Practicar mucho. Por ejemplo, un juego binario que se encuentra en Cisco Learning Network, en <https://learningnetwork.cisco.com/>, puede ayudarlo con la conversión entre sistemas de numeración binarios y decimales.

2. Para la mayoría de las direcciones IPv6, la porción de red de la dirección suele ser de 64 bits. ¿Cuántos hosts están disponibles en una subred donde los primeros 64 bits representan la red? Sugerencia: todas las direcciones host están disponibles en la subred para los hosts.

Se dejan 64 bits para las direcciones de host, que son más de 18,4 billones ($2^{64} - 2$) de hosts disponibles en una subred de 64 bits (/64).

Práctica de laboratorio: Conversión de direcciones IPv4 al sistema binario (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Convertir direcciones IPv4 de formato decimal punteado a binario

Parte 2: Utilizar la operación AND bit a bit para determinar las direcciones de red

Parte 3: Aplicar los cálculos de direcciones de red

Información básica/Situación

Cada dirección IPv4 consta de dos partes: una porción de red y una porción de host. La porción de red de una dirección es la misma para todos los dispositivos que residen en la misma red. La porción de host identifica un host específico dentro de una red determinada. La máscara de subred se utiliza para determinar la porción de red de una dirección IP. Los dispositivos en la misma red pueden comunicarse directamente; los dispositivos en redes diferentes requieren un dispositivo intermediario de capa 3, como un router, para comunicarse.

Para comprender el funcionamiento de los dispositivos en una red, debemos ver las direcciones de la manera en que lo hacen los dispositivos: en notación binaria. Para ello, debemos convertir el formato decimal punteado de una dirección IP y la máscara de subred a notación binaria. Después de hacerlo, podremos usar la operación AND bit a bit para determinar la dirección de red.

En esta práctica de laboratorio, se proporcionan instrucciones acerca de cómo determinar la porción de red y la porción de host de direcciones IP convirtiendo las direcciones y las máscaras de subred de la forma decimal punteada a la forma binaria y luego utilizando la operación AND bit a bit. Luego aplicará esta información para identificar las direcciones en la red.

Parte 1: Convertir direcciones IPv4 de formato decimal punteado a binaria

En la parte 1, convertirá números decimales a su equivalente binario. Después de dominar esta actividad, convertirá direcciones IPv4 y máscaras de subred del formato decimal punteado al formato binario.

Paso 1: Convertir números decimales a su equivalente binario

Complete la tabla siguiente convirtiendo el número decimal a un número binario de 8 bits. El primer número se completó a modo de referencia. Recuerde que los ocho valores de bits binarios en un octeto están basados en las potencias de 2 y, de izquierda a derecha, son 128, 64, 32, 16, 8, 4, 2 y 1.

Decimal	Binario
192	11000000
168	10101000
10	00001010
255	11111111
2	00000010

Paso 2: Convertir las direcciones IPv4 a su equivalente binario

Una dirección IPv4 se puede convertir utilizando la misma técnica que se usó anteriormente. Complete la tabla siguiente con el equivalente binario de las direcciones proporcionadas. Para que las respuestas sean más fáciles de leer, separe los octetos binarios con un punto.

Decimal	Binario
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	11010001.10100101.11001000.11100101
172.16.18.183	10101100.00010000.00010010.10110111
10.86.252.17	00001010.01010110.11111100.00010001
255.255.255.128	11111111.11111111.11111111.10000000
255.255.192.0	11111111.11111111.11000000.00000000

Parte 2: Utilizar la operación AND bit a bit para determinar las direcciones de red

En la parte 2, utilizará la operación AND bit a bit para calcular la dirección de red para las direcciones de host proporcionadas. Primero, deberá convertir una dirección decimal IPv4 y una máscara de subred a su equivalente binario. Una vez que tenga la forma binaria de la dirección de red, conviértala a su forma decimal.

Nota: el proceso de aplicación de AND compara el valor binario en cada posición de bit de la dirección IP del host de 32 bits con la posición correspondiente en la máscara de subred de 32 bits. Si hay dos 0 o un 0 y un 1, el resultado de la aplicación de AND es 0. Si hay dos 1, el resultado es un 1, como se muestra en el ejemplo siguiente.

Paso 1: Determinar la cantidad de bits que se utilizarán para calcular la dirección de red

Descripción	Decimal	Binario
Dirección IP	192.168.10.131	11000000.10101000.00001010.10000011
Máscara de subred	255.255.255.192	11111111.11111111.11111111.11000000
Dirección de red	192.168.10.128	11000000.10101000.00001010.10000000

¿Cómo se determina qué bits deben utilizarse para calcular la dirección de red?

Los bits que se utilizan para calcular la dirección de red son los que se establecen en 1 en la máscara de subred binaria.

En el ejemplo anterior, ¿cuántos bits se utilizan para calcular la dirección de red?

_____ 26 bits.

Paso 2: Utilizar la operación AND para determinar la dirección de red

- a. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	172.16.145.29	10101100.00010000.10010001.00011101
Máscara de subred	255.255.0.0	11111111.11111111.00000000.00000000
Dirección de red	172.16.0.0	10101100.00010000.00000000.00000000

- b. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	192.168.10.10	11000000.10101000.00001010.00001010
Máscara de subred	255.255.255.0	11111111.11111111.11111111.00000000
Dirección de red	192.168.10.0	11000000.10101000.00001010.00000000

- c. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	192.168.68.210	11000000.10101000.01000100.11010010
Máscara de subred	255.255.255.128	11111111.11111111.11111111.10000000
Dirección de red	192.168.68.128	11000000.10101000.01000100.10000000

- d. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	172.16.188.15	10101100.00010000.10111100.00001111
Máscara de subred	255.255.240.0	11111111.11111111.11110000.00000000
Dirección de red	172.16.176.0	10101100.00010000.10110000.00000000

- e. Introduzca la información que falta en la siguiente tabla:

Descripción	Decimal	Binario
Dirección IP	10.172.2.8	00001010.10101100.00000010.00001000
Máscara de subred	255.224.0.0	11111111.11100000.00000000.00000000
Dirección de red	10.160.0.0	00001010.10100000.00000000.00000000

Parte 3: Aplicar los cálculos de direcciones de red

En la parte 3, debe calcular la dirección de red para las direcciones IP y las máscaras de subred dadas. Una vez que tenga la dirección de red, debe poder determinar las respuestas para completar la práctica de laboratorio.

Paso 1: Determinar si las direcciones IP están en la misma red

- a. Está configurando dos PC para su red. A la PC-A se le asigna la dirección IP 192.168.1.18 y a la PC-B se le asigna la dirección IP 192.168.1.33. Las dos PC reciben una máscara de subred 255.255.255.240.
- ¿Cuál es la dirección de red para la PC-A? _____ 192.168.1.16
- ¿Cuál es la dirección de red para la PC-B? _____ 192.168.1.32
- ¿Estas PC podrán comunicarse directamente entre sí? _____ No
- ¿Cuál es la dirección más alta que se puede asignar a la PC-B que le permita estar en la misma red que la PC-A?
- _____ 192.168.1.30
- b. Está configurando dos PC para su red. A la PC-A se le asigna la dirección IP 10.0.0.16 y a la PC-B se le asigna la dirección IP 10.1.14.68. Las dos PC reciben la máscara de subred 255.254.0.0.
- ¿Cuál es la dirección de red para la PC-A? _____ 10.0.0.0
- ¿Cuál es la dirección de red para la PC-B? _____ 10.0.0.0
- ¿Estas PC podrán comunicarse directamente entre sí? _____ Sí
- ¿Cuál es la dirección más baja que se puede asignar a la PC-B que le permita estar en la misma red que la PC-A?
- _____ 10.0.0.1

Paso 2: Identificar la dirección de gateway predeterminado

- a. Su empresa tiene una política para utilizar la primera dirección IP de una red como la dirección de gateway predeterminado. Un host en la red de área local (LAN) tiene una dirección IP 172.16.140.24 y una máscara de subred 255.255.192.0.
- ¿Cuál es la dirección de red para esta red?
- _____ 172.16.128.0
- ¿Cuál es la dirección de gateway predeterminado para este host?
- _____ 172.16.128.1
- b. Su empresa tiene una política para utilizar la primera dirección IP de una red como la dirección de gateway predeterminado. Se le indicó configurar un servidor nuevo con una dirección IP 192.168.184.227 y una máscara de subred 255.255.255.248.
- ¿Cuál es la dirección de red para esta red?
- _____ 192.168.184.224
- ¿Cuál es el gateway predeterminado para este servidor?
- _____ 192.168.184.225

Reflexión

¿Por qué la máscara de subred es importante para determinar la dirección de red?

La máscara de subred proporciona la cantidad de bits que se deben usar para la porción de red de una dirección. La dirección de red no se puede determinar sin ella.

Práctica de laboratorio: Identificación de direcciones IPv4

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Identificar direcciones IPv4

- Identificar la porción de red y de host de una dirección IP.
- Identificar el rango de direcciones de host dado un par de máscara de red y prefijo.

Parte 2: Clasificar direcciones IPv4

- Identificar el tipo de dirección (red, host, multicast o broadcast).
- Identificar si una dirección es pública o privada.
- Determinar si una asignación de dirección es una dirección de host válida.

Información básica/Situación

El direccionamiento es una función importante de los protocolos de la capa de red, porque permite la comunicación de datos entre hosts en la misma red o en redes diferentes. En esta práctica de laboratorio, examinará la estructura de las direcciones del protocolo de Internet versión 4 (IPv4). Identificará los diversos tipos de direcciones IPv4 y los componentes que ayudan a formar la dirección, como la porción de red, la porción de host y la máscara de subred. Entre los tipos de direcciones que se abarcan, se incluyen las siguientes: pública, privada, unicast y multicast.

Nota para el instructor: esta actividad puede realizarse en forma individual en clase o asignarse como tarea para el hogar. La práctica de laboratorio también puede realizarse en clase con los estudiantes agrupados de a dos. Si se realiza en clase, debe ir seguida de un debate con las respuestas correctas. Todas las direcciones IP públicas que se utilizan en esta práctica de laboratorio son propiedad de Cisco.

Recursos necesarios

- Dispositivo con acceso a Internet
- Opcional: calculadora de direcciones IPv4

Parte 1: Identificar direcciones IPv4

En la parte 1, se le proporcionarán varios ejemplos de direcciones IPv4, y deberá completar las tablas con la información apropiada.

Paso 1: Analizar la tabla que se muestra a continuación e identificar la porción de red y la porción de host de las direcciones IPv4 dadas

En las dos primeras filas, se muestran ejemplos de la forma en que debe completarse la tabla.

Referencias para la tabla:

N = los 8 bits de un octeto están en la porción de red de la dirección

n = un bit en la porción de red de la dirección

H = los 8 bits de un octeto están en la porción de host de la dirección

h = un bit en la porción de host de la dirección

Dirección/prefijo IP	Red/host N, n = red H, h = host	Máscara de subred	Dirección de red
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27	N.N.N.nnnhhhhh	255.255.255.224	209.165.200.224
172.31.45.252/24	N.N.N.H	255.255.255.0	172.31.45.0
10.1.8.200/26	N.N.N.nnnhhhhh	255.255.255.192	10.1.8.192
172.16.117.77/20	N.N.nnnnhhhh.H	255.255.240.0	172.16.112.0
10.1.1.101/25	N.N.N.nnnhhhhh	255.255.255.128	10.1.1.0
209.165.202.140/27	N.N.N.nnnhhhhh	255.255.255.224	209.165.202.128
192.168.28.45/28	N.N.N.nnnnhhhh	255.255.255.240	192.168.28.32

Paso 2: Analizar la tabla siguiente e indicar el rango de direcciones de host y de broadcast, dado un par de máscara de red y prefijo

En la primera fila, se muestra un ejemplo de cómo se debe completar.

Dirección/prefijo IP	Primera dirección de host	Última dirección de host	Dirección de broadcast
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23	10.101.98.1	10.101.99.254	10.101.99.255
209.165.200.227/27	209.165.200.225	209.165.200.254	209.165.200.255
172.31.45.252/24	172.31.45.1	172.31.45.254	172.31.45.255
10.1.8.200/26	10.1.8.193	10.1.8.254	10.1.8.255
172.16.117.77/20	172.16.112.1	172.16.127.254	172.16.127.255
10.1.1.101/25	10.1.1.1	10.1.1.126	10.1.1.127
209.165.202.140/27	209.165.202.129	209.165.202.158	209.165.202.159
192.168.28.45/28	192.168.28.33	192.168.28.46	192.168.28.47

Parte 2: Clasificar direcciones IPv4

En la parte 2, identificará y clasificará varios ejemplos de direcciones IPv4.

Paso 1: Analizar la tabla siguiente e identificar el tipo de dirección (dirección de red, de host, multicast o broadcast)

En la primera fila, se muestra un ejemplo de cómo se debe completar.

Dirección IP	Máscara de subred	Tipo de dirección
10.1.1.1	255.255.255.252	direcciones
192.168.33.63	255.255.255.192	broadcast
239.192.1.100	255.252.0.0	multicast
172.25.12.52	255.255.255.0	direcciones
10.255.0.0	255.0.0.0	direcciones
172.16.128.48	255.255.255.240	red
209.165.202.159	255.255.255.224	broadcast
172.16.0.255	255.255.0.0	direcciones
224.10.1.11	255.255.255.0	multicast

Paso 2: Analizar la tabla siguiente e identificar la dirección como pública o privada

Dirección/prefijo IP	Pública o privada
209.165.201.30/27	Pública
192.168.255.253/24	Privada
10.100.11.103/16	Privada
172.30.1.100/28	Privada
192.31.7.11/24	Pública
172.20.18.150/22	Privada
128.107.10.1/16	Pública
192.135.250.10/24	Pública
64.104.0.11/16	Pública

Paso 3: Analizar la tabla siguiente e identificar si el par dirección/prefijo es una dirección de host válida

Dirección/prefijo IP	¿La dirección de host es válida?	Motivo
127.1.0.10/24	No	Loopback
172.16.255.0/16	Sí	Dirección de host
241.19.10.100/24	No	Reservado
192.168.0.254/24	Sí	Dirección de host
192.31.7.255/24	No	Broadcast
64.102.255.255/14	Sí	Dirección de host
224.0.0.5/16	No	Multicast
10.0.255.255/8	Sí	Dirección de host
198.133.219.8/24	Sí	Dirección de host

Reflexión

¿Por qué debemos seguir estudiando y aprendiendo sobre el direccionamiento IPv4 si el espacio de direcciones IPv4 disponible está agotado?

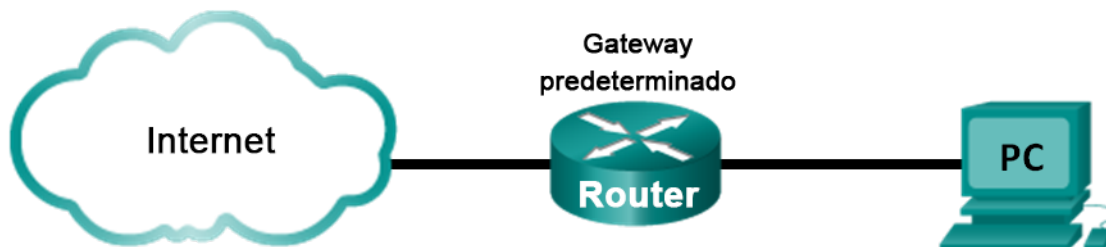
Muchas organizaciones seguirán usando el espacio de direcciones IPv4 privadas para sus necesidades internas de redes. Las direcciones IPv4 públicas se utilizarán por muchos años más.

Práctica de laboratorio: Identificación de direcciones IPv6

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Identificar los diferentes tipos de direcciones IPv6

- Revisar los distintos tipos de direcciones IPv6.
- Identificar la dirección IPv6 con el tipo correcto.

Parte 2: Examinar una interfaz y una dirección de red de host IPv6

- Revisar la configuración de la dirección de red IPv6 de la PC.

Parte 3: Practicar la abreviatura de direcciones IPv6

- Estudiar y revisar las reglas para la abreviatura de direcciones IPv6.
- Practicar la compresión y descompresión de direcciones IPv6.

Parte 4: Identificar la jerarquía del prefijo de red de dirección IPv6 unicast global

- Estudiar y revisar la jerarquía del prefijo de red IPv6.
- Practicar la obtención de información del prefijo de red desde una dirección IPv6.

Información básica/Situación

Debido al agotamiento del espacio de direcciones de red del protocolo de Internet versión 4 (IPv4) y a la adopción de IPv6 y la transición a este nuevo protocolo, los profesionales de redes deben entender cómo funcionan las redes IPv4 e IPv6. Muchos dispositivos y aplicaciones ya admiten el protocolo IPv6. Esto incluye la compatibilidad extendida del Sistema operativo Internetwork (IOS) de los dispositivos Cisco y la compatibilidad de sistemas operativos de estaciones de trabajo y servidores, como Windows y Linux.

Esta práctica de laboratorio se centra en las direcciones IPv6 y los componentes de la dirección. En la parte 1, identificará los tipos de direcciones IPv6 y, en la parte 2, verá las configuraciones de IPv6 en una PC. En la parte 3, practicará la abreviatura de direcciones IPv6 y, en la parte 4, identificará las partes del prefijo de red IPv6 haciendo foco en las direcciones unicast globales.

Nota para el instructor: esta práctica de laboratorio contiene cuatro secciones que pueden dividirse en dos partes: parte 1/2 y parte 3/4. Se puede realizar en varias sesiones o asignarse como tarea para el hogar.

Recursos necesarios

- 1 PC (Windows 7 o Vista con acceso a Internet)

Nota: el protocolo IPv6 se habilita en Windows 7 y en Windows Vista de manera predeterminada. El sistema operativo Windows XP no habilita el protocolo IPv6 de manera predeterminada, y no se recomienda su uso en esta práctica de laboratorio. En esta práctica de laboratorio se utilizan hosts de PC con Windows 7.

Nota para el instructor: para obtener instrucciones sobre cómo habilitar IPv6 y configurar direcciones de host con Windows XP, consulte el Manual de prácticas de laboratorio para el instructor.

Parte 1: Identificar los diferentes tipos de direcciones IPv6

En la parte 1, revisará las características de las direcciones IPv6 para identificar los diferentes tipos de direcciones IPv6.

Paso 1: Revisar los distintos tipos de direcciones IPv6.

Las direcciones IPv6 tienen una longitud de 128 bits. Con mayor frecuencia, se presenta como 32 caracteres hexadecimales. Cada carácter hexadecimal equivale a 4 bits ($4 \times 32 = 128$). A continuación, se muestra una dirección de host IPv6 no abreviada:

2001:0DB8:0001:0000:0000:0000:0000:0001

Un hexteto es la versión IPv6 hexadecimal de un octeto IPv4. Las direcciones IPv4 tienen una longitud de 4 octetos, separados por puntos. Una dirección IPv6 tiene una longitud de 8 hextetos, separados por dos puntos.

Una dirección IPv4 tiene una longitud de 4 octetos y, normalmente, se escribe o se muestra en notación decimal.

255.255.255.255

Una dirección IPv6 tiene una longitud de 8 hextetos y, normalmente, se escribe o se muestra en notación hexadecimal.

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

En una dirección IPv4, cada octeto individual tiene una longitud de 8 dígitos binarios (bits). Cuatro octetos equivalen a una dirección IPv4 de 32 bits.

11111111 = 255

11111111.11111111.11111111.11111111 = 255.255.255.255

En una dirección IPv6, cada hexteto individual tiene una longitud de 16 bits. Ocho hextetos equivalen a una dirección IPv6 de 128 bits.

1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.

1111111111111111.1111111111111111.1111111111111111.1111111111111111 =

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Si leemos una dirección IPv6 desde la izquierda, el primer hexteto (o el del extremo izquierdo) identifica el tipo de dirección IPv6. Por ejemplo, si la dirección IPv6 tiene todos ceros en el hexteto del extremo izquierdo, la dirección posiblemente sea una dirección de loopback.

0000:0000:0000:0000:0000:0000:0000:0001 = dirección de loopback

::1 = dirección de loopback abreviada

Como otro ejemplo, si la dirección IPv6 tiene FE80 en el primer hexteto, se trata de una dirección link-local.

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = dirección link-local

FE80::C5B7:CB51:3C00:D6CE = dirección link-local abreviada

Estudie el cuadro siguiente, que le resultará útil para identificar los diferentes tipos de direcciones IPv6 según los números en el primer hexteto.

Primer hexeteto (extremo izquierdo)	Tipo de dirección IPv6
De 0000 a 00FF	Dirección de loopback, cualquier dirección, dirección no especificada o compatible con IPv4
De 2000 a 3FFF	Dirección unicast global (una dirección enrutable en un rango de direcciones que actualmente se encuentra bajo la responsabilidad de la Internet Assigned Numbers Authority [IANA])
De FE80 a FEBF	Link-local (una dirección unicast que identifica el equipo host en la red local)
De FC00 a FCFE	Local única (una dirección unicast que puede asignarse a un host para identificarlo como parte de una subred específica en la red local)
De FF00 a FFFF	Dirección multicast

Existen otros tipos de direcciones IPv6 que aún no tienen una implementación muy extendida o que ya cayeron en desuso y no se admiten más. Por ejemplo, las **direcciones anycast** son nuevas en IPv6, los routers pueden utilizarlas para facilitar la tarea de compartir cargas y proporcionan flexibilidad para tomar rutas alternativas en caso de que un router deje de estar disponible. Solo los routers deben responder a las direcciones anycast. Por su parte, las **direcciones locales de sitio** cayeron en desuso y se reemplazaron por las direcciones locales únicas. Las direcciones locales de sitio se identificaban con los números FEC0 en el hexeteto inicial.

En las redes IPv6, no hay direcciones de red (cable) ni direcciones de broadcast como las que hay en las redes IPv4.

Paso 2: Identificar la dirección IPv6 con su tipo

Identifique las direcciones IPv6 con el tipo de dirección correspondiente. Observe que las direcciones se comprimieron a su notación abreviada y que no se muestra el número de prefijo de red con barra diagonal. Algunas opciones deben usarse más de una vez.

Dirección IPv6	Respuesta
2001:0DB8:1:ACAD::FE55:6789:B210	1. ____
::1	2. ____
FC00:22:A:2::CD4:23E4:76FA	3. ____
2033:DB8:1:1:22:A33D:259A:21FE	4. ____
FE80::3201:CC01:65B1	5. ____
FF00::	6. ____
FF00::DB7:4322:A231:67C	7. ____
FF02::2	8. ____

Opciones de respuesta

- a. Dirección de loopback
- b. Dirección unicast global
- c. Dirección link-local
- d. Dirección local única
- e. Dirección multicast

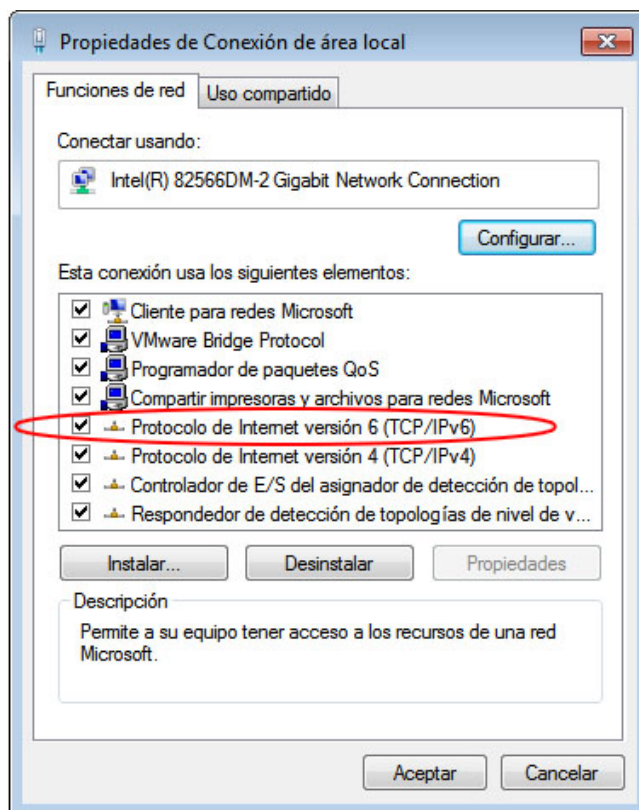
Respuestas: 1. B, 2. A, 3. D, 4. B, 5. C, 6. E, 7. E, 8. E

Parte 2: Examinar una interfaz y una dirección de red de host IPv6

En la parte 2, revisará la configuración de red IPv6 de la PC para identificar la dirección IPv6 de la interfaz de red.

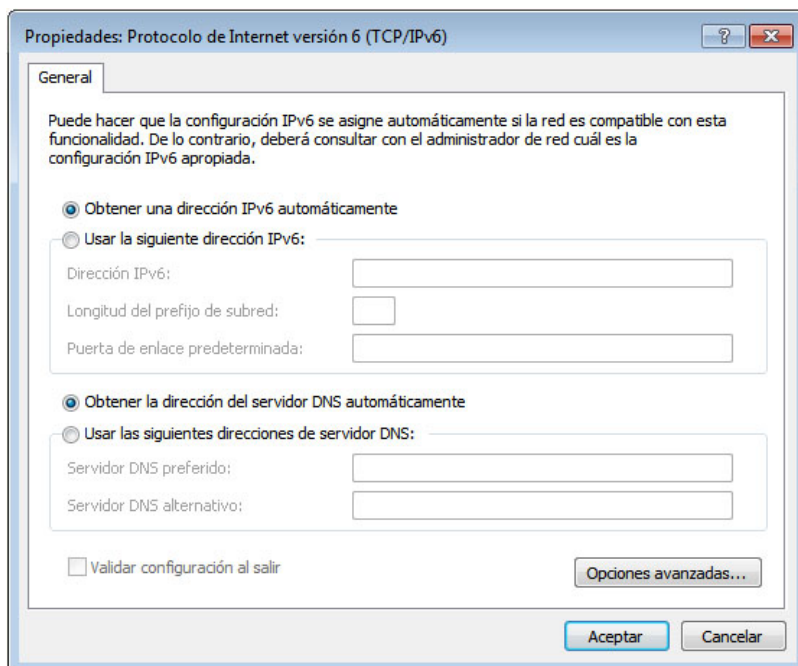
Paso 1: Revisar la configuración de la dirección de red IPv6 de la PC

- Verifique que el protocolo IPv6 esté instalado y activo en la PC-A (revise la configuración de la conexión de área local).
- Haga clic en el botón **Inicio** de Windows y luego en **Panel de control**. Cambie **Ver por: Categoría** por **Ver por: Íconos pequeños**.
- Haga clic en el ícono **Centro de redes y recursos compartidos**.
- En el lado izquierdo de la ventana, haga clic en **Cambiar configuración del adaptador**. Ahora debería ver íconos que representen los adaptadores de red instalados. Haga clic con el botón secundario en la interfaz de red activa (puede ser **Conexión de área local** o **Conexión de red inalámbrica**) y, luego, haga clic en **Propiedades**.
- Ahora debería ver la ventana Propiedades de la conexión de red. Desplácese por la lista de elementos para determinar si IPv6 está presente, lo que indica que está instalado, y si también está marcada la casilla de verificación, lo que indica que está activo.



- Seleccione el elemento **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Propiedades**. Debería ver la configuración de IPv6 para la interfaz de red. Es probable que la ventana de propiedades de IPv6 esté establecida en **Obtener una dirección IPv6 automáticamente**. Esto no significa que IPv6 dependa del protocolo de configuración dinámica de host (DHCP). En lugar de usar DHCP, IPv6 busca información de la red IPv6 en el router local y luego configura automáticamente sus propias direcciones IPv6. Para configurar IPv6 manualmente, debe proporcionar la dirección IPv6, la duración de prefijo de subred y el gateway predeterminado.

Nota: el router local puede referir las solicitudes de información de IPv6 del host, en especial la información del Sistema de nombres de dominios (DNS), a un servidor de DHCPv6 en la red.



- g. Después de verificar que IPv6 está instalado y activo en la PC, debe revisar la información de dirección IPv6. Para ello, haga clic en el botón **Inicio**, escriba **cmd** en el cuadro *Buscar programas y archivos* y presione Entrar. Esto abre una ventana del símbolo del sistema de Windows.
- h. Escriba **ipconfig /all** y presione Entrar. El resultado debe ser similar al siguiente:

```
C:\Users\user> ipconfig /all
```

```
Windows IP Configuration
```

```
<resultado omitido>
```

```
Wireless LAN adapter Wireless Network Connection:
```

```

Connection-specific DNS Suffix  . :
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 02-37-10-41-FB-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8d4f:4f4d:3237:95e2%14 (Preferred)
IPv4 Address. . . . . : 192.168.2.106 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06, 2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07, 2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-B1-1C-C1-DE-91-C3-5D

```

```
DNS Servers . . . . . : 192.168.1.1
                        8.8.4.4
```

<resultado omitido>

- i. Puede observar en el resultado que la PC cliente tiene una dirección IPv6 link-local con una ID de interfaz generada en forma aleatoria. ¿Qué indica esto acerca de la red con respecto a la dirección IPv6 unicast global, la dirección IPv6 local única o la dirección IPv6 de gateway?

Indica que no hay un router de gateway con IPv6 habilitado que proporcione la dirección global, la dirección local o la información de subred en la red.

- j. ¿Qué tipo de direcciones IPv6 encontró al utilizar `ipconfig /all`?

Las respuestas varían, pero lo más probable es que también sean direcciones link-local.

Parte 3: Practicar la abreviatura de direcciones IPv6

En la parte 3, estudiará y revisará las reglas de abreviación de direcciones IPv6 para comprimir y descomprimir correctamente las direcciones IPv6.

Paso 1: Estudiar y revisar las reglas para la abreviatura de direcciones IPv6.

Regla 1: en una dirección IPv6, una cadena de cuatro ceros (0) en un hexteto se puede abreviar como un solo cero.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:0404:0001:1000:0:0:0EF0:BC00 (abreviado con un solo cero)

Regla 2: en una dirección IPv6, los ceros iniciales en cada hexteto pueden omitirse, no así los ceros finales.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:404:1:1000:0:0:EF0:BC00 (abreviado con ceros iniciales omitidos)

Regla 3: en una dirección IPv6, una sola cadena continua de cuatro ceros o más puede abreviarse como dos puntos dobles (::). La abreviatura con dos puntos dobles se puede utilizar una sola vez en una dirección IP.

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:404:1:1000::EF0:BC00 (abreviado con ceros iniciales omitidos y ceros continuos reemplazados por dos puntos dobles)

En la siguiente imagen, se ilustran estas reglas de abreviatura de direcciones IPv6:

```
FF01:0000:0000:0000:0000:0000:1  
= FF01:0:0:0:0:0:1  
= FF01::1
```

```
E3D7:0000:0000:0000:51F4:00C8:C0A8:6420  
= E3D7::51F4:C8:C0A8:6420
```

```
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB  
= 3FFE:501:8:0:260:97FF:FE40:EFAB  
= 3FFE:501:8::260:97FF:FE40:EFAB
```

Paso 2: Practicar la compresión y descompresión de direcciones IPv6.

Aplice las reglas para la abreviatura de direcciones IPv6 y comprima o descomprima las siguientes direcciones:

- 1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

2002:EC0:200:1::4EB:44CE:8A2

- 2) FE80:0000:0000:0001:0000:60BB:008E:7402

FE80::1:0:60BB:8E:7402

- 3) FE80::7042:B3D7:3DEC:84B8

FE80:0000:0000:0000:7042:B3D7:3DEC:84B8

- 4) FF00::

FF00:0000:0000:0000:0000:0000:0000

- 5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

2001:30:1:ACAD::330E:10C2:32BF

Parte 4: Identificar la jerarquía del prefijo de red de dirección IPv6 unicast global

En la parte 4, estudiará y revisará las características del prefijo de red IPv6 para identificar los componentes de red jerárquicos del prefijo de red IPv6.

Paso 1: Estudiar y revisar la jerarquía del prefijo de red IPv6

Una dirección IPv6 es una dirección de 128 bits que consta de dos partes: la porción de red, identificada por los primeros 64 bits o los primeros cuatro hextetos, y la porción de host, identificada por los últimos 64 bits o los últimos cuatro hextetos. Recuerde que cada número, o carácter, en una dirección IPv6 se escribe en hexadecimales, lo que equivale a cuatro bits. La siguiente es una dirección unicast global típica:

Porción de red: **2001:DB8:0001:ACAD:xxxx:xxxx:xxxx:xxxx**

Porción de host: **xxxx:xxxx:xxxx:xxxx:0000:0000:0000:0001**

La mayoría de las direcciones unicast globales (enrutables) utilizan un prefijo de red de 64 bits y una dirección de host de 64 bits. Sin embargo, la porción de red de una dirección IPv6 no se limita a una longitud de 64 bits, y la longitud se identifica al final de la dirección mediante una notación de barra diagonal seguida de un número decimal. Si el prefijo de red es /64, la porción de red de la dirección IPv6 tiene una longitud de 64 bits de izquierda a derecha. La porción de host, o la ID de interfaz, que corresponde a los últimos 64 bits, es lo que resta de la dirección IPv6. En algunos casos, como en una dirección de loopback, el prefijo de red puede ser /128 (tener una longitud de ciento veintiocho bits). En este caso, no se dejan bits para el identificador de interfaz y, por lo tanto, la red está limitada a un solo host. Los siguientes son algunos ejemplos de direcciones IPv6 con distintas duraciones de prefijo de red:

Dirección unicast global:	2001:DB8:0001:ACAD:0000:0000:0000:0001/64
Dirección de loopback:	::1/128
Dirección multicast:	FF00::/8
Dirección de todas las redes:	::/0 (similar a una dirección quad cero en IPv4)
Dirección link-local	fe80::8d4f:4f4d:3237:95e2%14 (observe que la barra seguida de catorce al final de la dirección se representa con un signo de porcentaje y el número decimal catorce. Esta dirección se tomó del resultado de un comando ipconfig /all en el símbolo del sistema de Windows).

De izquierda a derecha, la porción de red de una dirección IPv6 unicast global tiene una estructura jerárquica que proporcionará la siguiente información:

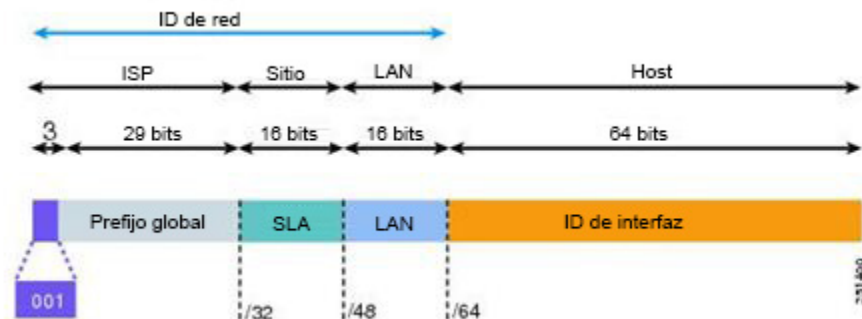
- 1) Número de enrutamiento global de IANA (los tres primeros bits binarios se fijan en 001)
200::/12
- 2) Prefijo del registro regional de Internet (RIR) (bits del /12 al /23)
2001:0D::/23 (el carácter D hexadecimal es 1101 en sistema binario. Los bits del 21 al 23 son 110, y el último bit es parte del prefijo del ISP)
- 3) Prefijo del proveedor de servicios de Internet (ISP) (bits hasta el /32)
2001:0DB8::/32
- 4) Prefijo de sitio o agregador de nivel de sitio (SLA), que el ISP asigna al cliente (bits hasta el /48)
2001:0DB8:0001::/48
- 5) Prefijo de subred (asignado por el cliente; bits hasta el /64)
2001:0DB8:0001:ACAD::/64

- 6) ID de interfaz (el host se identifica por los últimos 64 bits en la dirección)

2001:DB8:0001:ACAD:8D4F:4F4D:3237:95E2/64

En la imagen siguiente, se muestra que la dirección IPv6 puede agruparse en cuatro partes básicas:

- 1) Prefijo de enrutamiento global /32
- 2) Agregador de nivel de sitio (SLA) /48
- 3) ID de subred (LAN) /64
- 4) ID de interfaz (últimos 64 bits)



La porción de host de la dirección IPv6 se denomina “ID de interfaz”, porque no identifica al host propiamente dicho, sino a la tarjeta de interfaz de red del host. Cada interfaz de red puede tener varias direcciones IPv6 y, por lo tanto, también puede tener varias ID de interfaz.

Paso 2: Practicar la obtención de información del prefijo de red desde una dirección IPv6.

Dada la siguiente dirección, responda las siguientes preguntas:

2000:1111:aaaa:0:50a5:8a35:a5bb:66e1/64

- a. ¿Cuál es la ID de interfaz?

50a5:8a35:a5bb:66e1

- b. ¿Cuál es el número de subred?

0

- c. ¿Cuál es el número de sitio?

aaaa

- d. ¿Cuál es el número de ISP?

11

- e. ¿Cuál es el número de ISP en sistema binario?

0001 0001

- f. ¿Cuál es el número de registro?

011

- g. ¿Cuál es el número de registro en sistema binario?

0000 0001 0001

- h. ¿Cuál es el número global de IANA?

2

- i. ¿Cuál es el prefijo de enrutamiento global?

2000:1111:

Reflexión

1. ¿Cómo cree que debe dar soporte a IPv6 en el futuro?

Las respuestas varían.

2. ¿Considera que las redes IPv4 continuarán existiendo o que todos finalmente cambiarán a IPv6? ¿Cuánto tiempo cree que llevará esto?

Las respuestas varían.

Práctica de laboratorio: Configuración de direcciones IPv6 en dispositivos de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Duración de prefijo	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1	64	No aplicable
	G0/1	2001:DB8:ACAD:1::1	64	No aplicable
S1	VLAN 1	2001:DB8:ACAD:1::B	64	No aplicable
PC-A	NIC	2001:DB8:ACAD:1::3	64	FE80::1
PC-B	NIC	2001:DB8:ACAD:A::3	64	FE80::1

Objetivos

Parte 1: Establecer la topología y configurar los parámetros básicos del router y del switch

Parte 2: Configurar las direcciones IPv6 de forma manual

Parte 3: Verificar la conectividad de extremo a extremo

Información básica/Situación

Conocer los grupos multicast del protocolo de Internet versión 6 (IPv6) puede resultar útil al asignar direcciones IPv6 en forma manual. Entender la forma en que se asigna el grupo multicast de todos los routers y la forma en que se debe controlar la asignación de direcciones para el grupo multicast de nodos solicitados permite evitar problemas de enrutamiento IPv6 y asegurar la implementación de las prácticas recomendadas.

En esta práctica de laboratorio, configurará hosts e interfaces de dispositivos con direcciones IPv6 y explorará la forma en que el grupo multicast de todos los routers se asigna a un router. Utilizará comandos **show** para ver direcciones IPv6 unicast y multicast. También verificará la conectividad de extremo a extremo mediante los comandos **ping** y **traceroute**.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son ISR Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que el SDM utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing**. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

```
S1# configure terminal
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
S1(config)# end
```

```
S1# reload
```

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7 con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Gigabit Ethernet en los routers Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Nota: el protocolo IPv6 se habilita en Windows 7 y en Windows Vista de manera predeterminada. El sistema operativo Windows XP no habilita el protocolo IPv6 de manera predeterminada, y no se recomienda su uso en esta práctica de laboratorio. En esta práctica de laboratorio se utilizan hosts de PC con Windows 7.

Nota para el instructor: para obtener instrucciones sobre cómo habilitar IPv6 y configurar direcciones de host con Windows XP, consulte el Manual de prácticas de laboratorio para el instructor.

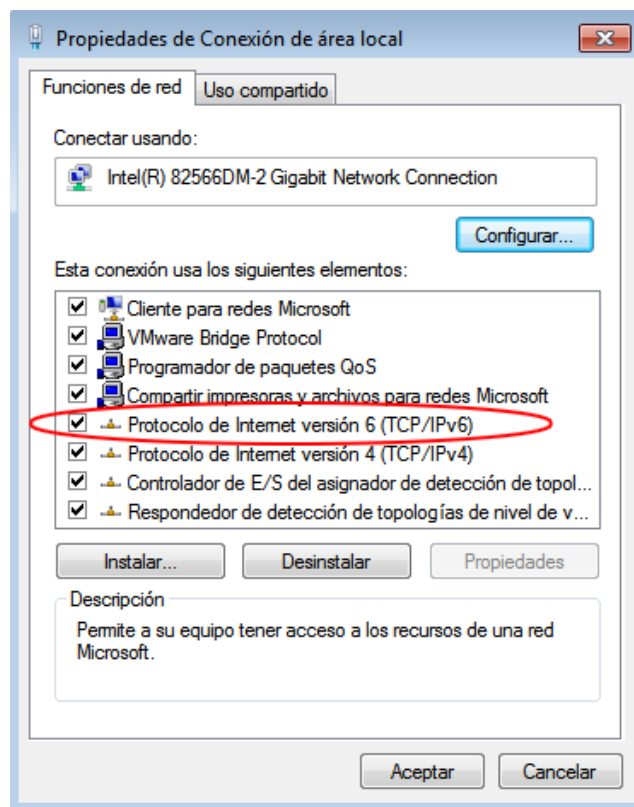
Parte 1: Establecer la topología y configurar los parámetros básicos del router y del switch

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Verificar que las interfaces de PC estén configuradas para utilizar el protocolo IPv6

Verifique que el protocolo IPv6 esté activo en las PC: en la ventana Propiedades de Conexión de área local, asegúrese de que la casilla de verificación de **Protocolo de Internet versión 6 (TCP/IPv6)** esté activada.



Paso 4: Configurar el router.

- Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- Asigne el nombre de dispositivo al router.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 5: Configure el switch.

- Acceda al switch mediante el puerto de consola y habilite al modo EXEC privilegiado.
- Asigne un nombre del dispositivo al switch.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

- f. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
- g. Encripte las contraseñas de texto no cifrado.
- h. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- i. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Configurar las direcciones IPv6 de forma manual

Paso 1: Asignar las direcciones IPv6 a interfaces Ethernet en el R1

- a. Asigne las direcciones IPv6 unicast globales que se indican en la tabla de direccionamiento a las dos interfaces Ethernet en el R1.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1#
```

Nota para el instructor: el prefijo global IPv6 2001:DB8::/32 es un prefijo reservado para propósitos de documentación, tal como se describe en la RFC 3849.

- b. Emita el comando **show ipv6 interface brief** para verificar que se asignó la dirección IPv6 unicast correcta a cada interfaz.

```
R1# show ipv6 interface brief
Em0/0                                [administratively down/down]
    unassigned
GigabitEthernet0/0                   [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:A::1
GigabitEthernet0/1                   [up/up]
    FE80::D68C:B5FF:FECE:A0C1
    2001:DB8:ACAD:1::1
Serial0/0/0                          [administratively down/down]
    unassigned
Serial0/0/1                          [administratively down/down]
    unassigned
R1#
```

- c. Emita el comando **show ipv6 interface g0/0**. Observe que la interfaz indica dos grupos multicast de nodos solicitados, porque la ID de interfaz link-local IPv6 (FE80) no se configuró manualmente para que coincida con la ID de interfaz IPv6 unicast.

Nota: la dirección link-local que se muestra se basa en direccionamiento EUI-64, que utiliza automáticamente la dirección de control de acceso al medio (MAC) de la interfaz para crear una dirección IPv6 link-local de 128 bits.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
```



```
IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C0
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
  FF02::1:FFCE:A0C0
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
```

- d. Para obtener una dirección link-local que coincida con la dirección unicast en la interfaz, introduzca manualmente las direcciones link-local en cada una de las interfaces Ethernet en el R1.

```
R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface g0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# end
R1#
```

Nota: cada interfaz del router pertenece a una red separada. Los paquetes con una dirección link-local nunca salen de la red local, por lo tanto, puede utilizar la misma dirección link-local en ambas interfaces.

- e. Vuelva a emitir el comando **show ipv6 interface g0/0**. Observe que la dirección link-local cambió a **FE80::1** y que se indica un solo grupo multicast de nodos solicitados.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
```

```
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
```

¿Qué grupos multicast se asignaron a la interfaz G0/0?

El grupo multicast de todos los nodos (FF02::1) y el grupo multicast de nodos solicitados (FF02::1:FF00:1).

Paso 2: Habilitar el enrutamiento IPv6 en el R1

- En el símbolo del sistema de la PC-B, introduzca el comando **ipconfig** para examinar la información de dirección IPv6 asignada a la interfaz de la PC.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::dd0e:67fb:d14f:1288%11
    Autoconfiguration IPv4 Address. . : 169.254.18.136
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\>_
```

¿Se asignó una dirección IPv6 unicast a la tarjeta de interfaz de red (NIC) en la PC-B? _____ **No**

- Habilite el enrutamiento IPv6 en el R1 por medio del comando **IPv6 unicast-routing**.

```
R1 # configure terminal
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
*Dec 17 18:29:07.415: %SYS-5-CONFIG_I: Configured from console by console
```

- Utilice el comando **show ipv6 interface g0/0** para ver los grupos multicast que se asignaron a la interfaz G0/0. Observe que el grupo multicast de todos los routers (FF02::2) ahora aparece en la lista de grupos para la interfaz G0/0.

Nota: esto permite que las PC obtengan la información de dirección IP y del gateway predeterminado automáticamente mediante la configuración automática de dirección sin estado (SLAAC).

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
R1#
```

- d. Ahora que el R1 forma parte del grupo multicast de todos los routers, vuelva a emitir el comando **ipconfig** en la PC-B. Examine la información de dirección IPv6.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8:acad:a:dd0e:67fb:d14f:1288
    Temporary IPv6 Address. . . . . : 2001:db8:acad:a:6082:dcb0:5fb2:3ece
    Link-local IPv6 Address . . . . . : fe80::dd0e:67fb:d14f:1288%11
    Autoconfiguration IPv4 Address. . : 169.254.18.136
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1%11

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\>
```

¿Por qué la PC-B recibió el prefijo de enrutamiento global y la ID de subred que configuró en el R1?

G0/0 del R1 ahora forma parte del grupo multicast de todos los routers, FF02::2. Esto permite que se envíen mensajes de anuncio de router (RA) con información de dirección de red global y de ID de subred a todos los nodos en la LAN. Observe que también se envió la dirección link-local, FE80::1, como gateway predeterminado. Las PC recibirán su dirección IP y gateway predeterminado a través de SLAAC.

Paso 3: Asignar direcciones IPv6 a la interfaz de administración (SVI) en el S1

- a. Asigne la dirección IPv6 que se indica en la tabla de direccionamiento a la interfaz de administración (VLAN 1) en el S1. También asigne una dirección link-local a esta interfaz. La sintaxis de los comandos IPv6 es igual que en el router.

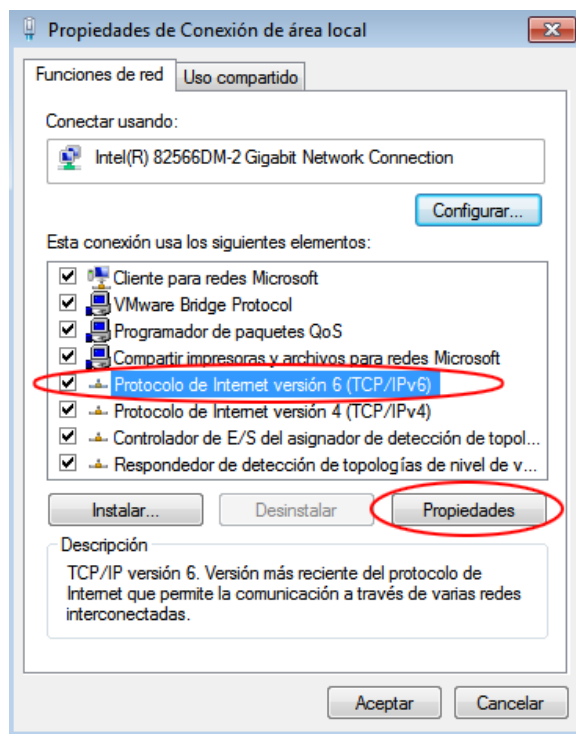
```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address 2001:db8:acad:1::b/64
S1(config-if)# ipv6 address fe80::b link-local
S1(config-if)# end
S1#
*Mar  1 03:25:26.681: %SYS-5-CONFIG_I: Configured from console by console
```

- b. Verifique que las direcciones IPv6 se hayan asignado correctamente a la interfaz de administración mediante el comando **show ipv6 interface vlan1**.

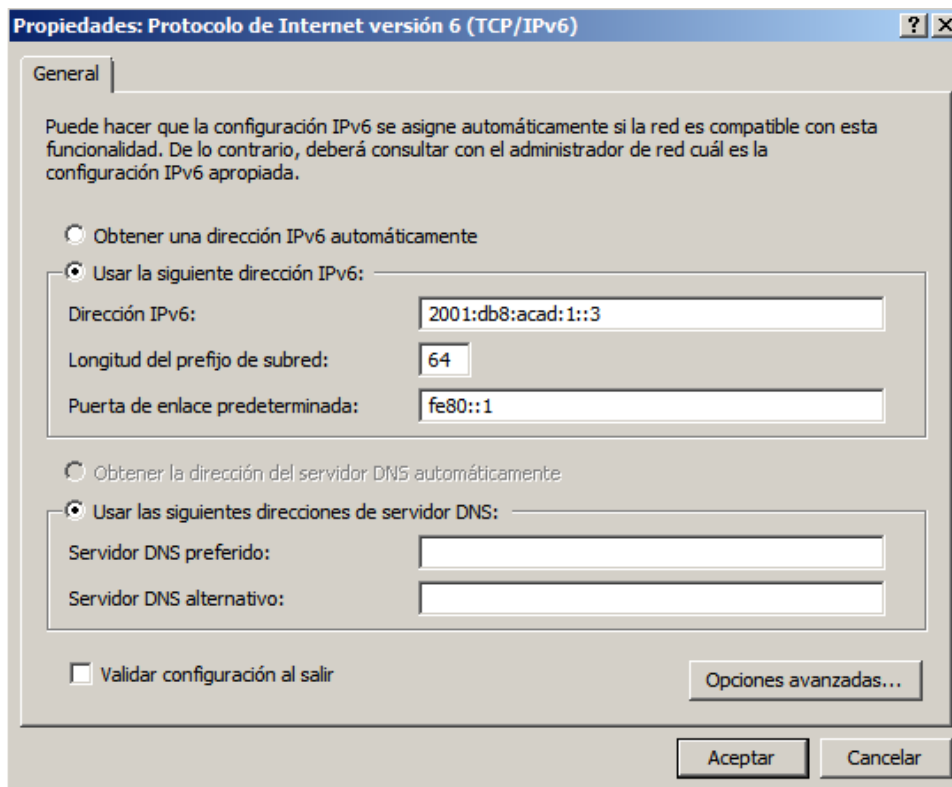
```
S1# show ipv6 interface vlan1
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::B
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::B, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:B
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: Check hwidb
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
S1#
```

Paso 4: Asignar direcciones IPv6 estáticas a las PC

- a. Abra la ventana **Propiedades de Conexión de área local** en la PC-A. Seleccione **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Propiedades**.



- b. Haga clic en el botón de opción **Usar la siguiente dirección IPv6**. Consulte la tabla de direccionamiento e introduzca la información en los campos **Dirección IPv6**, **Longitud del prefijo de subred** y **Puerta de enlace predeterminada**. Haga clic en **Aceptar**.



- c. Haga clic en **Cerrar** para cerrar la ventana Propiedades de Conexión de área local.
- d. Repita los pasos 4a a 4c para introducir la información de dirección IPv6 estática en la PC-B. Para obtener la información de dirección IPv6 correcta, consulte la tabla de direccionamiento.
- e. Emita el comando **ipconfig** en la línea de comandos de la PC-B para verificar la información de dirección IPv6.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8:acad:a::3
    IPv6 Address. . . . . : 2001:db8:acad:a:d428:7de2:997c:b05a
    Temporary IPv6 Address. . . . . : 2001:db8:acad:a:e19e:db9f:e38e:9252
    Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:b05a%11
    Default Gateway . . . . . : fe80::1%11

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\>
```

Parte 3: Verificar la conectividad de extremo a extremo

- a. En la PC-A, haga ping a **FE80::1**. Esta es la dirección link-local asignada a G0/1 en el R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Nota: también puede probar la conectividad mediante la dirección unicast global, en lugar de la dirección link-local.

- b. Haga ping a la interfaz de administración del S1 desde la PC-A.

```
C:\>ping 2001:db8:acad:1::b

Pinging 2001:db8:acad:1::b with 32 bytes of data:
Reply from 2001:db8:acad:1::b: time=14ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=3ms

Ping statistics for 2001:db8:acad:1::b:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\>
```

- c. Utilice el comando **tracert** en la PC-A para verificar que haya conectividad de extremo a extremo con la PC-B.

```
C:\>tracert 2001:db8:acad:a::3

Tracing route to 2001:db8:acad:a::3 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    2001:db8:acad:1::1
  2     5 ms    <1 ms    <1 ms    2001:db8:acad:a::3

Trace complete.

C:\>
```

- d. Desde la PC-B, haga ping a la PC-A.

```
C:\>ping 2001:db8:acad:1::3

Pinging 2001:db8:acad:1::3 with 32 bytes of data:
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms

Ping statistics for 2001:db8:acad:1::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- e. Desde la PC-B, haga ping a la dirección link-local para G0/0 en el R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Nota: si no se establece conectividad de extremo a extremo, resuelva los problemas de asignación de direcciones IPv6 para verificar que haya introducido las direcciones correctamente en todos los dispositivos.

Reflexión

1. ¿Por qué se puede la asignar misma dirección link-local, FE80::1, a las dos interfaces Ethernet en el R1?

Los paquetes link-local nunca salen de la red local, por eso se puede usar la misma dirección link-local en una interfaz asociada a una red local diferente.

2. ¿Cuál es la ID de subred de la dirección IPv6 unicast 2001:db8:acad::aaaa:1234/64?

0 (cero) o 0000 (ceros). El cuarto hexteto es la ID de subred de una dirección IPv6 con un prefijo /64. En el ejemplo, el cuarto hexteto contiene todos ceros, y la regla de omisión de los segmentos compuestos por todos ceros de IPv6 utiliza dos puntos dobles para representar la ID de subred y los dos primeros hextetos de la ID de interfaz.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Configuraciones de dispositivos

Router R1 (después de la parte 1 de esta práctica de laboratorio)

```
R1#sh run
Building configuration...

Current configuration : 1443 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
```



```
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
password 7 01100F175804
login
line aux 0
line 2
```

```
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 104D000A0618
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1 (después de la parte 1 de esta práctica de laboratorio)

```
S1#sh run
Building configuration...

Current configuration : 1624 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
```

```
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
```

```
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
no ip address  
!  
ip http server  
ip http secure-server  
!  
banner motd ^C  
*****  
* Warning: Unauthorized access is prohibited! *  
*****  
^C  
!  
line con 0  
password 7 121A0C041104  
login  
line vty 0 4  
password 7 121A0C041104  
login  
line vty 5 15  
password 7 121A0C041104  
login  
!  
end
```

Router R1 (Final)

```
R1#show run  
Building configuration...  
  
Current configuration : 1577 bytes  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
memory-size iomem 15  
!  
no ip domain lookup
```

```
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
password 7 01100F175804
login
```

```
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 104D000A0618
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1 (Final)

```
S1#sh run
```

```
Building configuration...
```

```
Current configuration : 1733 bytes
```

```
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

```
!  
interface FastEthernet0/1  
shutdown  
!  
interface FastEthernet0/2  
shutdown  
!  
interface FastEthernet0/3  
shutdown  
!  
interface FastEthernet0/4  
shutdown  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  ipv6 address FE80::B link-local
  ipv6 address 2001:DB8:ACAD:1::B/64
!
ip http server
ip http secure-server
!
!
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
  password 7 121A0C041104
  login
line vty 0 4
  password 7 121A0C041104
  login
line vty 5 15
  password 7 121A0C041104
  login
!
end
```


Práctica de laboratorio: Prueba de conectividad de red con ping y traceroute (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

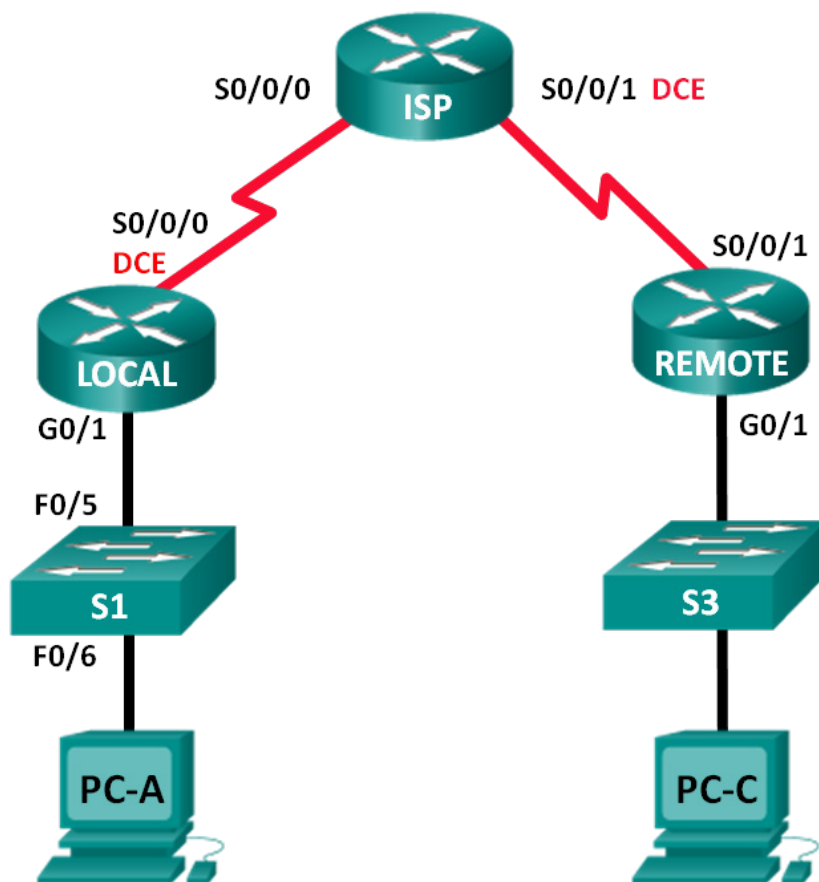


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
LOCAL	G0/1	192.168.1.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	No aplicable
ISP	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	No aplicable
REMOTE	G0/1	192.168.3.1	255.255.255.0	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objetivos

Parte 1: Armar y configurar la red

- Conectar la red
- Configurar las PC.
- Configurar los routers.
- Configurar los switches.

Parte 2: Utilizar el comando ping para realizar pruebas de red básicas

- Utilizar ping desde una PC.
- Utilizar ping desde dispositivos Cisco.

Parte 3: Utilizar los comandos tracert y traceroute para realizar pruebas de red básicas

- Utilizar tracert desde una PC.
- Utilizar traceroute desde dispositivos Cisco.

Parte 4: Resolver problemas de la topología

Información básica/Situación

Ping y traceroute son dos herramientas imprescindibles para probar la conectividad de red TCP/IP. Ping es una utilidad de administración de red que se utiliza para probar la posibilidad de conexión de un dispositivo en una red IP. Esta utilidad también mide el tiempo de ida y vuelta para los mensajes que se envían desde el host de origen hasta una PC de destino. La utilidad ping está disponible en Windows, en sistemas operativos (OS) del estilo de Unix y en el Sistema operativo Internetwork (IOS) de Cisco.

La utilidad traceroute es una herramienta de diagnóstico de red para mostrar la ruta y medir las demoras en el tránsito de los paquetes que viajan por una red IP. La utilidad tracert está disponible en Windows, y una utilidad similar, traceroute, está disponible en OS del estilo de Unix y en Cisco IOS.

En esta práctica de laboratorio, se examinan los comandos **ping** y **traceroute** y se exploran las opciones de comandos para modificar el comportamiento de estos. Además, se utilizan dispositivos Cisco y PC para explorar los comandos. Los routers Cisco usarán el protocolo de enrutamiento de gateway interior mejorado (EIGRP) para enrutar los paquetes entre las redes. En esta práctica de laboratorio, se proporcionan las configuraciones necesarias para los dispositivos Cisco.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 3 routers (Cisco 1941 con imagen universal de Cisco IOS, versión 15.2(4)M3 o comparable)
- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet y seriales, según se muestra en la topología

Parte 1: Armar y configurar la red

En la parte 1, configurará la red en la topología y configurará las PC y los dispositivos Cisco. Como referencia, se proporcionan las configuraciones iniciales para los routers y switches. En esta topología, el EIGRP se utiliza para enrutar paquetes entre redes.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Borrar las configuraciones en los routers y switches, y volver a cargar los dispositivos

Paso 3: Configurar las direcciones IP de las PC y los gateways predeterminados según la tabla de direccionamiento

Paso 4: Configurar los routers LOCAL, ISP y REMOTE mediante las configuraciones iniciales que se detallan a continuación

En la petición de entrada del modo de configuración global del switch o el router, copie y pegue la configuración para cada dispositivo. Guarde la configuración en startup-config.

Nota para el instructor: el comando “no auto-summary” para EIGRP se incluye para propósitos de compatibilidad con routers y versiones del IOS anteriores. Con el router 1941 y el IOS 15 especificados para esta práctica de laboratorio, el comando no auto-summary se incluye de manera predeterminada.

Configuraciones iniciales para el router LOCAL:

```
hostname LOCAL
no ip domain-lookup
```

```
interface s0/0/0
  ip address 10.1.1.1 255.255.255.252
  clock rate 56000
  no shutdown
interface g0/1
  ip add 192.168.1.1 255.255.255.0
  no shutdown
router eigrp 1
  network 10.1.1.0 0.0.0.3
  network 192.168.1.0 0.0.0.255
  no auto-summary
```

Configuraciones iniciales para el router ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
  ip address 10.1.1.2 255.255.255.252
  no shutdown
interface s0/0/1
  ip add 10.2.2.2 255.255.255.252
  clock rate 56000
  no shutdown
router eigrp 1
  network 10.1.1.0 0.0.0.3
  network 10.2.2.0 0.0.0.3
  no auto-summary
end
```

Configuraciones iniciales para el router REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
  ip address 10.2.2.1 255.255.255.252
  no shutdown
interface g0/1
  ip add 192.168.3.1 255.255.255.0
  no shutdown
router eigrp 1
  network 10.2.2.0 0.0.0.3
  network 192.168.3.0 0.0.0.255
  no auto-summary
end
```

Paso 5: Configurar los switches S1 y S3 con las configuraciones iniciales

Nota para el instructor: si se utiliza Netlab, las interfaces del switch FastEthernet 0/1–0/4 deben estar desactivadas para esta práctica de laboratorio. Utilice los siguientes comandos en los switches S1 y S3:

```
Switch (config)# interface range f0/1 - 4
Switch (config)# shutdown
```

Configuraciones iniciales para el S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Configuraciones iniciales para el S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
 ip add 192.168.3.11 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.3.1
end
```

Paso 6: Configurar una tabla de hosts IP en el router LOCAL

La tabla de hosts IP le permite utilizar un nombre de host para conectarse a un dispositivo remoto en lugar de una dirección IP. La tabla de hosts proporciona la resolución de nombres para el dispositivo con las siguientes configuraciones. Copie y pegue las siguientes configuraciones para el router LOCAL. Estas configuraciones le permitirán usar los nombres de host para los comandos **ping** y **traceroute** en el router LOCAL.

```
ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end
```

Parte 2: Utilizar el comando ping para realizar pruebas de red básicas

En la parte 2 de esta práctica de laboratorio, utilice el comando **ping** para verificar la conectividad de extremo a extremo. Ping opera mediante el envío de paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al host de destino y la espera de una respuesta del ICMP. Puede registrar el tiempo de ida y vuelta y la pérdida de paquetes.

Inspeccionará los resultados con el comando **ping** y las opciones de ping adicionales que están disponibles en las PC con Windows y en los dispositivos Cisco.

Paso 1: Probar la conectividad de red desde la red LOCAL por medio de la PC-A

Todos los pings de la PC-A a otros dispositivos en la topología deben realizarse correctamente. De lo contrario, revise la topología y el cableado, así como la configuración de los dispositivos Cisco y las PC.

- a. Haga ping de la PC-A al gateway predeterminado (la interfaz GigabitEthernet 0/1 del router LOCAL).

```
C:\Users\User1> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En este ejemplo, se enviaron cuatro (4) solicitudes de ICMP, de 32 bytes cada una, y las respuestas se recibieron en menos de un milisegundo sin pérdida de paquetes. El tiempo de transmisión y respuesta aumenta a medida que se procesan las solicitudes y respuestas de ICMP a través de más dispositivos en el trayecto hasta el destino final y desde este.

- b. Desde la PC-A, haga ping a las direcciones que se indican en la tabla siguiente y registre el tiempo de ida y vuelta promedio y el tiempo de vida (TTL).

Destino	Tiempo promedio de ida y vuelta (ms)	TTL
192.168.1.1 (LOCAL)	0	255
192.168.1.11 (S1)	0*	255
10.1.1.1 (LOCAL)	0	255
10.1.1.2 (ISP)	20	254
10.2.2.2 (ISP)	20	254
10.2.2.1 (REMOTE)	40	253
192.168.3.1 (REMOTE)	40	253
192.168.3.11 (S3)	40*	252
192.168.3.3 (PC-C)	40	125

***Nota para el instructor:** si apareció el mensaje “Tiempo de espera agotado” durante la primera solicitud de ICMP, se produjo un aumento del tiempo de ida y vuelta promedio. La demora se debió al protocolo ARP, y esto tuvo como resultado la pérdida de paquetes.

Observe el viaje promedio de ida y vuelta para 192.168.3.3 (PC-C). El tiempo aumentó porque las solicitudes de ICMP fueron procesadas por tres routers antes de que la PC-A recibiera la respuesta de la PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
```

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Paso 2: Utilizar los comandos de ping extendido en una PC

El comando **ping** predeterminado envía cuatro solicitudes a 32 bytes cada una. Espera la devolución de cada respuesta 4000 milisegundos (cuatro segundos) y luego muestra el mensaje "Tiempo de espera agotado". El comando **ping** se puede ajustar para resolver los problemas de una red.

- En el símbolo del sistema, escriba **ping** y presione Entrar.

```
C:\Users\User1> ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t           Ping the specified host until stopped.
                  To see statistics and continue - type Control-Break;
                  To stop - type Control-C.
    -a           Resolve addresses to hostnames.
    -n count     Number of echo requests to send.
    -l size      Send buffer size.
    -f           Set Don't Fragment flag in packet (IPv4-only).
    -i TTL       Time To Live.
    -v TOS       Type Of Service (IPv4-only. This setting has been deprecated
                  and has no effect on the type of service field in the IP Header).
    -r count     Record route for count hops (IPv4-only).
    -s count     Timestamp for count hops (IPv4-only).
    -j host-list Loose source route along host-list (IPv4-only).
    -k host-list Strict source route along host-list (IPv4-only).
    -w timeout   Timeout in milliseconds to wait for each reply.
    -R           Use routing header to test reverse route also (IPv6-only).
    -S srcaddr   Source address to use.
    -4           Force using IPv4.
    -6           Force using IPv6.
```

- Mediante la opción **-t**, haga ping a la PC-C para verificar que haya posibilidad de conexión con ella.

```
C:\Users\User1> ping -t 192.168.3.3
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

Para ilustrar los resultados cuando no hay posibilidad de conexión a un host, desconecte el cable entre el router REMOTE y el switch S3 o desactive la interfaz GigabitEthernet 0/1 en el router REMOTE.

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
```

```
Reply from 192.168.1.3: Destination host unreachable.
```

```
Reply from 192.168.1.3: Destination host unreachable.
```

Mientras la red funciona correctamente, el comando **ping** puede determinar si el destino respondió y cuánto tardó en recibir una respuesta del destino. Si existe un problema de conectividad de red, el comando **ping** muestra un mensaje de error.

- c. Vuelva a conectar el cable Ethernet o habilite la interfaz GigabitEthernet en el router REMOTE (mediante el comando **no shutdown**) antes de continuar con el paso siguiente. Después de 30 segundos, el ping debe volver a ser correcto.

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
```

```
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

- d. Presione **Ctrl+C** para detener el comando ping.

Paso 3: Probar la conectividad de red desde la red LOCAL por medio de dispositivos Cisco

El comando **ping** también está disponible en los dispositivos Cisco. En este paso, el comando **ping** se examina por medio del router LOCAL y el switch S1.

- a. Haga ping a la PC-C en la red REMOTE utilizando la dirección IP 192.168.3.3 desde el router LOCAL.

```
LOCAL# ping 192.168.3.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

El signo de exclamación (!) indica que el ping desde el router LOCAL hasta la PC-C se realizó correctamente. El tiempo promedio de ida y vuelta es de 64 ms sin pérdida de paquetes, según lo indica la tasa de éxito del 100%.

- b. Dado que se configuró una tabla de hosts locales en el router LOCAL, puede hacer ping a la PC-C en la red REMOTE utilizando el nombre de host configurado desde el router LOCAL.

```
LOCAL# ping PC-C
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- c. Hay más opciones disponibles para el comando **ping**. En la CLI, escriba **ping** y presione Entrar. Introduzca **192.168.3.3** o **PC-C** para Target IP address (Dirección IP de destino). Presione Entrar para aceptar el valor predeterminado para otras opciones.

```
LOCAL# ping
```

```
Protocol [ip]:
```

```
Target IP address: PC-C
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- d. Puede utilizar un ping extendido para tareas de observación cuando hay un problema de red. Inicie el comando **ping** a 192.168.3.3 con un conteo de repetición de 500. Luego, desconecte el cable entre el router REMOTE y el switch S3 o desactive la interfaz GigabitEthernet 0/1 en el router REMOTE.

Vuelva a conectar el cable Ethernet o habilite la interfaz GigabitEthernet en el router REMOTE después de reemplazar los signos de exclamación (!) por la letra U y puntos (.). Después de 30 segundos, el ping debe volver a ser correcto. Si lo desea, presione **Ctrl+Mayús+6** para detener el comando **ping**.

```
LOCAL# ping
Protocol [ip]:
Target IP address: 192.168.3.3
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!U.....
....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/63/72 ms
```

La letra U en los resultados indica que no hay posibilidad de conexión a un destino. El router LOCAL recibió una unidad de datos del protocolo (PDU) de error. Cada punto (.) en el resultado indica que el tiempo de espera del ping se agotó mientras se esperaba una respuesta de la PC-C. En este ejemplo, se perdió el 5% de los paquetes durante la interrupción de red simulada.

Nota: también puede utilizar el comando siguiente para obtener los mismos resultados:

```
LOCAL# ping 192.168.3.3 repeat 500

o

LOCAL# ping PC-C repeat 500
```

- e. También puede probar la conectividad de red con un switch. En este ejemplo, el switch S1 hace ping al switch S3 en la red REMOTE.

```
S1# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/67/68 ms
```

El comando **ping** es extremadamente útil al resolver problemas en la conectividad de red. Sin embargo, no puede indicar la ubicación del problema cuando un ping no se realiza correctamente. El comando **tracert** (o **tracert**) puede mostrar la latencia de red e información sobre la ruta.

Parte 3: Utilizar los comandos **tracert** y **tracert** para realizar pruebas de red básicas

En las PC y los dispositivos de red, existen comandos para rastrear las rutas. En las PC con Windows, el comando **tracert** utiliza mensajes de ICMP para rastrear la ruta hacia el destino final. En dispositivos Cisco y PC del estilo de Unix, el comando **tracert** utiliza los datagramas del protocolo de datagramas de usuario (UDP) para rastrear las rutas hacia el destino final.

En la parte 3, examinará los comandos **tracert** y determinará la ruta de un paquete hasta el destino final. Utilizará el comando **tracert** en las PC con Windows y el comando **tracert** en los dispositivos Cisco. También analizará las opciones disponibles para ajustar los resultados de **tracert**.

Paso 1: Utilizar el comando **tracert** de la PC-A a la PC-C

- a. En el símbolo del sistema, escriba **tracert 192.168.3.3**.

```
C:\Users\User1> tracert 192.168.3.3
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    PC-C [192.168.3.3]
```

Trace complete.

Los resultados de **tracert** indican que la ruta de la PC-A a la PC-C va de la PC-A a LOCAL, a ISP, a REMOTE y a la PC-C. La ruta a la PC-C pasó por tres saltos de router hasta llegar el destino final en la PC-C.

Paso 2: Explorar opciones adicionales para el comando **tracert**

- a. En el símbolo del sistema, escriba **tracert** y presione Entrar.

```
C:\Users\User1> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

-d	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target.
-j host-list	Loose source route along host-list (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.
-6	Force using IPv6.

- b. Utilice la opción **-d**. Observe que la dirección IP 192.168.3.3 no se resolvió como PC-C.

```
C:\Users\User1> tracert -d 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    192.168.3.3

Trace complete.
```

Paso 3: Utilizar el comando traceroute del router LOCAL a la PC-C

- a. En la petición de entrada de comandos del router local, escriba **traceroute 192.168.3.3** o **traceroute PC-C**. Los nombres de host se resuelven porque se configuró una tabla de hosts IP locales en el router LOCAL.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
 1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
 2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
 3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec

LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
 1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
 2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
 3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Paso 4: Utilizar el comando traceroute del switch S1 a la PC-C

- a. En el switch S1, escriba **traceroute 192.168.3.3**. Los nombres de host no se muestran en los resultados del comando traceroute porque no se configuró una tabla de hosts IP locales en este switch.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.1.1 1007 msec 0 msec 0 msec
 2 10.1.1.2 17 msec 17 msec 16 msec
 3 10.2.2.1 34 msec 33 msec 26 msec
 4 192.168.3.3 33 msec 34 msec 33 msec
```

El comando **traceroute** tiene opciones adicionales. Puede utilizar **?** o simplemente presionar Entrar después de escribir **traceroute** en la petición de entrada para explorar estas opciones.

El enlace siguiente proporciona más información acerca de los comandos **ping** y **traceroute** para dispositivos Cisco:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Parte 4: Resolver problemas de la topología

Paso 1: Borrar las configuraciones en el router REMOTE

Paso 2: Volver a cargar el router REMOTE

Paso 3: Copiar y pegar la siguiente configuración en el router REMOTE

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
  ip address 10.2.2.1 255.255.255.252
  no shutdown
interface g0/1
  ip add 192.168.8.1 255.255.255.0
  no shutdown
router eigrp 1
  network 10.2.2.0 0.0.0.3
  network 192.168.3.0 0.0.0.255
  no auto-summary
end
```

Paso 4: Desde la red LOCAL, utilizar los comandos ping y tracert o traceroute para resolver y corregir problemas en la red REMOTE

- a. Utilice los comandos **ping** y **tracert** desde la PC-A.

Puede utilizar el comando **tracert** para determinar la conectividad de red de extremo a extremo. Este resultado de tracert indica que la PC-A puede conectarse a su gateway predeterminado 192.168.1.1, pero no tiene conectividad de red con la PC-C.

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to 192.168.3.3 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2  192.168.1.1  reports: Destination host unreachable.
```

```
Trace complete.
```

Una manera de localizar el problema de la red es hacer ping a cada salto en la red hacia la PC-C. Determine primero si la PC-A tiene posibilidad de conexión a la interfaz Serial 0/0/1 del router ISP con la dirección IP 10.2.2.2.

```
C:\Users\Utraser1> ping 10.2.2.2
```

```
Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
```

```
Ping statistics for 10.2.2.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

El ping se realizó correctamente para el router ISP. El salto siguiente en la red es el router REMOTE. Haga ping a la interfaz Serial 0/0/1 del router REMOTE con la dirección IP 10.2.2.1.

```
C:\Users\User1> ping 10.2.2.1
```

```
Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
```

```
Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

La PC-A tiene posibilidad de conexión al router REMOTE. Según los resultados correctos del ping de la PC-A al router REMOTE, el problema de conectividad de red es con la red 192.168.3.0/24. Haga ping al gateway predeterminado de la PC-C, que es la interfaz GigabitEthernet 0/1 del router REMOTE.

```
C:\Users\User1> ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

La PC-A no tiene posibilidad de conexión a la interfaz GigabitEthernet 0/1 del router REMOTE, tal como lo muestran los resultados del comando **ping**.

También se puede hacer ping al switch S3 desde la PC-A para verificar la ubicación del problema de conectividad de red escribiendo **ping 192.168.3.11** en el símbolo del sistema. Dado que la PC-A no tiene posibilidad de conexión a la interfaz GigabitEthernet 0/1 del router REMOTE, es probable que la PC-A no pueda hacer ping al switch S3 correctamente, como lo indican los siguientes resultados.

```
C:\Users\User1> ping 192.168.3.11
```

```
Pinging 192.168.3.11 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Mediante los resultados de `tracert` y `ping`, se concluye que la PC-A tiene posibilidad de conexión a los routers LOCAL, ISP y REMOTE, pero no a la PC-C, el switch S3 ni el gateway predeterminado para la PC-C.

- b. Utilice los comandos **show** para examinar las configuraciones en ejecución del router REMOTE.

```
REMOTE# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.8.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	10.2.2.1	YES	manual	up	up

```
REMOTE# show run
<resultado omitido>
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.8.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  ip address 10.2.2.1 255.255.255.252
<resultado omitido>
```

Los resultados de los comandos **show run** y **show ip interface brief** indican que el estado de la interfaz GigabitEthernet 0/1 es up/up (activo/activo), pero se configuró con una dirección IP incorrecta.

- c. Corrija la dirección IP para GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

- d. Verifique que la PC-A pueda hacer ping y `tracert` a la PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
```

```
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 44ms, Average = 41ms
```

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	24 ms	24 ms	24 ms	10.1.1.2
3	48 ms	48 ms	48 ms	10.2.2.1
4	59 ms	59 ms	59 ms	PC-C [192.168.3.3]

```
Trace complete.
```

Nota: esto también se puede lograr mediante los comandos **ping** y **tracert** desde la CLI en el router LOCAL y el switch S1 después de verificar que no haya problemas de conectividad de red en la red 192.168.1.0/24.

Reflexión

1. ¿Qué podría evitar que las respuestas de los comandos ping o traceroute lleguen al dispositivo de origen, además de problemas de conectividad de red?

Un firewall en las PC, el comando de listas de acceso, problemas de enrutamiento, la interfaz no funciona, demoras en la red.

2. Si hace ping a una dirección inexistente en la red remota, como 192.168.3.4, ¿qué mensaje mostrará el comando **ping**? ¿Qué significa esto? Si hace ping a una dirección de host válida y recibe esta respuesta, ¿qué debe revisar?

Tiempo de espera agotado o puntos (.). Significa que no hubo respuesta en el período predeterminado. Algunos elementos que se pueden revisar: si el router no funciona, si el host de destino no funciona, la ruta de retorno al dispositivo y si la latencia de la respuesta no supera el período predeterminado.

3. Si hace ping a una dirección que no existe en ninguna red de la topología, como 192.168.5.3, desde una PC con Windows, qué mensaje que mostrará el comando **ping**? ¿Qué significa este mensaje?

Host de destino inalcanzable. Este mensaje indica que no hay una ruta hacia el destino, debido a que la red no se encuentra en la tabla de enrutamiento.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Configuraciones de dispositivos

LOCAL del router

```
LOCAL# show running-config
Building configuration...
```

```
Current configuration : 1462 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname LOCAL
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 15
!
!
```



```
!  
!  
!  
!  
!  
no ip domain lookup  
ip host REMOTE 10.2.2.1 192.168.3.1  
ip host ISP 10.1.1.2 10.2.2.2  
ip host LOCAL 192.168.1.1 10.1.1.1  
ip host PC-C 192.168.3.3  
ip host PC-A 192.168.1.3  
ip host S1 192.168.1.11  
ip host S3 192.168.3.11  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
ip address 10.1.1.1 255.255.255.252  
clock rate 56000  
!  
interface Serial0/0/1  
no ip address  
shutdown
```

```
!  
!  
router eigrp 1  
  network 10.1.1.0 0.0.0.3  
  network 192.168.1.0  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login  
  transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

ROUTER ISP

```
ISP# show running-config  
Building configuration...  
  
Current configuration : 1265 bytes  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname ISP
```

```
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
memory-size iomem 15  
!  
!  
!  
!  
!  
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto
```

```
!  
interface Serial0/0/0  
 ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/0/1  
 ip address 10.2.2.2 255.255.255.252  
 clock rate 56000  
!  
!  
router eigrp 1  
 network 10.1.1.0 0.0.0.3  
 network 10.2.2.0 0.0.0.3  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
 no activation-character  
 no exec  
 transport preferred none  
 transport input all  
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
 stopbits 1  
line vty 0 4  
 login  
 transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

REMOTE del router

```
REMOTE# show running-config
```

Building configuration...

Current configuration : 1440 bytes

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname REMOTE  
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
memory-size iomem 10  
!  
!  
!  
!  
!  
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0
```

```
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
!
!
router eigrp 1
network 10.2.2.0 0.0.0.3
network 192.168.3.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
```

```
line vty 0 4
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1# show running-config
Building configuration...

Current configuration : 1565 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
!  
!  
!  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!
```



```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
!
!
 line con 0
 line vty 5 15
!
end
```

Switch S3

```
S3# show running-config
Building configuration...

Current configuration : 1563 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
!
```

```
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
```

```
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.3.11 255.255.255.0
!
 ip default-gateway 192.168.3.1
 ip http server
 ip http secure-server
!
!
 line con 0
 line vty 5 15
!
end
```

Internet de todo, por supuesto (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la necesidad de direcciones de red IPv6.

Esta es una actividad basada en una aplicación. Los estudiantes desarrollan un plan para demostrar cómo podrían utilizarse las transmisiones multicast, las transmisiones unicast y las subredes de IdT en la vida cotidiana para modificar la comunicación de datos.

Información básica/Situación

(Nota: esta actividad se puede completar en forma individual o en grupos pequeños o grandes).

En este capítulo, se analizaron las formas en que las pequeñas y medianas empresas están conectadas a redes en grupos. Al principio de este capítulo, se presentó el IdT en la actividad de creación de modelos.

Para esta actividad, elija una de las siguientes opciones:

- Servicios bancarios en línea
- Noticias del mundo
- Pronóstico meteorológico/clima
- Condiciones del tráfico

Elabore un esquema de direccionamiento IPv6 para el área que eligió. El esquema de direccionamiento debe incluir la forma en que planearía lo siguiente:

- División en subredes
- Transmisiones unicast
- Transmisiones multicast

Conserve una copia del esquema para compartir con la clase o la comunidad de aprendizaje. Esté preparado para explicar lo siguiente:

- Cómo podrían incorporarse la división en subredes, las transmisiones unicast y las transmisiones multicast.
- Dónde podría utilizarse el esquema de direccionamiento.
- Cómo se verían afectadas las pequeñas y medianas empresas al utilizar el plan.

Nota para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a reflexionar acerca de sus percepciones respecto de la forma en que una red podría utilizar IPv6 y los sextillones de direcciones disponibles para la práctica tanto personal como corporativa. Como resultado de esta actividad, los instructores deben facilitar un debate en clase para el intercambio de ideas.

Recursos necesarios

- Papel, lápices o lapiceras, o tablet PC
- Packet Tracer (si desea mostrar cómo se vería su red físicamente)
- Copias impresas o electrónicas de la topología de la red final con direccionamiento IPv6 indicadas para compartir con la clase

Reflexión

1. ¿Cuál fue la parte más difícil del diseño de este modelo de red? Justifique su respuesta.

Las respuestas varían en los grupos (como las topologías desarrolladas). Algunos estudiantes pueden mencionar el diseño de un grupo principal y luego de grupos en subredes a partir del grupo principal, otros pueden indicar el direccionamiento real de la red y otros pueden indicar que tuvieron problemas en cuanto al lugar donde pudieron producirse transmisiones unicast y transmisiones multicast.

Una solución posible para la situación podría incluir:

Pronóstico meteorológico/clima

El área donde vive tiene muchos días de calor durante los meses de verano. Los costos de la electricidad se disparan en esos días.

Su área eléctrica local incluye seis ciudades locales, y todas estas ciudades luego integran un estado grande. Varios estados integran un país grande. Para reducir los costos y aumentar la productividad de la electricidad, podría instalar molinos de viento o paneles solares que generarían corriente eléctrica para su área inmediata y áreas geográficas más grandes. Los molinos de viento o los paneles solares podrían controlarse mediante la accesibilidad a la red.

Al utilizar un esquema de direccionamiento IPv6:

- Se asignaría una dirección IPv6 a cada molino de viento (o panel solar).
- Los molinos de viento o los paneles solares se encenderían para generar electricidad por ciudad, estado o país (división en subredes).
- Las ciudades, los estados o los países recibirán electricidad adicional según el funcionamiento de las transmisiones unicast o multicast de los molinos de viento o paneles solares.

(Nota: según el enfoque o el uso de esta actividad, los estudiantes podrán diseñar efectivamente un esquema de molinos de viento o paneles solares y utilizarlos para demostrar el dominio del concepto de división en subredes. También podrán agrupar los molinos de viento o los paneles solares para mostrar los tipos de transmisiones de unicast y multicast).

Entre otras situaciones posibles, podrían incluirse las siguientes:

1. Eficiencia energética

- Cada lámpara doméstica podría conectarse a la red y administrarse en forma remota. Por lo tanto, cada una necesitaría una dirección IPv6.

- Cada electrodoméstico también se conectaría a la red y también necesitaría una dirección IPv6.

- La estructura de red podría agrupar todos los artefactos del hogar en una subred. Se podrían crear resúmenes de las rutas para agrupar los vecindarios. Se utilizarían mensajes de transmisión unicast para administrar dispositivos únicos. Los artefactos del mismo tipo podrían tener un grupo multicast (todos los televisores, por ejemplo) y administrarse a granel.

2. Pronóstico meteorológico

- El sensor en los árboles necesitaría direcciones IPv6 para conectarse a la red.
- Las estaciones meteorológicas móviles también necesitarían IPv6 (varias estaciones por ciudad, para lograr precisión).
- Las estaciones meteorológicas flotantes reunirían información sobre los océanos y ríos, y también necesitarían IPv6.
- Una vez más, los resúmenes de rutas agruparían y representarían ubicaciones físicas. Podrían crearse grupos multicast según la ubicación de la estación (tierra, río y océano) y utilizarse direcciones unicast para administrar una estación específica.

3. Condiciones del tráfico

- Cada semáforo necesitaría una dirección IPv6 para conectarse a la red.
- Los sensores de tráfico de los caminos (para proporcionar el índice de vehículos por minuto) también podrían conectarse a la red y necesitarían direcciones IPv6.
- Podrían crearse grupos multicast según el tipo de dispositivo (sensor o semáforo) y podrían usarse direcciones unicast para administrar un dispositivo específico.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Internet de todo (IdT): tecnología ecológica
- División en subredes
- Direccionamiento IPv6
- Transmisiones unicast
- Transmisiones multicast

Lláname (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar por qué es necesario el enrutamiento para que los hosts que se encuentran en diferentes subredes puedan comunicarse.

- Los estudiantes reconocerán que los datos se entregan más rápido si se utilizan identificadores de direccionamiento de grupo.
- Los estudiantes verán la forma en que se facilita la comunicación al proporcionar grupos grandes para luego dividirlos en partes más manejables. Después de reflexionar acerca de la forma en que se divide su número de teléfono fijo o celular smartphone, pueden obtener inferencias acerca de la forma en que las redes emplean las mismas prácticas.

Información básica/Situación

En este capítulo, aprenderá cómo se pueden agrupar los dispositivos de una red grande en subredes o grupos de redes más pequeños.

En esta actividad de creación de modelos, deberá pensar en un número que probablemente utilice a diario, como su número de teléfono. A medida que complete la actividad, piense en qué forma su número de teléfono es comparable con las estrategias que los administradores de red pueden utilizar para identificar hosts a fin de lograr una comunicación eficaz de datos.

Complete las dos secciones que se indican a continuación y registre las respuestas. Conserve una copia impresa o electrónica de las dos secciones para analizarlas más adelante en clase.

- Explique la forma en que su número de teléfono móvil o fijo se divide en grupos para su identificación. ¿Su número de teléfono posee código de área, identificador ISP o prefijo de ciudad, estado o país?
- ¿De qué manera la separación del número de teléfono en partes organizadas ayuda a contactarse y comunicarse con otras personas?

Nota para el instructor: esta es una actividad de creación de modelos para realizar en forma individual o en clase, en grupos pequeños o grandes. No tiene como fin ser una asignación con calificación. El objetivo es motivar a los estudiantes a que reflexionen acerca de su conocimiento actual de la forma en que las redes se agrupan utilizando una base numérica. Como resultado de esta actividad, se facilitará el debate.

Nota para el instructor: los estudiantes deben ajustar sus respuestas de manera que incorporen un código de área de país, si fuera necesario.

Recursos necesarios

- Capacidades de registro (papel, tablet PC, etc.) para compartir los comentarios de reflexión con la clase.

Reflexión

1. ¿Por qué piensa que los ISP necesitan su número de teléfono cuando configuraran los parámetros de su cuenta?
-

Ejemplo de número de teléfono y grupos de identificación en ese número (si en su país se utiliza otro identificador, este debe incluirse en las respuestas de esta sección):

Código de área (o identificador ISP)	Ciudad	Identificador de teléfono
571	555	1212

El 571 dirige las llamadas desde mi teléfono y muestra la ubicación geográfica general de mi ISP o estado. Si quiero llamar a alguien que se encuentra en otro estado o a través de un ISP diferente, el código de área o identificador ISP será distinto.

El 555 indica la ciudad desde la cual realizo la llamada y permite enrutar las comunicaciones a los switches o routers correctos.

El 1212 indica mi identificación personal de teléfono fijo o celular smartphone cuando se combina con los dos primeros grupos. Así, mi teléfono puede recibir la comunicación después de que se procesa; por lo general, a través de los indicadores de código de área/ISP y ciudad.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Cuando se utilizan esquemas de direccionamiento, se emplean jerarquías.
- La conectividad se ve influenciada por los identificadores de los esquemas de direccionamiento.

Práctica de laboratorio: Investigación de calculadoras de subredes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Hacer una revisión de las calculadoras de subredes disponibles

Parte 2: Realizar cálculos de red mediante una calculadora de subredes

Información básica/Situación

Si bien es importante entender cómo convertir una dirección IP decimal a su formato binario y aplicar la operación AND bit a bit para determinar la dirección de red, se trata de un proceso tedioso y propenso a errores. Para obtener ayuda con estos cálculos, muchos administradores de red utilizan programas con utilidades de calculadora de subredes IP. Se desarrollaron varios programas de este tipo, que pueden descargarse de Internet o ejecutarse directamente allí.

En esta práctica de laboratorio, se presentarán algunas de las calculadoras de subredes IP gratuitas disponibles. También se utilizará una calculadora de subredes IP basada en la Web para realizar las operaciones de red.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Hacer una revisión de las calculadoras de subredes disponibles

En la parte 1, se presentan dos tipos de calculadoras de subredes: basadas en el cliente (programas que se descargan e instalan) y basadas en la Web (utilidades que se ejecutan desde un explorador).

Paso 1: Hacer una revisión de las calculadoras de subredes basadas en el cliente

Solarwinds proporciona una calculadora de subredes gratuita que puede descargarse e instalarse en una PC con sistema operativo Windows. Para poder descargar este programa, se le pedirá que proporcione información personal (nombre, compañía, ubicación, dirección de correo electrónico y número de teléfono). Para descargar e instalar la calculadora de subredes de Solarwinds, visite www.solarwinds.com.

Si tiene una PC con Linux, se recomienda que use la utilidad **ipcalc** (disponible con la mayoría de las distribuciones de Linux). Utilice el comando **apt-get install ipcalc** para instalar ipcalc en una PC con Linux.

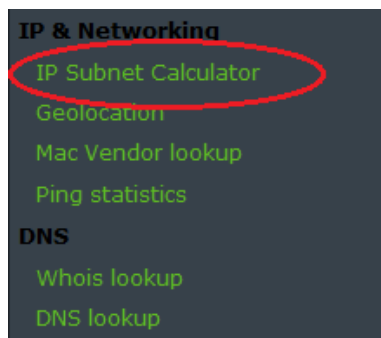
Paso 2: Utilizar una calculadora de subredes basada en la Web

Las calculadoras de subredes basadas en la Web no requieren instalación, pero es necesario tener acceso a Internet para poder usarlas. Se puede acceder a la siguiente calculadora de subredes basada en la Web desde cualquier dispositivo que tenga acceso a Internet, incluidos los smartphones y las tablet PC.

- Con el explorador, acceda a www.ipcalc.org y haga clic en el enlace **IP Subnet Calculator** (Calculadora de subredes IP).

Nota: en el menú, también se incluyen varias utilidades prácticas más, como Mac Vendor lookup (Búsqueda de proveedores MAC), Whois lookup (Búsqueda de Whois) y DNS lookup (búsqueda de DNS).

Nota: en el momento en que se redactó este documento, se encontró un problema de formato de página al acceder al sitio Web www.ipcalc.org con Internet Explorer (versión 9). Si bien el sitio funcionaba correctamente, tal vez prefiera usar otro explorador (Firefox o Chrome) para acceder al sitio.



- b. En la pantalla de la calculadora de subredes IP, introduzca una dirección IP y una máscara de subred o una dirección IP y una notación de prefijo CIDR. En el área Introduction (Introducción), se muestran ejemplos de cómo introducir cada uno de estos valores.

:: IP Subnet Calculator ::

Introduction:

A subnet is a logically visible subdivision of an IP network. The practice of dividing a network into subnetworks is called subnetting.

This application will help you to compute information about IP subnetting. It's easy to use.

In the following form you can enter differents address format:

Description	Format
IP & CIDR Netmask	10.0.0.1/22
IP & Netmask	10.0.0.1 255.255.252.0
IP & Wildcard Mask	10.0.0.1 0.0.3.255

The behavior of this application is the same that the *ipcalc* binary of GNU/Linux system's !

Application:

Enter IP & Mask or CIDR here !

- c. En el campo Application (Aplicación), introduzca **192.168.50.50/27** y haga clic en **Calc!** (Calcular). En la pantalla siguiente, se muestra una tabla con información sobre la red, tanto en formato decimal como binario.

Application:

192.168.50.50/27

Description	Value	Extra
Address	192.168.50.50	11000000.10101000.00110010.00110010
Netmask	255.255.255.224	11111111.11111111.11111111.11100000 /27
Network	192.168.50.32	11000000.10101000.00110010.00100000
Broadcast	192.168.50.63	
Host min	192.168.50.33	11000000.10101000.00110010.00100001
Host max	192.168.50.62	11000000.10101000.00110010.00111110
Host/net	30	Class C, Private Internet

d. Con la información proporcionada en el ejemplo anterior, responda las siguientes preguntas.

¿Cuál es la dirección de red? _____ 192.168.50.32

¿Cuál es la máscara de subred? _____ 255.255.255.224

¿Cuántos hosts admitirá esta red? _____ 30

¿Cuál es la dirección de host más baja? _____ 192.168.50.33

¿Cuál es la dirección de host más alta? _____ 192.168.50.62

¿Cuál es la dirección de broadcast? _____ 192.168.50.63

Parte 2: Realizar cálculos de red mediante una calculadora de subredes

En la parte 2, utilice la calculadora de subredes basada en la Web de www.ipcalc.org para completar las tablas que se proporcionan.

Paso 1: Complete la siguiente tabla para la dirección 10.223.23.136/10:

Descripción	Decimal	Binario
Dirección	10.223.23.136	00001010.11011111.00010111.10001000
máscara de subred	255.192.0.0	11111111.11000000.00000000.00000000
Dirección de red	10.192.0.0	00001010.11000000.00000000.00000000
Dirección de broadcast	10.255.255.255	00001010.11111111.11111111.11111111
Primera dirección de host	10.192.0.1	00001010.11000000.00000000.00000001
Última dirección de host	10.255.255.254	00001010.11111111.11111111.11111110
Cantidad de hosts disponibles	4,194,302	No aplicable

¿Qué tipo de dirección: pública o privada? _____ Privada

Paso 2: Complete la siguiente tabla para la dirección 172.18.255.92 con una máscara de subred 255.255.224.0:

Descripción	Decimal	Binario
Dirección	172.18.255.92	10101100.00010010.11111111.01011100
máscara de subred	255.255.224.0	11111111.11111111.11100000.00000000
Dirección de red	172.18.224.0	10101100.00010010.11100000.00000000
Dirección de broadcast	172.18.255.255	10101100.00010010.11111111.11111111
Primera dirección de host	172.18.224.1	10101100.00010010.11100000.00000001
Última dirección de host	172.18.255.254	10101100.00010010.11111111.11111110
Cantidad de hosts disponibles	8190	No aplicable

¿Cuál es la notación de prefijo CIDR para esta red? _____ /19

¿Qué tipo de dirección: pública o privada? _____ Privada

Paso 3: Complete la siguiente tabla utilizando la dirección 192.168.184.78 con una máscara de subred 255.255.255.252:

Descripción	Decimal	Binario
Dirección	192.168.184.78	11000000.10101000.10111000.01001110
máscara de subred	255.255.255.252	11111111.11111111.11111111.11111100
Dirección de red	192.168.184.76	11000000.10101000.10111000.01001100
Dirección de broadcast	192.168.184.79	11000000.10101000.10111000.01001111
Primera dirección de host	192.168.184.77	11000000.10101000.10111000.01001101
Última dirección de host	192.168.184.78	11000000.10101000.10111000.01001110
Cantidad de hosts disponibles	2	No aplicable

¿Cuál es la notación de prefijo CIDR para esta red? _____ /30

¿Qué tipo de dirección: pública o privada? _____ Privada

¿Dónde es más probable que encuentre una red como la que se está usando?

Las respuestas pueden variar, pero un buen uso para una red /30 es el enlace serial entre dos routers. Solo se necesitan dos direcciones de host para este tipo de enlace.

Paso 4: Complete la siguiente tabla para la dirección 209.165.200.225/27:

Descripción	Decimal	Binario
Dirección	209.165.200.225	11010001.10100101.11001000.11100001
máscara de subred	255.255.255.224	11111111.11111111.11111111.11100000
Dirección de red	209.165.200.224	11010001.10100101.11001000.11100000
Dirección de broadcast	209.165.200.255	11010001.10100101.11001000.11111111
Primera dirección de host	209.165.200.225	11010001.10100101.11001000.11100001
Última dirección de host	209.165.200.254	11010001.10100101.11001000.11111110
Cantidad de hosts disponibles	30	No aplicable

¿Qué tipo de dirección: pública o privada? _____ Pública

Paso 5: Complete la siguiente tabla para la dirección 64.104.110.7/20:

Descripción	Decimal	Binario
Dirección	64.104.110.7	01000000.01101000.01101110.00000111
máscara de subred	255.255.240.0	11111111.11111111.11110000.00000000
Dirección de red	64.104.96.0	01000000.01101000.01100000.00000000
Dirección de broadcast	64.104.111.255	01000000.01101000.01101111.11111111
Primera dirección de host	64.104.96.1	01000000.01101000.01100000.00000001
Última dirección de host	64.104.111.254	01000000.01101000.01101111.11111110
Cantidad de hosts disponibles	4096	No aplicable

¿Qué tipo de dirección: pública o privada? _____ Pública

Reflexión

1. Indique una ventaja de utilizar una calculadora de subredes basada en el cliente.

Las respuestas pueden variar. Las calculadoras de subredes basadas en el cliente no requieren acceso a Internet.

2. Indique una ventaja de utilizar una calculadora de subredes basada en la Web.

Las respuestas pueden variar, pero las calculadoras de subredes basadas en la Web no requieren descarga ni instalación. Se puede acceder a ellas desde cualquier dispositivo con acceso a Internet, incluso dispositivos móviles como smartphones o tablet PC.

Práctica de laboratorio: Cálculo de subredes IPv4

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Determinar la división en subredes de la dirección IPv4

- identificar la dirección de red.
- Determinar la dirección de broadcast.
- Determinar la cantidad de hosts.

Parte 2: Calcular la división en subredes de la dirección IPv4

- Determinar la cantidad de subredes creadas.
- Determinar la cantidad de hosts por subred.
- Determinar la dirección de subred.
- Determinar el rango de hosts para la subred.
- Determinar la dirección de broadcast para la subred.

Información básica/Situación

La capacidad de trabajar con subredes IPv4 y de determinar la información de red y host sobre la base de una dirección IP y una máscara de subred determinadas es fundamental para comprender la forma en que funcionan las redes IPv4. La primera parte se diseñó para reforzar el conocimiento de la forma de calcular la información de dirección IP de una red a partir de una dirección IP y una máscara de subred determinadas. Al tener una dirección IP y una máscara de subred específicas, podrá determinar información adicional sobre la subred, por ejemplo:

- Dirección de red
- Dirección de broadcast
- Cantidad total de bits de host
- Cantidad de hosts por subred

En la segunda parte de la práctica de laboratorio, determinará la información siguiente para una dirección IP y una máscara de subred:

- Dirección de red de esta subred
- Dirección de broadcast de esta subred
- Rango de direcciones de host para esta subred
- Cantidad de subredes creadas
- Cantidad de hosts para cada subred

Nota para el instructor: esta actividad puede realizarse en clase o asignarse como tarea para el hogar. Si se realiza en clase, tal vez prefiera que los estudiantes trabajen solos o de a dos. Se sugiere resolver el primer problema todos juntos en clase, para orientar a los estudiantes sobre cómo proceder con el resto del trabajo.

Las direcciones IP públicas que se utilizan en esta práctica de laboratorio son propiedad de Cisco.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con acceso a Internet)
- Opcional: calculadora de direcciones IPv4

Parte 1: Determinar la división en subredes de la dirección IPv4

En la parte 1, determinará las direcciones de red y de broadcast, así como la cantidad de hosts, dada una dirección IPv4 y una máscara de subred.

REPASO: para determinar la dirección de red, realice la operación AND binaria en la dirección IPv4 utilizando la máscara de subred que se proporciona. El resultado será la dirección de red. Sugerencia: si la máscara de subred tiene el valor decimal 255 en un octeto, el resultado SIEMPRE será el valor original de ese octeto. Si la máscara de subred tiene el valor decimal 0 en un octeto, el resultado SIEMPRE será 0 para ese octeto.

Ejemplo:

Dirección IP	192.168.10.10
Máscara de subred	255.255.255.0
	=====
Resultado (red)	192.168.10.0

Al saber esto, es posible que solo tenga que realizar una operación AND binaria en un octeto que no tenga 255 o 0 en la porción de máscara de subred.

Ejemplo:

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0

Al analizar este ejemplo, puede ver que solo tiene que realizar la operación AND binaria en el tercer octeto. El resultado de los dos primeros octetos será 172.30, debido a la máscara de subred. El resultado del cuarto octeto será 0, debido a la máscara de subred.

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0
	=====
Resultado (red)	172.30.? .0

Realice la operación AND binaria en el tercer octeto.

	Decimal	Binario
	239	11101111
	192	11000000
		=====
Resultado	192	11000000

Si se vuelve a analizar este ejemplo, el resultado será el siguiente:

Dirección IP	172.30.239.145
Máscara de subred	255.255.192.0
	=====
Resultado (red)	172.30.192.0

Con este mismo ejemplo, para calcular la cantidad de hosts por red puede analizarse la máscara de subred. La máscara de subred estará representada en formato decimal punteado, como 255.255.192.0, o en formato de prefijo de red, como /18. Las direcciones IPv4 siempre tienen 32 bits. Restar la cantidad de bits utilizados para la porción de red (representada por la máscara de subred) da como resultado la cantidad de bits utilizados para los hosts.

Con el ejemplo anterior, la máscara de subred 255.255.192.0 equivale a /18 en notación de prefijo. Restar 18 bits de red de 32 bits da como resultado 14 bits para la porción de host. A partir de allí, es un cálculo simple:

$$2^{(\text{cantidad de bits del host})} - 2 = \text{cantidad de hosts}$$

$$2^{14} = 16\,384 - 2 = 16\,382 \text{ hosts}$$

Determine las direcciones de red y broadcast y la cantidad de bits de host y hosts para las direcciones IPv4 y los prefijos dados en la siguiente tabla.

Dirección IPv4/prefijo	Dirección de red	Dirección de broadcast	Cantidad total de bits de host	Cantidad total de hosts
192.168.100.25/28	192.168.100.16	192.168.100.31	4	14
172.30.10.130/30	172.30.10.128	172.30.10.131	2	2
10.1.113.75/19	10.1.96.0	10.1.127.255	13	8190
198.133.219.250/24	198.133.219.0	198.133.219.255	8	254
128.107.14.191/22	128.107.12.0	128.107.15.255	10	1022
172.16.104.99/27	172.16.104.96	172.16.104.127	5	30

Parte 2: Calcular la división en subredes de la dirección IPv4

Dada una dirección IPv4, la máscara de subred original y la nueva máscara de subred, podrá determinar lo siguiente:

- Dirección de red de esta subred
- Dirección de broadcast de esta subred
- Rango de direcciones de host de esta subred
- Cantidad de subredes creadas
- Cantidad de hosts por subred

A continuación, se muestra un problema de ejemplo junto con la solución:

Dado:	
Dirección IP del host:	172.16.77.120
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.240.0
Encontrar:	
Cantidad de bits de subred	4
Cantidad de subredes creadas	16
Cantidad de bits de host por subred	12
Cantidad de hosts por subred	4,094
Dirección de red de esta subred	172.16.64.0
Dirección IPv4 del primer host en esta subred	172.16.64.1
Dirección IPv4 del último host en esta subred	172.16.79.254
Dirección de broadcast IPv4 en esta subred	172.16.79.255

Analicemos cómo se completó esta tabla.

La máscara de subred original era 255.255.0.0 o /16. La nueva máscara de subred es 255.255.240.0 o /20. La diferencia resultante es 4 bits. Como se tomaron prestados 4 bits, podemos determinar que se crearon 16 subredes, ya que $2^4 = 16$.

La nueva máscara 255.255.240.0 o /20 deja 12 bits para los hosts. Con 12 bits para los hosts, utilizamos la siguiente fórmula: $2^{12} = 4096 - 2 = 4094$ hosts por subred.

La operación AND binaria lo ayudará a determinar la subred de este problema, que da como resultado la red 172.16.64.0.

Finalmente, necesita determinar el primer host, el último host y la dirección de broadcast para cada subred. Un método para determinar el rango de hosts es aplicar cálculos binarios para la porción de host de la dirección. En el ejemplo, los últimos 12 bits de la dirección corresponden a la porción de host. El primer host tendría todos los bits significativos establecidos en cero y el bit menos significativo establecido en 1. El último host tendría todos los bits significativos establecidos en 1 y el bit menos significativo establecido en 0. En este ejemplo, la porción de host de la dirección reside en el tercero y el cuarto octetos.

Descripción	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto	Descripción
Red/host	nnnnnnnn	nnnnnnnn	nnnnhhhh	hhhhhhhh	Máscara de subred
Binario	10101100	00010000	01000000	00000001	Primer host
Decimal	172	16	64	1	Primer host
Binario	10101100	00010000	01001111	11111110	Último host
Decimal	172	16	79	254	Último host
Binario	10101100	00010000	01001111	11111111	Broadcast
Decimal	172	16	79	255	Broadcast

Paso 1: Complete las tablas siguientes con las respuestas correspondientes dadas la dirección IPv4, la máscara de subred original y la nueva máscara de subred.

a. Problema 1:

Dado:	
Dirección IP del host:	192.168.200.139
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.224
Encontrar:	
Cantidad de bits de subred	3
Cantidad de subredes creadas	8
Cantidad de bits de host por subred	5
Cantidad de hosts por subred	30
Dirección de red de esta subred	192.168.200.128
Dirección IPv4 del primer host en esta subred	192.168.200.129
Dirección IPv4 del último host en esta subred	192.168.200.158
Dirección de broadcast IPv4 en esta subred	192.168.200.159

b. Problema 2:

Dado:	
Dirección IP del host:	10.101.99.228
Máscara de subred original	255.0.0.0
Máscara de subred nueva:	255.255.128.0
Encontrar:	
Cantidad de bits de subred	9
Cantidad de subredes creadas	512
Cantidad de bits de host por subred	15
Cantidad de hosts por subred	32,766
Dirección de red de esta subred	10.101.0.0
Dirección IPv4 del primer host en esta subred	10.101.0.1
Dirección IPv4 del último host en esta subred	10.101.127.254
Dirección de broadcast IPv4 en esta subred	10.101.127.255

c. Problema 3:

Dado:	
Dirección IP del host:	172.22.32.12
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.224.0
Encontrar:	
Cantidad de bits de subred	3
Cantidad de subredes creadas	8
Cantidad de bits de host por subred	13
Cantidad de hosts por subred	8190
Dirección de red de esta subred	172.22.32.0
Dirección IPv4 del primer host en esta subred	172.22.32.1
Dirección IPv4 del último host en esta subred	172.22.63.254
Dirección de broadcast IPv4 en esta subred	172.22.63.255

d. Problema 4:

Dado:	
Dirección IP del host:	192.168.1.245
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.252
Encontrar:	
Cantidad de bits de subred	6
Cantidad de subredes creadas	64
Cantidad de bits de host por subred	2
Cantidad de hosts por subred	2
Dirección de red de esta subred	192.168.1.244
Dirección IPv4 del primer host en esta subred	192.168.1.245
Dirección IPv4 del último host en esta subred	192.168.1.246
Dirección de broadcast IPv4 en esta subred	192.168.1.247

e. Problema 5:

Dado:	
Dirección IP del host:	128.107.0.55
Máscara de subred original	255.255.0.0
Máscara de subred nueva:	255.255.255.0
Encontrar:	
Cantidad de bits de subred	8
Cantidad de subredes creadas	256
Cantidad de bits de host por subred	8
Cantidad de hosts por subred	254
Dirección de red de esta subred	128.107.0.0
Dirección IPv4 del primer host en esta subred	128.107.0.1
Dirección IPv4 del último host en esta subred	128.107.0.254
Dirección de broadcast IPv4 en esta subred	128.107.0.255

f. Problema 6:

Dado:	
Dirección IP del host:	192.135.250.180
Máscara de subred original	255.255.255.0
Máscara de subred nueva:	255.255.255.248
Encontrar:	
Cantidad de bits de subred	5
Cantidad de subredes creadas	32
Cantidad de bits de host por subred	3
Cantidad de hosts por subred	6
Dirección de red de esta subred	192.135.250.176
Dirección IPv4 del primer host en esta subred	192.135.250.177
Dirección IPv4 del último host en esta subred	192.135.250.182
Dirección de broadcast IPv4 en esta subred	192.135.250.183

Reflexión

¿Por qué la máscara de subred es tan importante cuando se analiza una dirección IPv4?

La máscara de subred determina toda la información de la dirección: la red, la cantidad de bits de host, la cantidad de hosts y la dirección de broadcast. Con solo mirar una dirección IPv4, no obtendrá nada. Necesita la máscara de subred para obtener toda la información importante.

Práctica de laboratorio: División de topologías de red en subredes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

De la parte 1 a la 5, para todas las topologías de red:

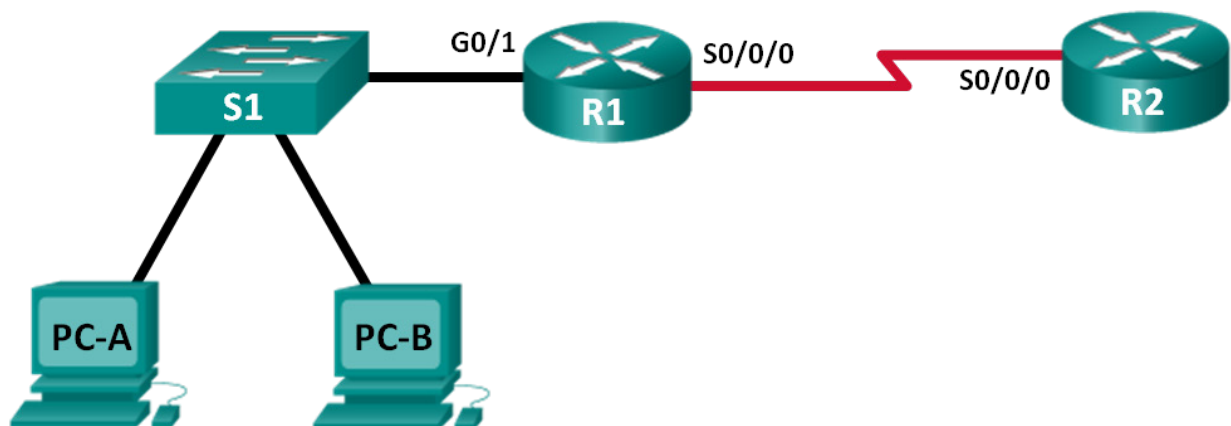
- Determinar la cantidad de subredes.
- Diseñar un esquema de direccionamiento adecuado.
- Asignar direcciones y pares de mascarar de subred a las interfaces del dispositivo.
- Examinar el uso del espacio de direcciones de red disponible y el crecimiento potencial futuro.

Información básica/Situación

Ante una topología de la red, es importante poder determinar la cantidad de subredes necesarias. En esta práctica de laboratorio, se proporcionarán varias situaciones de topologías, junto con una máscara y una dirección de red base. Dividirá la dirección de red en subredes y proporcionará un esquema de direccionamiento IP que admitirá la cantidad de subredes que se muestra en el diagrama de topología. Deberá determinar la cantidad de bits que se deben tomar prestados, la cantidad de hosts por subred y el potencial de crecimiento según lo especificado en las instrucciones.

Parte 1: Topología de la red A

En la parte 1, se otorgó la dirección de red 192.168.10.0/24 a la subred, con la siguiente topología. Determine la cantidad de redes necesarias y luego diseñe un esquema de direccionamiento adecuado.



Paso 1: Determine la cantidad de subredes en la topología de la red A.

- ¿Cuántas subredes hay? 2
- ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? 1
- ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento?
126
- ¿Cuál es la máscara de subred nueva en formato decimal punteado? 255.255.255.128
- ¿Cuántas subredes quedan disponibles para usar en el futuro? 0

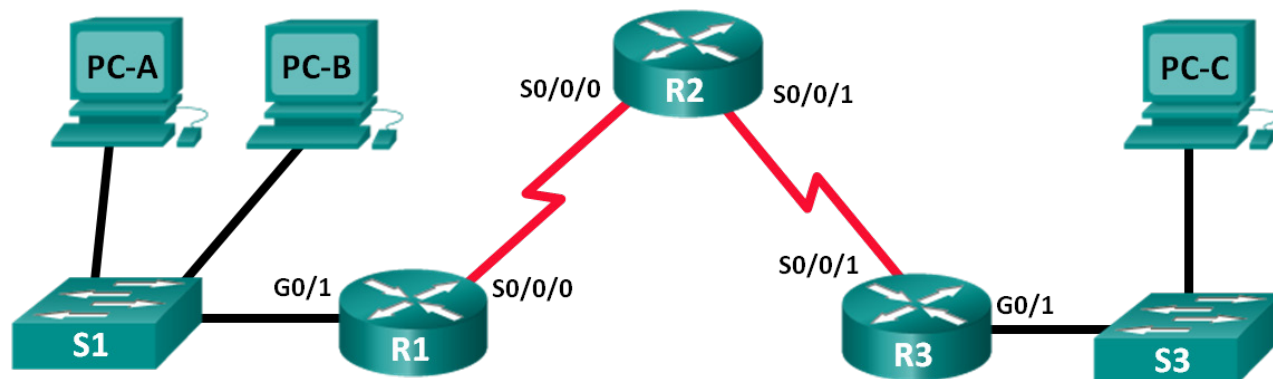
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.10.0	192.168.10.1	192.168.10.126	192.168.10.127
1	192.168.10.128	192.168.10.129	192.168.10.254	192.168.10.255
2				
3				
4				
5				

Parte 2: Topología de la red B

La topología de la red de la parte 1 se expandió para admitir el agregado del router R3 y la red complementaria, como se ilustra en la topología siguiente. Utilice la dirección de red 192.168.10.0/24 para proporcionar direcciones a los dispositivos de red y luego diseñe un nuevo esquema de direccionamiento para admitir el requisito de red adicional.



Paso 1: Determine la cantidad de subredes en la topología de la red B.

- ¿Cuántas subredes hay? 4
- ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? 2
- ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? 62
- ¿Cuál es la máscara de subred nueva en formato decimal punteado? 255.255.255.192
- ¿Cuántas subredes quedan disponibles para usar en el futuro? 0

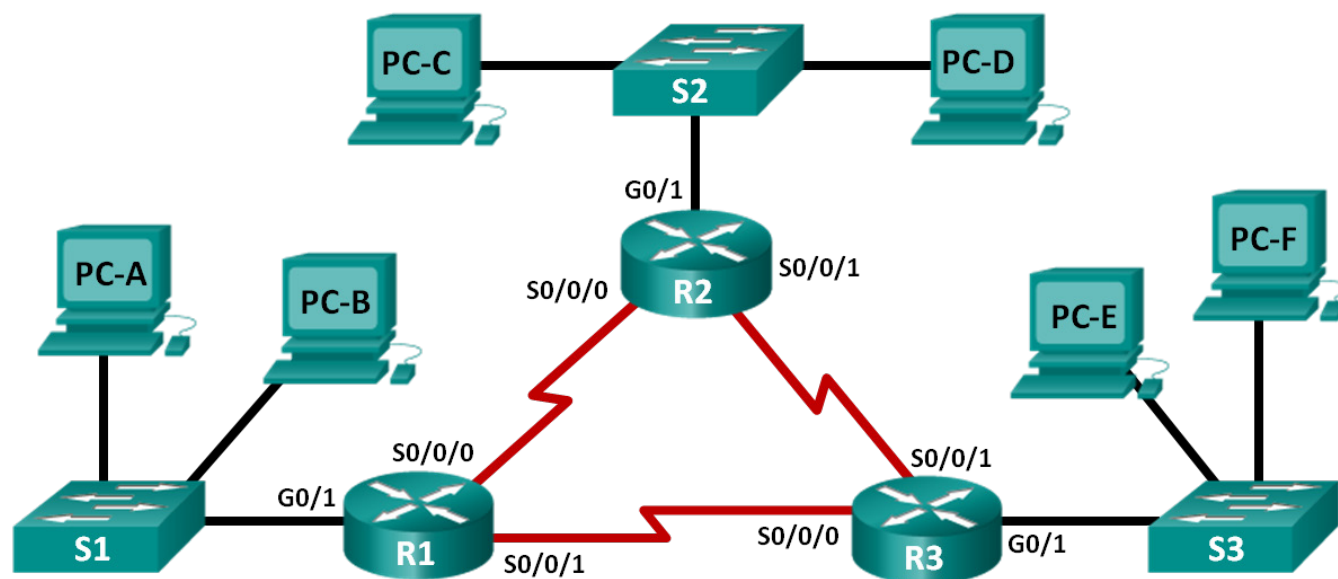
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
1	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
2	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
3	192.168.10.192	192.168.10.193	192.168.10.254	192.168.10.255
4				
5				
6				
7				

Parte 3: Topología de la red C

La topología volvió a cambiar con una LAN nueva agregada al R2 y un enlace redundante entre R1 y R3. Utilice la dirección de red 192.168.10.0/24 para proporcionar direcciones a los dispositivos de red. También proporcione un esquema de direcciones IP que admita estos dispositivos adicionales. Para esta topología, asigne una subred a cada red.



Paso 1: Determine la cantidad de subredes en la topología de la red C.

- ¿Cuántas subredes hay? 6
- ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? 3
- ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? 30
- ¿Cuál es la máscara de subred nueva en formato decimal punteado? 255.255.255.224
- ¿Cuántas subredes quedan disponibles para usar en el futuro? 2

Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.10.0	192.168.10.1	192.168.10.30	192.168.10.31
1	192.168.10.32	192.168.10.33	192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65	192.168.10.94	192.168.10.95
3	192.168.10.96	192.168.10.97	192.168.10.126	192.168.10.127
4	192.168.10.128	192.168.10.129	192.168.10.158	192.168.10.159
5	192.168.10.160	192.168.10.161	192.168.10.190	192.168.10.191
6	192.168.10.192	192.168.10.193	192.168.10.222	192.168.10.223
7	192.168.10.224	192.168.10.225	192.168.10.254	192.168.10.255
8				
9				
10				

Paso 3: Asignar direcciones a los dispositivos de red en las subredes

- a. Complete la siguiente tabla con las direcciones IP y las máscaras de subred para las interfaces del router:

Nota para el instructor: estas son direcciones IP sugeridas de acuerdo con el uso de las primeras seis subredes de la tabla anterior tal como se asignaron a cada segmento.

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	GigabitEthernet 0/1	192.168.10.1	255.255.255.224
	Serial 0/0/0	192.168.10.33	255.255.255.224
	Serial 0/0/1	192.168.10.65	255.255.255.224
R2	GigabitEthernet 0/1	192.168.10.97	255.255.255.224
	Serial 0/0/0	192.168.10.34	255.255.255.224
	Serial 0/0/1	192.168.10.129	255.255.255.224
R3	GigabitEthernet 0/1	192.168.10.161	255.255.255.224
	Serial 0/0/0	192.168.10.66	255.255.255.224
	Serial 0/0/1	192.168.10.130	255.255.255.224

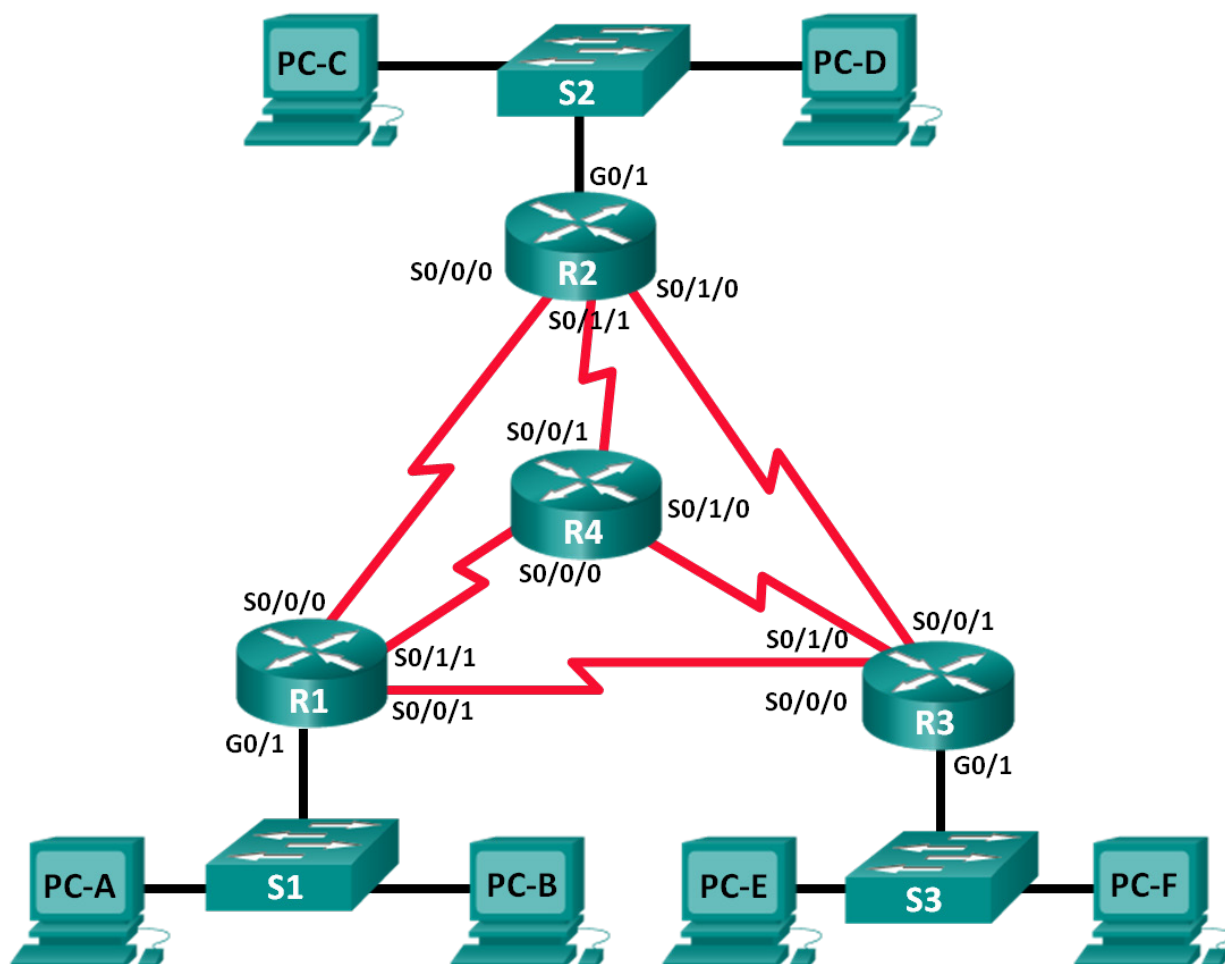
- b. Complete la tabla siguiente con las direcciones IP y las máscaras de subred para los dispositivos en la LAN, como se muestra en la topología.

Nota para el instructor: estas son direcciones IP sugeridas de acuerdo con el uso de las primeras seis subredes de la tabla anterior tal como se asignaron a cada segmento.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC-A	NIC	192.168.10.30	255.255.255.224	192.168.10.1
PC-B	NIC	192.168.10.29	255.255.255.224	192.168.10.1
S1	VLAN 1	192.168.10.2	255.255.255.224	192.168.10.1
PC-C	NIC	192.168.10.126	255.255.255.224	192.168.10.97
PC-D	NIC	192.168.10.125	255.255.255.224	192.168.10.97
S2	VLAN 1	192.168.10.98	255.255.255.224	192.168.10.97
PC-E	NIC	192.168.10.190	255.255.255.224	192.168.10.161
PC-F	NIC	192.168.10.189	255.255.255.224	192.168.10.161
S3	VLAN 1	192.168.10.162	255.255.255.224	192.168.10.161

Parte 4: Topología de la red D

La red se modificó para admitir cambios en la organización. Se utiliza la dirección de red 192.168.10.0/24 para proporcionar las direcciones en la red.



Paso 1: Determine la cantidad de subredes en la topología de la red D.

- ¿Cuántas subredes hay? 9
- ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? 4
- ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? 14
- ¿Cuál es la máscara de subred nueva en formato decimal punteado? 255.255.255.240
- ¿Cuántas subredes quedan disponibles para usar en el futuro? 7

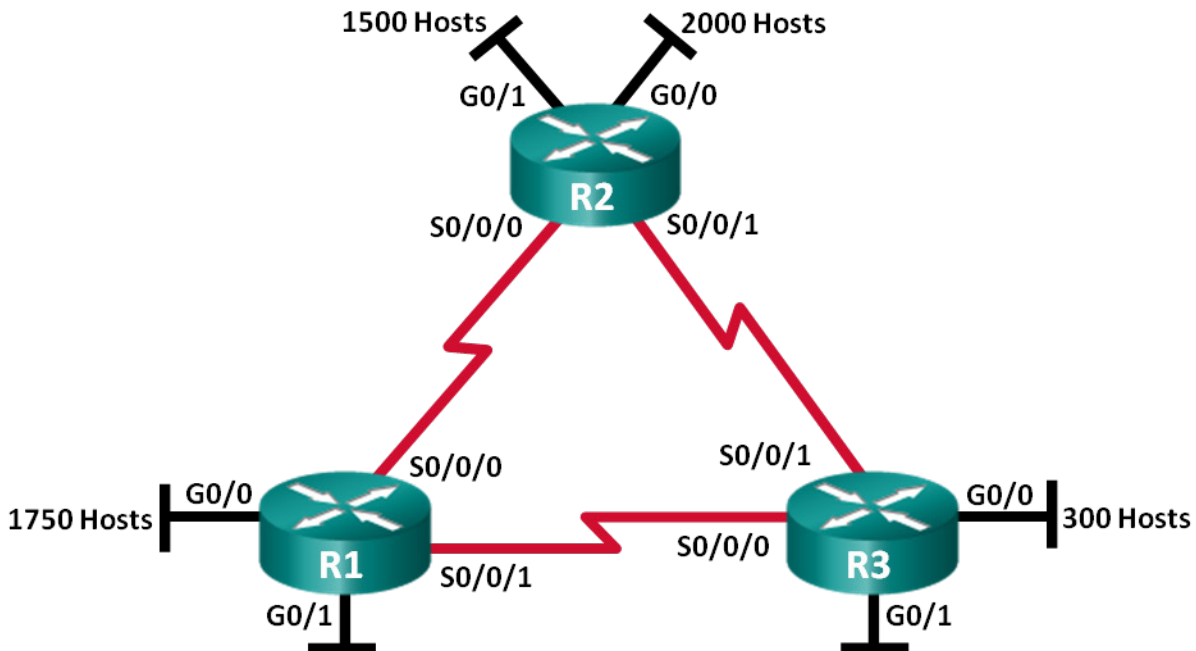
Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred.

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.10.0	192.168.10.1	192.168.10.14	192.168.10.15
1	192.168.10.16	192.168.10.17	192.168.10.30	192.168.10.31
2	192.168.10.32	192.168.10.33	192.168.10.46	192.168.10.47
3	192.168.10.48	192.168.10.49	192.168.10.62	192.168.10.63
4	192.168.10.64	192.168.10.65	192.168.10.78	192.168.10.79
5	192.168.10.80	192.168.10.81	192.168.10.94	192.168.10.95
6	192.168.10.96	192.168.10.97	192.168.10.110	192.168.10.111
7	192.168.10.112	192.168.10.111	192.168.10.126	192.168.10.127
8	192.168.10.128	192.168.10.129	192.168.10.142	192.168.10.143
9	192.168.10.144	192.168.10.145	192.168.10.158	192.168.10.159
10	192.168.10.160	192.168.10.161	192.168.10.174	192.168.10.175
11	192.168.10.176	192.168.10.177	192.168.10.190	192.168.10.191
12	192.168.10.192	192.168.10.193	192.168.10.206	192.168.10.207
13	192.168.10.208	192.168.10.209	192.168.10.222	192.168.10.223
14	192.168.10.224	192.168.10.225	192.168.10.238	192.168.10.239
15	192.168.10.240	192.168.10.241	192.168.10.254	192.168.10.255
16				
17				

Parte 5: Topología de la red E

La organización tiene una dirección de red 172.16.128.0/17 que se dividirá como se ilustra en la topología siguiente. Debe elegir un esquema de direccionamiento que pueda admitir la cantidad de redes y hosts en la topología.



Paso 1: Determine la cantidad de subredes en la topología de la red E.

- ¿Cuántas subredes hay? 9
- ¿Cuántos bits debe tomar prestados para crear la cantidad de subredes requeridas? 4
- ¿Cuántas direcciones de host utilizables por subred se encuentran en este esquema de direccionamiento? 2046
- ¿Cuál es la máscara de subred nueva en formato decimal punteado? 255.255.248.0
- ¿Cuántas subredes quedan disponibles para usar en el futuro? 7

Paso 2: Registre la información de subred.

Complete la siguiente tabla con la información de la subred:

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	172.16.128.0	172.16.128.1	172.16.135.254	172.16.135.255
1	172.16.136.0	172.16.136.1	172.16.143.254	172.16.143.255
2	172.16.144.0	172.16.144.1	172.16.151.254	172.16.151.255
3	172.16.152.0	172.16.152.1	172.16.159.254	172.16.159.255
4	172.16.160.0	172.16.160.1	172.16.167.254	172.16.167.255
5	172.16.168.0	172.16.168.1	172.16.175.254	172.16.175.255
6	172.16.176.0	172.16.176.1	172.16.183.254	172.16.183.255
7	172.16.184.0	172.16.184.1	172.16.191.254	172.16.191.255
8	172.16.192.0	172.16.192.1	172.16.199.254	172.16.199.255
9	172.16.200.0	172.16.200.1	172.16.207.254	172.16.207.255
10	172.16.208.0	172.16.208.1	172.16.215.254	172.16.215.255
11	172.16.216.0	172.16.216.1	172.16.223.254	172.16.223.255
12	172.16.224.0	172.16.224.1	172.16.231.254	172.16.231.255
13	172.16.232.0	172.16.232.1	172.16.239.254	172.16.239.255
14	172.16.240.0	172.16.240.1	172.16.247.254	172.16.247.255
15	172.16.248.0	172.16.248.1	172.16.255.254	172.16.255.255
16				
17				

Paso 3: Asignar direcciones a los dispositivos de red en las subredes

- a. Complete la siguiente tabla con las direcciones IP y las máscaras de subred para las interfaces del router:

Nota para el instructor: estas son direcciones IP sugeridas de acuerdo con el uso de las primeras nueve subredes de la tabla anterior, tal como se asignaron a cada segmento.

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	GigabitEthernet 0/0	172.16.128.1	255.255.248.0
	GigabitEthernet 0/1	172.16.136.1	255.255.248.0
	Serial 0/0/0	172.16.144.1	255.255.248.0
	Serial 0/0/1	172.16.152.1	255.255.248.0
R2	GigabitEthernet 0/0	172.16.160.1	255.255.248.0
	GigabitEthernet 0/1	172.16.168.1	255.255.248.0
	Serial 0/0/0	172.16.144.2	255.255.248.0
	Serial 0/0/1	172.16.176.1	255.255.248.0
R3	GigabitEthernet 0/0	172.16.184.1	255.255.248.0
	GigabitEthernet 0/1	172.16.192.1	255.255.248.0
	Serial 0/0/0	172.16.152.2	255.255.248.0
	Serial 0/0/1	172.16.176.2	255.255.248.0

Reflexión

1. ¿Qué información es necesaria cuando debe determinar un esquema de direccionamiento adecuado para una red?

Se necesita la cantidad de redes y hosts para determinar un esquema de direccionamiento adecuado para una red.

2. Una vez asignadas las subredes, ¿se utilizarán todas las direcciones de host en cada subred?

No. Para los enlaces seriales WAN, solo se usarán dos direcciones. Para las subredes con PC host, se pueden usar todas las direcciones en cada subred.

Práctica de laboratorio: Diseño e implementación de un esquema de direccionamiento IPv4 dividido en subredes (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

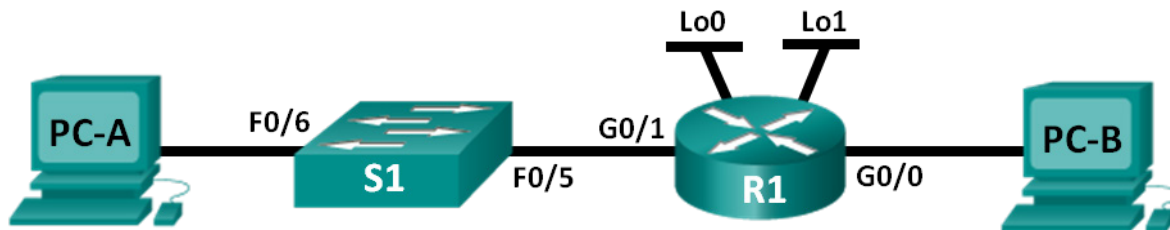


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0			No aplicable
	G0/1			No aplicable
	Lo0			No aplicable
	Lo1			No aplicable
S1	VLAN 1	No aplicable	No aplicable	No aplicable
PC-A	NIC			
PC-B	NIC			

Objetivos

Parte 1: Diseñar un esquema de división en subredes

- Crear un esquema de división en subredes que cumpla con la cantidad requerida de subredes y direcciones de host.
- Completar el diagrama para mostrar dónde se aplicarán las direcciones IP de host.

Parte 2: Configurar los dispositivos

- Asignar una dirección IP, una máscara de subred y un gateway predeterminado a las PC.
- Configurar las interfaces Gigabit Ethernet del router con una dirección IP y una máscara de subred.
- Crear dos interfaces loopback en el router y configurar cada una con una dirección IP y una máscara de subred.

Parte 3: Probar la red y resolver los problemas encontrados

- Verificar y resolver problemas de conectividad de red mediante el comando ping.

Información básica/Situación

En esta práctica de laboratorio, a partir de una sola dirección de red y una máscara de red, dividirá la red en varias subredes. El esquema de división en subredes se basará en la cantidad de equipos host necesarios en cada subred, así como en otras consideraciones de redes, como la futura expansión de hosts de la red.

Después de crear un esquema de división en subredes y completar el diagrama de red con las direcciones IP de hosts e interfaces, configurará las PC host y las interfaces del router, incluidas las interfaces loopback. Las interfaces loopback se crean para simular LAN adicionales conectadas al router R1.

Una vez configurados los dispositivos de red y las PC host, utilizará el comando **ping** para probar la conectividad de red.

En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos reales necesarios para configurar el router. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento intentando configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Gigabit Ethernet en los routers Cisco 1941 cuentan con detección automática. Se puede usar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: Diseñar un esquema de división en subredes

Paso 1: Crear un esquema de división en subredes que cumpla con la cantidad requerida de subredes y de direcciones de host

En esta situación, usted es un administrador de red para una pequeña subdivisión de una compañía más grande. Debe crear varias subredes a partir del espacio de direcciones de red 192.168.0.0/24 para cumplir los siguientes requisitos:

- La primera subred es la red de los empleados. Necesita un mínimo de 25 direcciones IP de host.
- La segunda subred es la red de administración. Necesita un mínimo de 10 direcciones IP.
- La tercera y la cuarta subredes están reservadas como redes virtuales en las interfaces virtuales del router loopback 0 y loopback 1. Estas interfaces virtuales del router simulan LAN conectadas al R1.

- También necesita dos subredes adicionales sin utilizar para la futura expansión de la red.

Nota: no se usarán máscaras de subred de longitud variable. Todas las máscaras de subred de los dispositivos tendrán la misma longitud.

Responda las siguientes preguntas para poder crear un esquema de división en subredes que cumpla con los requisitos de red mencionados:

- 1) ¿Cuántas direcciones de host se necesitan en la subred requerida más grande? _____ **25**
- 2) ¿Cuál es la cantidad mínima de subredes necesaria? _____

Los requisitos arriba mencionados especifican dos redes de la compañía más dos redes virtuales de loopback y dos redes adicionales para expansión futura. Entonces, la respuesta es un mínimo de seis redes.

- 3) La red que se le asignó para la división en subredes es 192.168.0.0/24. ¿Cómo es la máscara de subred /24 en formato binario?

11111111.11111111.11111111.00000000

- 4) La máscara de subred consta de dos partes: la porción de red y la porción de host. En sistema binario, esto se representa mediante unos y ceros en la máscara de subred.

En la máscara de red, ¿qué representan los unos? _____

Los unos representan la porción de red.

En la máscara de red, ¿qué representan los ceros? _____

Los ceros representan la porción de host.

- 5) Para dividir una red en subredes, los bits de la porción de host de la máscara de red original cambian por bits de subred. La cantidad de bits de subred define la cantidad de subredes. Dada cada una de las posibles máscaras de subred presentadas a continuación en formato binario, ¿cuántas subredes y cuántos hosts se crean en cada ejemplo?

Sugerencia: recuerde que la cantidad de bits de host (en potencia de 2) define la cantidad de hosts por subred (menos 2), y que la cantidad de bits de subred (en potencia de 2) define la cantidad de subredes. Los bits de subred (representados en negrita) son los bits que se tomaron prestados más allá de la máscara de red original /24. /24 es la notación de prefijo de barra y corresponde a la máscara decimal punteada 255.255.255.0.

(/25) 11111111.11111111.11111111.10000000

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.128

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Dos subredes (2^1) y 128 hosts (2^7) – 2 = 126 hosts por subred

(/26) 11111111.11111111.11111111.11000000

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.192

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Cuatro subredes (2^2) y 64 hosts (2^6) – 2 = 62 hosts por subred

(/27) 11111111.11111111.11111111.11100000

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.224

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Ocho subredes (2^3) y 32 hosts (2^5) – 2 = 30 hosts por subred

(/28) 11111111.11111111.11111111.11110000

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.240

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Dieciséis subredes (2^4) y 16 hosts (2^4) – 2 = 14 hosts por subred

(/29) 11111111.11111111.11111111.11111000

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.248

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Treinta y dos subredes (2^5) y 8 hosts (2^3) – 2 = 6 hosts por subred

(/30) 11111111.11111111.11111111.11111100

Equivalente decimal punteado de la máscara de subred: _____

255.255.255.252

¿Cantidad de subredes? _____ ¿Cantidad de hosts? _____

Sesenta y cuatro subredes (2^6) y 4 hosts (2^2) – 2 = 2 hosts por subred

- 6) Sobre la base de sus respuestas, ¿qué máscaras de subred cumplen con la cantidad mínima requerida de direcciones de host?

/25, /26, /27

- 7) Sobre la base de sus respuestas, ¿qué máscaras de subred cumplen con la cantidad mínima requerida de subredes?

/27, /28, /29, /30 darán la cantidad requerida de subredes.

- 8) Sobre la base de sus respuestas, ¿qué máscara de subred cumple con la cantidad mínima requerida de hosts y también con la cantidad mínima requerida de subredes?

/27 le dará ocho subredes, que es mayor que la cantidad mínima requerida de cinco, y 30 hosts por subred, que es mayor que los 25 hosts requeridos para la primera subred.

- 9) Cuando haya determinado qué máscara de subred cumple con todos los requisitos de red mencionados, derivará cada una de las subredes a partir de la dirección de red original. Indique las subredes desde la primera hasta la última a continuación. Recuerde que la primera subred es 192.168.0.0, con la máscara de subred recién adquirida.

Dirección de subred / PrefijoMáscara de subred (decimal punteada)

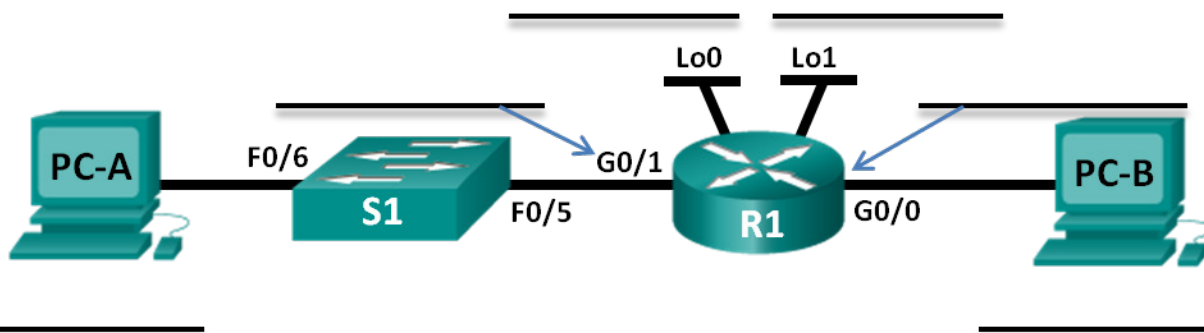
_____/_____
_____/_____

_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____

192.168.0.0, 192.168.0.32, 192.168.0.64, 192.168.0.96, 192.168.0.128, 192.168.0.160, 192.168.0.192, 192.168.0.224. En todos los casos, el prefijo es /27. En todos los casos, la máscara de subred es 255.255.255.224 (decimal punteada).

Paso 2: Completar el diagrama para mostrar dónde se aplicarán las direcciones IP de host

En las líneas siguientes, complete las direcciones IP y las máscaras de subred en notación de prefijo de barra. En el router, utilice la primera dirección utilizable en cada subred para cada una de las interfaces: Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 y loopback 1. Complete una dirección IP para la PC-A y la PC-B. También introduzca esta información en la tabla de direccionamiento de la página 1.



Las direcciones de las interfaces Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 y loopback 1 del router serían: 192.168.0.1/27, 192.168.0.33/27, 192.168.0.65/27, 192.168.0.97/27. Si la interfaz Gigabit 0/0 es la primera subred, la dirección IP de la PC-B será un número entre 192.168.0.2 y 192.168.0.30. Si la interfaz Gigabit 0/1 es la segunda subred, la dirección IP de la PC-A será un número entre 192.168.0.34 y 192.168.0.62.

Parte 2: Configurar los dispositivos

En la parte 2, establecerá la topología de la red y configurará los parámetros básicos en las PC y el router, como las direcciones IP de la interfaz Gigabit Ethernet del router y las direcciones IP, las máscaras de subred y los gateways predeterminados de las PC. Consulte la tabla de direccionamiento para obtener los nombres e información de dirección de los dispositivos.

Nota: en el apéndice A, se proporcionan detalles de configuración para los pasos de la parte 2. Antes de consultar el apéndice A, intente completar la parte 2.

Paso 1: Configurar el router.

- Ingresa al modo EXEC privilegiado y, luego, al modo de configuración global.

- b. Asigne **R1** como nombre de host para el router.
- c. Configure las interfaces **G0/0** y **G0/1** con direcciones IP y máscaras de subred y, luego, habilítelas.
- d. Las interfaces loopback se crean para simular LAN adicionales en el router R1. Configure las interfaces loopback con direcciones IP y máscaras de subred. Una vez que se crean, las interfaces loopback se habilitan de manera predeterminada. (Para crear las direcciones de loopback, introduzca el comando **interface loopback 0** en el modo de configuración global).

Nota: si lo desea, puede crear varios loopbacks adicionales para probar con diferentes esquemas de direccionamiento.

- e. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 2: Configure las interfaces de la PC.

- a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.
- b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.

Parte 3: Probar la red y resolver los problemas encontrados

En la parte 3, utilizará el comando **ping** para probar la conectividad de red.

- a. Pruebe si la PC-A puede comunicarse con el gateway predeterminado. En la PC-A, abra un símbolo del sistema y haga ping a la dirección IP de la interfaz Gigabit Ethernet 0/1 del router. ¿Obtiene una respuesta?

Si la interfaz de la PC y la interfaz del router se configuraron correctamente, el ping debe ser correcto. Si no es así, revise los puntos “d” y “e” a continuación.

- b. Pruebe si la PC-B puede comunicarse con el gateway predeterminado. En la PC-B, abra un símbolo del sistema y haga ping a la dirección IP de la interfaz Gigabit Ethernet 0/0 del router. ¿Obtiene una respuesta?

Si la interfaz de la PC y la interfaz del router se configuraron correctamente, el ping debe ser correcto. Si no es así, revise los puntos “d” y “e” a continuación.

- c. Pruebe si la PC-A puede comunicarse con la PC-B. En la PC-A, abra un símbolo del sistema y haga ping a la dirección IP de la PC-B. ¿Obtiene una respuesta? _____

Si las PC y las interfaces Gigabit Ethernet del router se configuraron correctamente, los pings deben realizarse de manera correcta. Si no es así, revise los puntos “d” y “e” a continuación.

- d. Si alguna de sus respuestas a las preguntas anteriores fue negativa, debe revisar todas las configuraciones de dirección IP y máscara de subred, y asegurarse de que los gateways predeterminados estén configurados correctamente en la PC-A y la PC-B.
- e. Si verifica que todas las configuraciones son correctas y aún no puede hacer ping correctamente, hay algunos otros factores que pueden bloquear los pings de ICMP. En Windows, en la PC-A y la PC-B, asegúrese de que el Firewall de Windows esté desactivado para las redes de trabajo, doméstica y pública.
- f. Experimente configurando a propósito la dirección del gateway de manera incorrecta en la PC-A como 10.0.0.1. ¿Qué sucede cuando intenta hacer ping de la PC-B a la PC-A? ¿Recibe una respuesta?

Con configuraciones incorrectas deliberadas, la respuesta debe ser no.

Reflexión

1. Dividir una red grande en subredes más pequeñas brinda mayor flexibilidad y seguridad en el diseño de redes. Sin embargo, ¿cuáles piensa que son algunas de las desventajas cuando las subredes están limitadas a tener el mismo tamaño?

Las respuestas varían. Los estudiantes pueden sugerir que, debido a que algunas subredes requieren muchas direcciones IP y otras requieren solo unas pocas, tener todas las subredes del mismo tamaño no es la forma más eficaz de dividir las subredes.

2. ¿Por qué piensa que la dirección IP del gateway o del router es generalmente la primera dirección IP utilizable en la red?

Las respuestas varían. Puede sugerirse que se debe a que el router o el gateway son como una puerta a la red y, por lo tanto, es lógico que la dirección esté al comienzo de la red. Sin embargo, no es más que una convención y, por lo tanto, no es obligatorio que el router tenga la primera o la última dirección en la red.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Apéndice A: Detalles de configuración para los pasos de la parte 2

Paso 1: Configurar el router.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
```

```
Router#
```

- b. Entre al modo de configuración.

```
Router# conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

- c. Asigne un nombre de dispositivo al router.

```
Router(config)# hostname R1
```

```
R1(config)#
```

- d. Configure las interfaces **G0/0** y **G0/1** con direcciones IP y máscaras de subred, y habilítelas.

```
R1(config)# interface g0/0
```

```
R1(config-if)# ip address <ip address> <subnet mask>
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# interface g0/1
```

```
R1(config-if)# ip address <ip address> <subnet mask>
```

```
R1(config-if)# no shutdown
```

- e. Las interfaces loopback se crean para simular LAN adicionales fuera del router R1. Configure las interfaces loopback con direcciones IP y máscaras de subred. Cuando se crean, las interfaces loopback se habilitan de manera predeterminada.

```
R1(config)# interface loopback 0
```

```
R1(config-if)# ip address <ip address> <subnet mask>
```

```
R1(config-if)# interface loopback 1
```

```
R1(config-if)# ip address <ip address> <subnet mask>
```

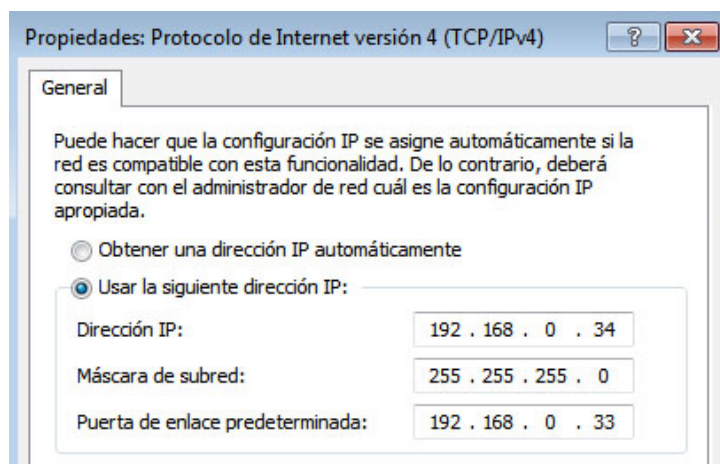
```
R1(config-if)# end
```

- f. Guarde la configuración en ejecución en el archivo de configuración de inicio.

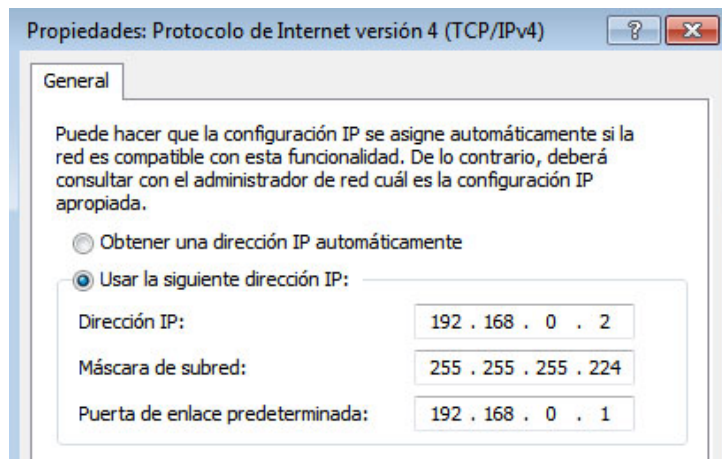
```
R1# copy running-config startup-config
```

Paso 2: Configure las interfaces de la PC.

- a. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-A.



- b. Configure la dirección IP, la máscara de subred y las configuraciones de gateway predeterminado en la PC-B.



Configuraciones de dispositivos

Router R1

```
R1#show run
```

```
Building configuration...
```

```
Current configuration : 1518 bytes
```

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
!  
!  
no ipv6 cef  
ip auth-proxy max-login-attempts 5  
ip admission max-login-attempts 5  
!  
!  
!  
!  
!  
ip cef
```

```
!  
multilink bundle-name authenticated  
!  
crypto pki token default removal timeout 0  
!  
!  
!  
!  
!  
redundancy  
!  
!  
!  
!  
interface Loopback0  
 ip address 192.168.0.65 255.255.255.224  
!  
interface Loopback1  
 ip address 192.168.0.97 255.255.255.224  
!  
interface Embedded-Service-Engine0/0  
 no ip address  
 shutdown  
!  
interface GigabitEthernet0/0  
 ip address 192.168.0.1 255.255.255.224  
 duplex auto  
 speed auto  
!  
interface GigabitEthernet0/1  
 ip address 192.168.0.33 255.255.255.224  
 duplex auto  
 speed auto  
!  
interface Serial0/0/0  
 no ip address  
 shutdown  
 clock rate 2000000  
!  
interface Serial0/0/1  
 no ip address  
 shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!
```

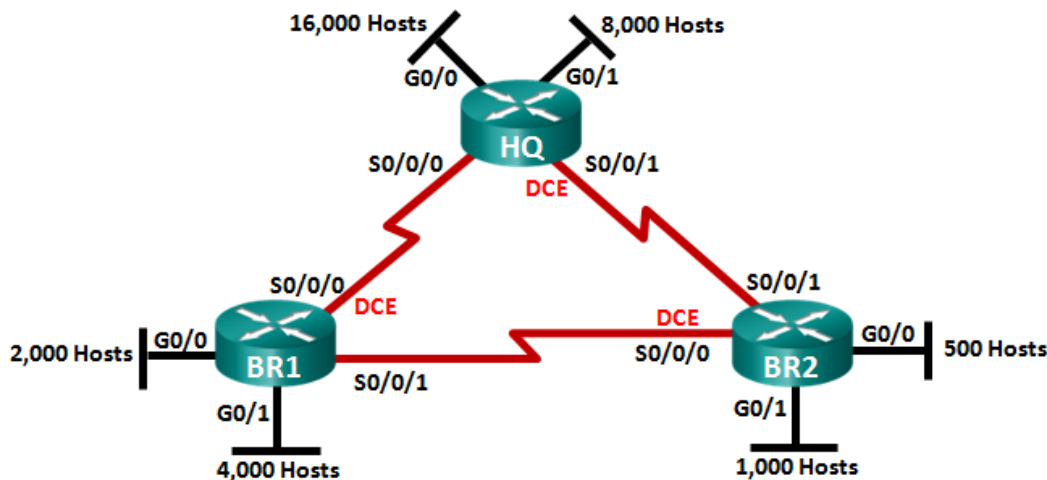


```
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login  
  transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

Práctica de laboratorio: Diseño e implementación de un esquema de direccionamiento VLSM (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Examinar los requisitos de la red

Parte 2: Diseñar el esquema de direcciones VLSM

Parte 3: Cablear y configurar la red IPv4

Información básica/Situación

La máscara de subred de longitud variable (VLSM) se diseñó para evitar el desperdicio de direcciones IP. Con VLSM, una red se divide en subredes y luego se vuelve a dividir en subredes. Este proceso se puede repetir varias veces para crear subredes de diversos tamaños según la cantidad de hosts necesarios en cada subred. El uso eficaz de VLSM requiere la planificación de direcciones.

En esta práctica de laboratorio, utilice la dirección de red 172.16.128.0/17 para desarrollar un esquema de direcciones para la red que se muestra en el diagrama de topología. VLSM se utiliza para cumplir con los requisitos de direccionamiento IPv4. Después de diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información de direcciones IP correspondiente.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Se pueden utilizar otros routers y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan eliminado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Si el tiempo es un problema, esta práctica de laboratorio se puede realizar en varias sesiones. Las partes 1 y 2 se resuelven de manera escrita, por lo que pueden asignarse como tarea para el hogar. La parte 3 es práctica y requiere equipos para prácticas de laboratorio.

Cabe mencionar a los estudiantes que, como administrador de red, no tendría una sola red con más de 1000 hosts, sino que los dividiría en una red de producción.

Recursos necesarios

- 3 routers (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o comparable)
- 1 PC (con programa de emulación de terminal, como Tera Term, para configurar los routers)
- Cable de consola para configurar los dispositivos Cisco IOS a través de los puertos de consola
- Cables Ethernet (optativos) y seriales, según se muestra en la topología
- Calculadora de Windows (optativo)

Parte 1: Examinar los requisitos de la red

En la parte 1, examinará los requisitos de la red para desarrollar un esquema de direcciones VLSM para la red que se muestra en el diagrama de topología utilizando la dirección de red 172.16.128.0/17.

Nota: para obtener ayuda con los cálculos, puede utilizar la aplicación de calculadora de Windows y la calculadora de subredes IP de www.ipcalc.org.

Paso 1: Determinar cuántas direcciones de host y cuántas subredes hay disponibles

¿Cuántas direcciones de host hay disponibles en una red /17? _____ 32,766

¿Cuál es la cantidad total de direcciones de host necesarias en el diagrama de topología? _____ 31,506

¿Cuántas subredes se necesitan en la topología de la red? _____ 9

Paso 2: Determinar la subred más grande

¿Cuál es la descripción de la subred (p. ej., enlace BR1 G0/1 LAN o BR1-HQ WAN)? _____
HQ G0/0 LAN

¿Cuántas direcciones IP se requieren en la subred más grande? _____ 16,000

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ /18 o 255.255.192.0

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ 16,382

¿Puede dividir la dirección de red 172.16.128.0/17 en subredes para admitir esta subred? _____ Sí

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ 172.16.128.0/18

_____ 172.16.192.0/18

Utilice la primera dirección de red para esta subred.

Paso 3: Determinar la segunda subred más grande

¿Cuál es la descripción de la subred? _____ HQ G0/1 LAN

¿Cuántas direcciones IP se requieren para la segunda subred más grande? _____ 8,000

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ /19 o 255.255.224.0

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ 8,190

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred? _____ sí

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ 172.16.192.0/19

_____ 172.16.224.0/19

Utilice la primera dirección de red para esta subred.

Paso 4: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred? _____ BR1 G0/1 LAN

¿Cuántas direcciones IP se requieren para la siguiente subred más grande? _____ 4,000

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ /20 o 255.255.240.0

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ 4,094

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred? _____ sí

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ 172.16.224.0/20

_____ 172.16.240.0/20

Utilice la primera dirección de red para esta subred.

Paso 5: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred? _____ BR1 G0/0 LAN

¿Cuántas direcciones IP se requieren para la siguiente subred más grande? _____ 2,000

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ /21 o 255.255.248.0

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ 2,046

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred? _____ sí

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ 172.16.240.0/21

_____ 172.16.248.0/21

Utilice la primera dirección de red para esta subred.

Paso 6: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred? _____ BR2 G0/1 LAN

¿Cuántas direcciones IP se requieren para la siguiente subred más grande? _____ 1,000

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ /22 o 255.255.252.0

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ 1,022

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred? _____ **sí**

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ **172.16.248.0/22**

_____ **172.16.252.0/22**

Utilice la primera dirección de red para esta subred.

Paso 7: Determine la siguiente subred más grande.

¿Cuál es la descripción de la subred? _____ **BR2 G0/0 LAN**

¿Cuántas direcciones IP se requieren para la siguiente subred más grande? _____ **500**

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ **/23 o 255.255.254.0**

¿Cuántas direcciones de host totales puede admitir esa máscara de subred? _____ **510**

¿Puede volver a dividir la subred restante en subredes y aún admitir esta subred? _____ **sí**

¿Cuáles son las dos direcciones de red que derivarían de esta división en subredes?

_____ **172.16.252.0/23**

_____ **172.16.254.0/23**

Utilice la primera dirección de red para esta subred.

Paso 8: Determinar las subredes necesarias para admitir los enlaces seriales

¿Cuántas direcciones de host se requieren para cada enlace serial de subred? _____ **2**

¿Qué máscara de subred puede admitir esa cantidad de direcciones de host?

_____ **/30 o 255.255.255.252**

- a. Continúe subdividiendo la primera subred de cada subred nueva hasta que tenga cuatro subredes /30. Escriba las tres primeras direcciones de red de estas subredes /30 a continuación.

_____ **172.16.254.0/30**

_____ **172.16.254.4/30**

_____ **172.16.254.8/30**

- b. Introduzca las descripciones de subred para estas tres subredes a continuación.

_____ **Enlace serial HQ - BR1**

_____ **Enlace serial HQ - BR2**

_____ **Enlace serial BR1 - BR2**

Parte 2: Diseñar el esquema de direcciones VLSM

Paso 1: Calcular la información de subred

Utilice la información que obtuvo en la parte 1 para completar la siguiente tabla.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red /CIDR	Primera dirección de host	Dirección de broadcast
HQ G0/0	16 000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8 000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4 000	172.16.224.0/20	172.16.224.1	172.16.239.255
BR1 G0/0	2 000	172.16.240.0/21	172.16.240.1	172.16.247.255
BR2 G0/1	1000	172.16.248.0/22	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0/23	172.16.252.1	172.16.253.255
HQ S0/0/0 – BR1 S0/0/1	2	172.16.254.0/30	172.16.254.1	172.16.254.3
HQ S0/0/1 – BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5	172.16.254.7
BR1 S0/0/1 – BR2 S0/0/0	2	172.16.254.8/30	172.16.254.9	172.168.254.11

Paso 2: Completar la tabla de direcciones de interfaces de dispositivos

Asigne la primera dirección de host en la subred a las interfaces Ethernet. A HQ se le debe asignar la primera dirección de host en los enlaces seriales a BR1 y BR2. A BR1 se le debe asignar la primera dirección de host para el enlace serial a BR2.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Interfaz de dispositivo
HQ	G0/0	172.16.128.1	255.255.192.0	LAN de 16 000 hosts
	G0/1	172.16.192.1	255.255.224.0	LAN de 8000 hosts
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	LAN de 2000 hosts
	G0/1	172.16.224.1	255.255.240.0	LAN de 4000 hosts
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0
BR2	G0/0	172.16.252.1	255.255.254.0	LAN de 500 hosts
	G0/1	172.16.248.1	255.255.252.0	LAN de 1000 hosts
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

Parte 3: Cablear y configurar la red IPv4

En la parte 3, realizará el cableado de la topología de la red y configurará los tres routers mediante el esquema de direcciones VLSM que desarrolló en la parte 2.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Configurar los parámetros básicos en cada router

- Asigne el nombre de dispositivo al router.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

Paso 3: Configurar las interfaces en cada router

- Asigne una dirección IP y una máscara de subred a cada interfaz por medio de la tabla que completó en la parte 2.
- Configure una descripción de la interfaz para cada interfaz.
- Establezca la velocidad del reloj de todas las interfaces seriales DCE en 128000.
`HQ(config-if)# clock rate 128000`
- Active las interfaces.

Paso 4: Guardar la configuración en todos los dispositivos

Paso 5: Probar la conectividad

- En HQ, haga ping a la dirección de la interfaz S0/0/0 de BR1.
- En HQ, haga ping a la dirección de la interfaz S0/0/1 de BR2.
- En BR1, haga ping a la dirección de la interfaz S0/0/0 de BR2.
- Si los pings no se realizaron correctamente, resuelva los problemas de conectividad.

Nota: los pings a las interfaces GigabitEthernet en otros routers no se realizarán correctamente. Las LAN definidas para las interfaces GigabitEthernet son simuladas. Dado que no hay dispositivos conectados a estas LAN, el estado será down/down (inactivo/inactivo). Debe haber un protocolo de enrutamiento implementado para que los otros dispositivos adviertan esas subredes. Las interfaces GigabitEthernet también deben tener un estado up/up (activo/activo) para que un protocolo de enrutamiento pueda agregar las subredes a la tabla de enrutamiento. Estas interfaces permanecerán en un estado down/down hasta que se conecte un dispositivo al otro extremo del cable de la interfaz Ethernet. Esta práctica de laboratorio se centra en VLSM y en la configuración de las interfaces.

Reflexión

¿Puede pensar en un atajo para calcular las direcciones de red de las subredes /30 consecutivas?

Las respuestas pueden variar. Una red /30 tiene 4 espacios de dirección: la dirección de red, 2 direcciones de host y una dirección de broadcast. Otra técnica para obtener la próxima dirección de red /30 sería tomar la dirección de red /30 anterior y sumarle 4 al último octeto.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos

Router BR1 (configuración final)

```
BR1#sh run
Building configuration...

Current configuration : 1555 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BR1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```



```
!  
no aaa new-model  
memory-size iomem 15  
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  description LAN with 2,000 hosts.  
  ip address 172.16.240.1 255.255.248.0  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  description LAN with 4,000 hosts.  
  ip address 172.16.224.1 255.255.240.0  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  description Connection to HQ S0/0/0.  
  ip address 172.16.254.2 255.255.255.252  
  clock rate 128000  
!  
interface Serial0/0/1  
  description Connection to BR2 S0/0/0.  
  ip address 172.16.254.9 255.255.255.252  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
control-plane  
!  
!  
banner motd ^C  
  Warning: Unauthorized access is prohibited!  
^C  
!
```

```
line con 0
 password 7 14141B180F0B
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 094F471A1A0A
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Router HQ (configuración final)

```
HQ#sh run
Building configuration...

Current configuration : 1554 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
no ip domain lookup
ip cef
no ipv6 cef
```

```
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  description LAN with 16,000 hosts.
  ip address 172.16.128.1 255.255.192.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  description LAN with 8,000 hosts.
  ip address 172.16.192.1 255.255.224.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  description Connection to BR1 S0/0/0.
  ip address 172.16.254.1 255.255.255.252
!
interface Serial0/0/1
  description Connection to BR2 S0/0/1.
  ip address 172.16.254.5 255.255.255.252
  clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
banner motd ^C
  Warning: Unauthorized access is prohibited!
^C
!
line con 0
  password 7 02050D480809
  login
line aux 0
```

```
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 00071A150754
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Router BR2 (configuración final)

```
BR2#sh run
Building configuration...

Current configuration : 1593 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BR2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
```

```
!  
interface GigabitEthernet0/0  
  description LAN with 500 hosts.  
  ip address 172.16.252.1 255.255.254.0  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  description LAN with 1,000 hosts.  
  ip address 172.16.248.1 255.255.252.0  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  description Connection to BR1 S0/0/1.  
  ip address 172.16.254.10 255.255.255.252  
  clock rate 128000  
!  
interface Serial0/0/1  
  description Connection to HQ S0/0/1.  
  ip address 172.16.254.6 255.255.255.252  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
control-plane  
!  
!  
banner motd ^C  
  Warning: Unauthorized access is prohibited!  
^C  
!  
line con 0  
  password 7 070C285F4D06  
  login  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  password 7 0822455D0A16  
  login  
  transport input all
```

```
!  
scheduler allocate 20000 1000  
!  
end
```

¿Puedes llamarme ahora? (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Calcular la máscara de subred necesaria para admitir una cierta cantidad de hosts.

La división en subredes es jerárquica y puede ayudar a entregar tráfico de la red con mayor facilidad si se diseñan grupos pequeños de direcciones IP para satisfacer las necesidades de la red.

Información básica/Situación

Nota: esta actividad se puede realizar de forma individual o en grupos pequeños o grandes utilizando el software Packet Tracer.

- Está configurando un esquema dedicado de direccionamiento de PC para las habitaciones de un hospital. El switch estará ubicado de manera central en la enfermería, ya que cada una de las cinco habitaciones estará conectada por cable de modo que los pacientes simplemente puedan conectarse a un puerto RJ-45 incorporado en la pared de su habitación. Diseñe una topología física y lógica para solo uno de los seis pisos con los siguientes requisitos para el esquema de direccionamiento: hay seis pisos con cinco habitaciones de pacientes en cada piso, lo que da un total de 30 conexiones. Cada habitación necesita una conexión de red.
- Debe incorporarse división en subredes al esquema.
- Utilice un router, un switch y cinco estaciones host para fines de direccionamiento.
- Verifique que todas las PC puedan conectarse a los servicios internos del hospital.

Conserve una copia del esquema para compartirlo más adelante con la clase o la comunidad de aprendizaje. Esté preparado para explicar la forma en que se incorporarían la división en subredes y las transmisiones unicast, multicast y broadcast, y dónde podría utilizarse su esquema de direccionamiento.

Nota para el instructor: esta actividad de creación de modelos puede ser una asignación con calificación o sin calificar. El objetivo es revisar el dominio que tienen los estudiantes de las subredes jerárquicas y de la operación de las máscaras de subred. Como resultado de esta actividad, se puede facilitar un debate como repaso del capítulo.

Recursos necesarios

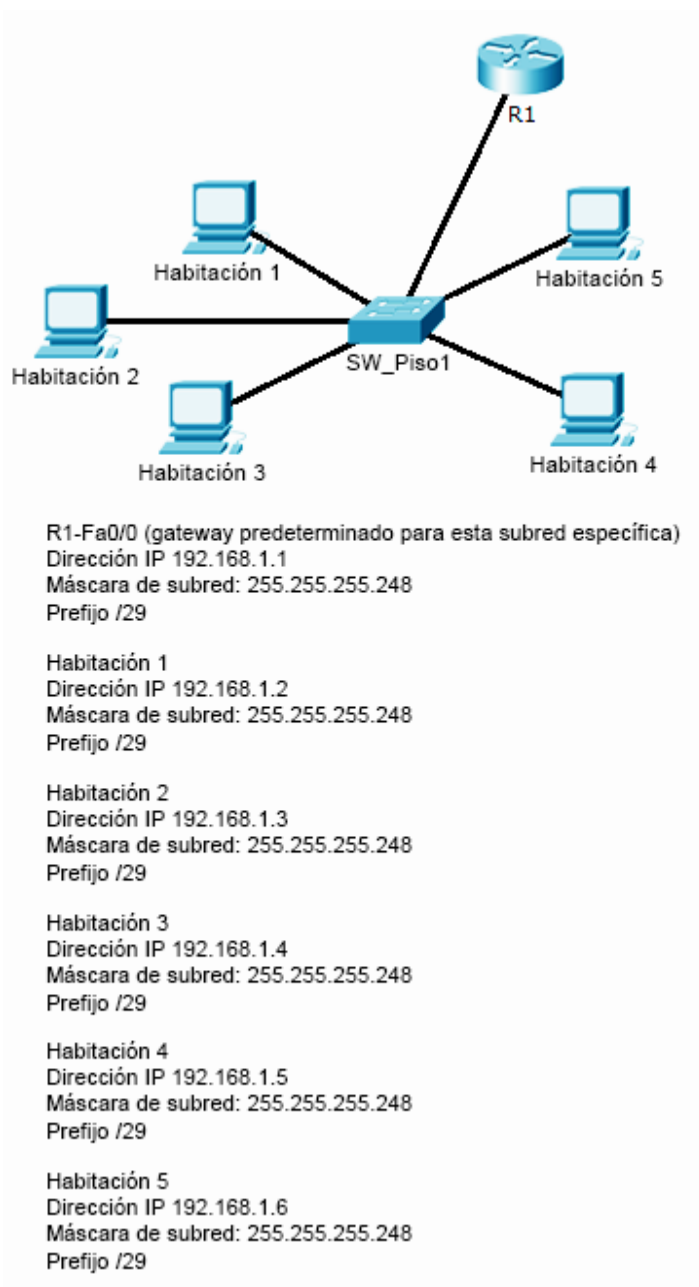
- Software Packet Tracer

Reflexión

1. ¿Cómo cambiaría su esquema de direccionamiento si fuera a agregar una conexión de red adicional a las habitaciones del hospital con un total de diez conexiones por piso o dos puertos por habitación?

Si la cantidad de conexiones de red se duplicara, se necesitaría la máscara de subred 255.255.255.240 con el prefijo /28 para admitir la conectividad.

Otra solución posible para la actividad original podría ser la siguiente:



Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Cuando se utilizan esquemas de direccionamiento, se emplean jerarquías. Los pisos del hospital representan las subredes, y las conexiones de los pacientes representan las direcciones de host.
- La conectividad se ve influenciada por los identificadores de los esquemas de direccionamiento. El switch representa un dispositivo intermediario válido para el procesamiento de datos entre dispositivos finales con direcciones estáticas.

Qué sucedería si... (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar el funcionamiento de la capa de aplicación en cuanto a dar soporte a las aplicaciones de usuario final.

- Los estudiantes imaginarán cómo sería no tener aplicaciones de red disponibles en el lugar de trabajo. También podrán estimar cuál sería el costo de no poder utilizar las aplicaciones conectadas en red por un período breve.

Información básica/Situación

Comienza la semana laboral. Su empleador decidió instalar teléfonos IP en el lugar de trabajo, lo que provocó que la red se encuentre fuera de servicio hasta la semana próxima.

Sin embargo, usted debe continuar con su trabajo. Tiene correos electrónicos que enviar y cotizaciones que preparar para obtener la aprobación del gerente. Debido a posibles problemas de seguridad, no tiene permitido finalizar el trabajo de la compañía utilizando sistemas informáticos o equipos de computación personales o externos, o equipos y sistemas que se encuentren en otra ubicación.

El instructor puede solicitarle que complete las preguntas de las dos situaciones que se presentan a continuación o que elija una de ellas (A. Correos electrónicos, o B. Cotización para obtener la aprobación del gerente). Responda las preguntas para las situaciones de forma completa. Esté preparado para comentar sus respuestas en clase.

A. Correos electrónicos

- ¿Qué métodos puede utilizar para enviar comunicaciones por correo electrónico?
- ¿Cómo puede enviar el mismo correo electrónico a varios destinatarios?
- ¿Cómo enviaría un archivo adjunto grande a varios destinatarios, en caso de ser necesario?
- ¿Estos métodos son rentables para la compañía?
- ¿Infringen alguna política de seguridad de la compañía?

B. Cotización para obtener la aprobación del gerente.

- Tiene un paquete de software de aplicaciones de escritorio instalado en su PC. ¿Será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? ¿Qué limitaciones experimentará al intentar finalizar la cotización?
- ¿Cómo presentará la cotización al gerente para obtener su aprobación? ¿Cómo cree que el gerente enviará la cotización al cliente para que la apruebe?
- ¿Estos métodos son rentables para la compañía? Justifique su respuesta.

Nota para el instructor: esta actividad de creación de modelos es de carácter introductorio; el objetivo es centrarse en cuán necesaria es la capa de aplicación para que las redes funcionen de forma eficaz. Para ahorrar tiempo de clase (para el debate), los estudiantes pueden completar una sola de las dos situaciones.

Reflexión

1. ¿Qué pasos identificó como importantes para la comunicación sin tener aplicaciones de red disponibles durante una semana en el lugar de trabajo? ¿Qué pasos no fueron importantes? Justifique su respuesta.

Entre algunas de las alternativas para resolver este problema, se podrían incluir:

Correos electrónicos:

¿Qué métodos puede utilizar para enviar comunicaciones por correo electrónico? La correspondencia podría tener que adoptar el formato de entrega de cada mensaje por correo postal regular o en mano. También podrían usarse el formato manuscrito, la copia impresa localmente, etc.

¿Cómo puede enviar el mismo correo electrónico a varios destinatarios? Una vez finalizada la carta manuscrita (per se), tendrían que hacerse copias para todos los destinatarios. Luego, las copias se enviarían individualmente a los destinatarios.

Si fuera necesario enviar un archivo adjunto grande, ¿qué haría para que llegue a varios destinatarios? Tendrían que hacerse varias copias del documento adjunto grande para enviar junto con la carta producida localmente.

¿Estos métodos son rentables para la compañía? No. Preparar el correo y el archivo adjunto para la entrega demandaría mucho tiempo, recursos y pasos.

Cotización para obtener la aprobación del gerente.

Tiene un paquete de software de aplicaciones de escritorio instalado en su PC. ¿Será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? Sí, el software de aplicación local no se vería afectado por no tener acceso a la red.

Cuando termine de redactar la cotización, ¿cómo la presentará al gerente para obtener su aprobación? ¿Cómo enviará el gerente la cotización al cliente para que la evalúe y la apruebe? La cotización deberá imprimirse (o guardarse en dispositivos multimedia). La copia impresa (o la copia en dispositivos multimedia) deberá entregarse personalmente al gerente. Es probable que sea necesario utilizar el correo postal en este ejemplo.

¿Estos métodos son rentables para la compañía? No. Imprimir la cotización, entregarla al gerente, prepararla para su entrega en la oficina de correos, etc. llevaría mucho tiempo.

Identifique los elementos del modelo que corresponden a contenido de TI:

- Las aplicaciones de red facilitan la comunicación en el lugar de trabajo.
- Las aplicaciones de red afectan la cantidad de trabajo que se realiza diariamente.
- El tiempo de procesamiento aumenta sin el uso de las aplicaciones de red.
- Las aplicaciones de red reducen el costo de completar las comunicaciones comerciales.

Práctica de laboratorio: Investigación del intercambio de archivos punto a punto (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Identificar redes P2P, protocolos de intercambio de archivos y aplicaciones

Parte 2: Investigar los problemas del intercambio de archivos mediante P2P

Parte 3: Investigar litigios de derechos de autor relacionados con P2P

Información básica/Situación

La computación punto a punto (P2P) es una tecnología eficaz que tiene muchos usos. Las redes P2P se pueden utilizar para compartir e intercambiar música, películas, software y otro material electrónico.

El uso de redes P2P para subir, descargar o compartir material protegido por leyes de derechos de autor, como películas, música y software, puede infringir los derechos de los propietarios de los derechos de autor. En el contexto de intercambio de archivos P2P, puede producirse una infracción, por ejemplo, cuando una persona compra una copia autorizada y luego la sube a una red P2P para compartirla con otros. Pueden considerarse que tanto la persona que proporciona el archivo como las que hacen las copias infringen los derechos de autor, y también es posible que infrinjan la ley de derechos de autor.

Otro problema con el intercambio de archivos P2P es que se cuenta con muy poca protección para asegurar que los archivos intercambiados en estas redes no sean malintencionados. Las redes P2P son un medio ideal para propagar malware (virus de computadora, gusanos, caballos de Troya, spyware, adware y otros programas malintencionados). En 2010, Cisco informó aumentos en la actividad de P2P, sumado a recientes desarrollos de malware P2P, lo que sugirió que los usuarios y atacantes de malware por igual están favoreciendo cada vez más los intercambios de archivos P2P.

En esta práctica de laboratorio, investigará el software disponible de intercambio de archivos P2P e identificará algunos problemas que pueden surgir del uso de esta tecnología.

Recursos necesarios

Dispositivo con acceso a Internet

Parte 1: Identificar redes P2P, protocolos de intercambio de archivos y aplicaciones

En la parte 1, investigará redes P2P e identificará algunos protocolos y aplicaciones P2P conocidos.

Paso 1: Definir redes P2P

a. ¿Qué es una red P2P?

Una red P2P permite que cada PC de la red actúe como un cliente o servidor para otras PC en la red, lo que permite el acceso compartido a diversos recursos sin necesidad de un servidor central.

- b. Indique algunas ventajas que ofrece P2P en comparación con la arquitectura cliente-servidor.

En las redes P2P, los clientes proporcionan recursos, entre los que se pueden incluir ancho de banda, espacio de almacenamiento y capacidad de cómputo. Esta propiedad es una de las principales ventajas de usar redes P2P, porque reduce en gran medida los costos de instalación y ejecución para el distribuidor de contenido original. A medida que los nodos llegan y la demanda en el sistema aumenta, la capacidad total del sistema también aumenta, y la probabilidad de fallas disminuye. Si un punto en la red no funciona correctamente, esto no comprometerá ni dañará toda la red. Por el contrario, con una arquitectura cliente-servidor típica, los clientes comparten solo sus demandas con el sistema, pero no sus recursos. En este caso, a medida que se suman clientes al sistema, hay menos recursos disponibles para servir a cada cliente, y si el servidor central falla, toda la red se perjudica. La naturaleza descentralizada de las redes P2P aumenta la solidez, porque quita el único punto de falla que puede ser inherente a un sistema cliente-servidor.

- c. Indique algunas desventajas de las redes P2P.

Una red P2P es descentralizada, lo que dificulta su administración. La seguridad es difícil de implementar y mantener, lo que favorece la posibilidad de transmisión de material protegido por leyes de derechos de autor y malware a través de una red P2P.

Paso 2: Identificar protocolos y aplicaciones de intercambio de archivos P2P

- a. Identifique algunos de los protocolos de intercambio de archivos P2P que se utilizan en la actualidad.

Las respuestas varían, pero pueden incluir: Ares, BitTorrent, Direct Connect, FastTrack, eDonkey, Gnutella, MANOLITO/MP2PN, OpenNap, 100BAo, Aimster, Applejuice, Freenet, GnucleusLAN GoBoogy, KuGoo, OpenFT, MUTE, Soribada, Soulseek, Xunlei.

- b. ¿Cuáles son algunas aplicaciones de intercambio de archivos P2P conocidas disponibles en la actualidad?

Las respuestas varían, pero pueden incluir: ABC [Yet Another Bit Torrent Client], Ares Galaxy, Azureus, BCD+++, BearShare, BitComet, BitSpirit, BitTornado, BitTorrent.Net, DC++, eMule, G3 Torrent, Gnutella, Gnucleus, Grokster, GTK-gnutella, iMesh, iMesh, Kazaa, LimeWire, Mactella, mIMAC, MLdonkey, Morpheus, Napigator, NeoModus Direct Connect, Overnet, QTorrent, Shareaza, uTorrent, Warez P2P, WinMX.

- c. ¿Qué protocolo de intercambio de archivos P2P se atribuye a la producción de la mayor parte del tráfico P2P en Internet en la actualidad?

Las respuestas pueden variar, pero la mayor parte del tráfico punto a punto probablemente sea de BitTorrent, después de la desaparición de LimeWire. Desde enero de 2012, unos 150 millones de usuarios activos utilizan BitTorrent (de acuerdo con BitTorrent, Inc.). En un instante determinado, BitTorrent tiene, en promedio, más usuarios activos que YouTube y Facebook combinados (esto se refiere a la cantidad de usuarios activos en un instante cualquiera y no a la cantidad total de usuarios exclusivos).

Parte 2: Investigar problemas del intercambio de archivos P2P

En la parte 2, investigará la infracción de derechos de autor relacionados con P2P e identificará otros problemas que pueden tener lugar al intercambiar archivos P2P.

Paso 1: Investigar la infracción de derechos de autor relacionados con P2P

- a. ¿Qué significa el acrónimo DMCA y a qué se refiere?

La Ley de derechos de autor para medios digitales en el nuevo milenio (DMCA) es una ley estadounidense sobre derechos de autor que implementa dos tratados de 1996 de la Organización Mundial de la Propiedad Intelectual (OMPI). Mediante esta ley, se declara ilegal la producción y la difusión de tecnología, dispositivos o servicios cuyo fin es evadir las medidas (comúnmente conocidas como “administración de derechos digitales”, o DRM) que controlan el acceso a las obras protegidas por leyes de derechos de autor. También declara ilegal el acto de evadir un control de acceso, ya sea que haya, o no, una infracción efectiva de los derechos de autor. Además, la DMCA aumenta las sanciones por infracción de los derechos de autor en Internet. Fue aprobada el 12 de octubre de 1998 por voto unánime del Senado de los Estados Unidos y ratificada por el presidente Bill Clinton el 28 de octubre de 1998.

- b. Nombre dos asociaciones que persiguen activamente la infracción de los derechos de autor relacionados con P2P.

La Asociación de la Industria Discográfica Americana (RIAA) y la Motion Picture Association of America (MPAA) interpusieron acciones legales contra una serie de individuos y sitios de intercambio de archivos P2P.

- c. ¿Cuáles son las sanciones por infringir los derechos de autor?

Las sanciones tanto civiles como penales pueden ser graves. Las sanciones civiles pueden incluir daños reales o daños legales (por un importe máximo de USD 30 000 por obra que se infringe). Además, el tribunal también puede adjudicar gastos y honorarios razonables de abogados y aumentar el monto por daños y perjuicios en caso de infracción voluntaria (por un importe máximo de USD 150 000 por obra que se infringe). Las sanciones penales pueden incluir multas y encarcelamiento.

- d. ¿Cuáles son las leyes de derechos de autor aplicables al intercambio de archivos en su área? ¿Son más estrictas o menos estrictas que las de otras áreas del mundo? ¿Con qué intensidad los organismos encargados de velar por el cumplimiento de las leyes en su área persiguen a aquellos que comparten material protegido por leyes de derechos de autor?

Las respuestas varían según la región.

Paso 2: Investigar otros problemas de P2P

- a. ¿Qué tipos de malware pueden transportarse en el intercambio de archivos P2P?

Las respuestas pueden variar, pero pueden incluir: adware, virus de computadora, spyware, caballos de Troya y gusanos.

- b. ¿Qué es “torrent poisoning”?

“Torrent poisoning” es el acto de compartir intencionalmente datos dañados o datos con nombres de archivo engañosos mediante el protocolo BitTorrent. Esta práctica de subir torrents falsos a veces es realizada por organizaciones antipiratería como intento de evitar el intercambio P2P de contenido protegido por leyes de derechos de autor y de reunir las direcciones IP de quienes realizan descargas.

- c. ¿Cómo podría ocurrir el robo de identidad mediante el uso de intercambio de archivos P2P?

Si el software de cliente P2P se configura incorrectamente, podría proporcionar acceso a información personal y a los archivos almacenados en la PC.

Parte 3: Investigar litigios por derechos de autor relacionados con P2P

En la parte 3, investigará e identificará algunas acciones legales históricas que tuvieron lugar como resultado de una infracción de derechos de autor relacionados con P2P.

- a. ¿Cuál fue la primera aplicación P2P reconocida que se especializaba en el intercambio de archivos MP3 y que fue inhabilitada por orden judicial?

Napster. Comenzó sus actividades en 1999 y en julio de 2001 fue inhabilitada por orden judicial. Shawn Fanning, John Fanning y Sean Parker fueron los cofundadores. En su mejor momento, tenía 25 millones de usuarios y 80 millones de canciones, y el sistema nunca colapsó.

- b. ¿Cuál fue uno de los litigios más grandes por intercambio de archivos P2P?

En mayo de 2011, el estudio jurídico Dunlap, Grubb and Weaver (también conocido como U.S. Copyright Group) inició el litigio más grande a BitTorrent, en el que se demandaba a 24 583 usuarios de BitTorrent por compartir la película Hurt Locker.

Reflexión

1. ¿Cómo puede estar seguro de que los archivos que descarga de las redes P2P no están protegidos por leyes de derechos de autor y están protegidos contra el malware?

No hay garantía absoluta de que los archivos P2P estén libres de malware y no estén protegidos por leyes de derechos de autor. Utilice las aplicaciones de intercambio de archivos P2P bajo su propia responsabilidad.

Práctica de laboratorio: Observación de la resolución DNS

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Observar la conversión de un URL en una dirección IP mediante DNS

Parte 2: Observar la búsqueda DNS mediante el comando nslookup en un sitio Web

Parte 3: Observar la búsqueda DNS mediante el comando nslookup en servidores de correo

Información básica/Situación

Cuando se escribe una dirección del localizador uniforme de recursos (URL), como <http://www.cisco.com>, en un explorador Web, se invoca el sistema de nombres de dominios (DNS). La primera parte del URL describe el protocolo que se utiliza. Los protocolos comunes son el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de hipertexto sobre la capa de sockets seguros (HTTPS) y el protocolo de transferencia de archivos (FTP).

El DNS utiliza la segunda parte de la dirección URL, que en este ejemplo es www.cisco.com. El DNS traduce el nombre de dominio (www.cisco.com) por una dirección IP para permitirle al host de origen llegar al host de destino. En esta práctica de laboratorio, observará el DNS en acción y utilizará el comando **nslookup** (búsqueda de nombre de servidor) para obtener información adicional de DNS. Trabaje con un compañero para completar esta práctica de laboratorio.

Recursos necesarios

1 PC (Windows 7, Vista o XP, con acceso a Internet y al símbolo del sistema)

Parte 1: Observar la conversión de un URL en una dirección IP mediante DNS

- Haga clic en el botón **Inicio de Windows**, escriba **cmd** en el campo de búsqueda y presione Entrar. Aparecerá la ventana de la petición de entrada de comandos.
- En el símbolo del sistema, haga ping al URL del Internet Corporation for Assigned Names and Numbers (ICANN), **www.icann.net**. ICANN coordina las funciones de DNS, de las direcciones IP, de la administración de nivel superior del sistema de nombres de dominio y de la administración del sistema de servidores raíz. La PC debe traducir www.icann.net por una dirección IP para saber adónde enviar los paquetes del protocolo de mensajes de control de Internet (ICMP).
- La primera línea del resultado muestra el nombre de dominio www.icann.net convertido en una dirección IP por el DNS. Debería poder ver el efecto del DNS, aun cuando haya un firewall instalado en la institución que impida la realización de pings o aun cuando el servidor de destino le haya impedido hacer ping a su servidor Web.


```
C:\>ping www.icann.net

Pinging www.icann.net [192.0.43.22] with 32 bytes of data:
Reply from 192.0.43.22: bytes=32 time=112ms TTL=241
Reply from 192.0.43.22: bytes=32 time=119ms TTL=241
Reply from 192.0.43.22: bytes=32 time=113ms TTL=241
Reply from 192.0.43.22: bytes=32 time=115ms TTL=241

Ping statistics for 192.0.43.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 112ms, Maximum = 119ms, Average = 114ms
```

Registre la dirección IP de www.icann.net. 192.0.43.22

- d. Escriba la dirección IP del **paso c** en un explorador Web, en lugar del URL. Observe que se muestra la página Web de inicio de ICANN.



A la mayoría de los seres humanos nos resulta más fácil recordar palabras que números. Si le indica a alguien que acceda a **www.icann.net**, probablemente lo recordará, pero si le indica que acceda a 192.0.43.22, le resultará difícil recordar una dirección IP. Las PC realizan procesos con números. El DNS es el proceso por el cual las palabras se traducen por números. Luego, se realiza una segunda traducción. Los seres humanos pensamos en números con base 10 (sistema decimal). Las computadoras procesan números con base 2 (sistema binario). La dirección IP 192.0.43.22 con base 10 es 11000000.00000000.00101011.00010110 con base 2. ¿Qué sucede si corta estos números con base 2 y los pega en un explorador?

El sitio Web no aparece. El código de software que se usa en los exploradores Web reconoce números con base 10, no reconoce números con base 2.

- e. Ahora escriba ping www.cisco.com.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.144.170] with 32 bytes of data:
Reply from 23.1.144.170: bytes=32 time=51ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58

Ping statistics for 23.1.144.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 51ms, Average = 50ms
```

- f. Cuando hace ping a www.cisco.com, ¿obtiene la misma dirección IP que la del ejemplo o una dirección IP diferente? ¿Por qué?
-
-

La respuesta varía según dónde se encuentre geográficamente. Cisco aloja su contenido Web en una serie de servidores reflejados. Esto significa que Cisco carga exactamente el mismo contenido en servidores distintos en términos geográficos (esparcidos por todo el mundo). Cuando alguien intenta acceder a www.cisco.com, el tráfico se dirige al servidor reflejado más cercano.

- g. Escriba la dirección IP que obtuvo cuando hizo ping a www.cisco.com en un explorador. ¿Aparece el sitio Web? ¿Por qué o por qué no?
-
-

El sitio Web **cisco.com** no aparece. Hay, al menos, dos explicaciones posibles: 1. Algunos servidores Web se configuran para que acepten direcciones IP que se envían desde un explorador; otros no. 2. Puede haber una regla de firewall en el sistema de seguridad de Cisco que prohíba el envío de una dirección IP a través de un explorador.

Parte 2: Observar la búsqueda DNS mediante el comando nslookup en un sitio Web

- a. En la petición de entrada de comandos escriba el comando **nslookup**.

```
C:\>nslookup
Default Server:  dslrouter.westell.com
Address:  192.168.1.1
>
```

¿Cuál es el servidor DNS predeterminado que se utiliza?

Depende del sitio

Observe que el símbolo del sistema cambió por el símbolo “mayor que” (>). Esta es la petición de entrada de **nslookup**. Desde aquí puede introducir comandos relacionados con el DNS.

En la petición de entrada, escriba ? para ver una lista de todos los comandos disponibles que puede utilizar en el modo **nslookup**.

- b. En la petición de entrada de **nslookup**, escriba **www.cisco.com**.

```
> www.cisco.com
Server:  dslrouter.westell.com
Address:  192.168.1.1

Non-authoritative answer:
Name:     e144.dscb.akamaiedge.net
Addresses: 2600:1408:7:1:9300::90
           2600:1408:7:1:8000::90
           2600:1408:7:1:9800::90
           23.1.144.170
Aliases:  www.cisco.com
           www.cisco.com.akadns.net
           wwwds.cisco.com.edgekey.net
           wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

¿Cuál es la dirección IP traducida? _____

Desde una ubicación específica, 23.1.144.170. La dirección IP de su ubicación probablemente sea distinta, porque Cisco utiliza servidores reflejados en diversas ubicaciones en todo el mundo.

¿Es la misma dirección IP que aparece con el comando **ping**? _____ **Sí**

Debajo de las direcciones, además de la dirección IP 23.1.144.170, aparecen los siguientes números: 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9800::90. ¿De qué se trata?

Son las direcciones IP IPv6, o IP versión 6, en las que se puede acceder al sitio Web.

- c. En la petición de entrada de comandos escriba la dirección IP del servidor Web de Cisco que acaba de encontrar. Si no conoce el URL, puede usar el comando **nslookup** para obtener el nombre de dominio de una dirección IP.

```
> 23.1.144.170
Server:  dslrouter.westell.com
Address: 192.168.1.1

Name:    a23-1-144-170.deploy.akamaitechnologies.com
Address: 23.1.144.170
```

Puede utilizar la herramienta **nslookup** para traducir nombres de dominio por direcciones IP. También puede utilizarla para traducir direcciones IP por nombres de dominio.

Mediante la herramienta **nslookup**, registre las direcciones IP asociadas con www.google.com.

La respuesta puede variar. En el momento de redactar este documento, las direcciones IP son 173.194.75.147, 173.194.75.105, 173.194.75.99, 173.194.75.103, 173.194.75.106, 173.194.75.104.

```
> www.google.com
Server:  dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses: 2607:f8b0:400c:c01::93
          173.194.75.147
          173.194.75.105
          173.194.75.99
          173.194.75.103
          173.194.75.106
          173.194.75.104
```

Parte 3: Observar la búsqueda DNS mediante el comando nslookup en servidores de correo

- a. En la petición de entrada, escriba **set type=mx** a fin de usar **nslookup** para identificar los servidores de correo.

```
> set type=mx
```

- b. En la petición de entrada, escriba **cisco.com**.

```
> cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
cisco.com      MX preference = 10, mail exchanger = rcdn-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = alln-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = ams-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = rtp-mx-01.cisco.com

ams-mx-01.cisco.com  internet address = 64.103.36.169
rcdn-mx-01.cisco.com internet address = 72.163.7.166
```

Un principio fundamental del diseño de red es la redundancia (la configuración de más de un servidor de correo). De esta manera, si no es posible acceder a uno de los servidores de correo, la PC que realiza la consulta intenta con el segundo servidor. Los administradores de correo electrónico determinan a qué servidor se contacta primero mediante **MX preference** (preferencia MX; consulte la imagen de arriba). Primero se contacta al servidor de correo con el valor de **MX preference** más bajo. Según el resultado de la imagen de arriba, ¿qué servidor se contactará primero cuando se envíe correo electrónico a cisco.com?

rcdn-mx-01.cisco.com

- c. En la petición de entrada de nslookup, escriba **exit** (salir) para volver al símbolo del sistema normal de la PC.
- d. En el símbolo del sistema de la PC, escriba **ipconfig /all**.
- e. Escriba las direcciones IP de todos los servidores DNS que utilice su escuela.

Depende del sitio

Reflexión

¿Cuál es el propósito fundamental del DNS?

Las personas realizan procesos con palabras. Las PC realizan procesos con números. A las personas les resulta difícil recordar una cadena larga de números. Por lo tanto, el DNS sirve para traducir el mundo de los "números" de las computadoras en el mundo de las "palabras" de las personas.

Práctica de laboratorio: Exploración del protocolo FTP

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Utilizar el protocolo FTP desde el símbolo del sistema

Parte 2: Descargar un archivo FTP usando WS_FTP LE

Parte 3: Utilizar el protocolo FTP en un explorador

Información básica/Situación

El protocolo de transferencia de archivos (FTP) es parte de la suite TCP/IP. FTP se utiliza para transferir archivos desde un dispositivo de red hasta otro. Windows incluye una aplicación de cliente FTP que se puede ejecutar desde el símbolo del sistema. También existen versiones gratuitas de interfaz gráfica de usuario (GUI) del protocolo FTP que se pueden descargar. Las versiones de GUI son más fáciles de usar que la escritura en la petición de entrada de comandos. El protocolo FTP se utiliza con frecuencia para transferir archivos que podrían ser muy grandes para adjuntarse a un correo electrónico.

Al usar FTP, una computadora normalmente actúa como servidor y la otra como cliente. Cuando se accede al servidor desde el cliente es necesario proporcionar un nombre de usuario y una contraseña. Algunos servidores FTP tienen un usuario denominado **anonymous** (anónimo). Para acceder a este tipo de sitios, simplemente se debe escribir "anonymous" en el campo de usuario, sin contraseña. Por lo general, el administrador del sitio presenta archivos que se pueden copiar, pero no permite que se carguen archivos con el usuario anónimo.

En esta práctica de laboratorio, aprenderá a utilizar un FTP anónimo desde el símbolo del sistema C:\> de la línea de comandos de Windows. También utilizará el programa FTP basado en GUI WS_FTP LE. Finalmente, utilizará un FTP anónimo en un explorador.

Recursos necesarios

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema y acceso a Internet, y WS_FTP LE instalado)

Parte 1: Utilizar el protocolo FTP desde el símbolo del sistema

Nota para el instructor: en esta práctica de laboratorio, se utiliza el sitio FTP anónimo para el Centro para el Control y la Prevención de Enfermedades de los EE. UU. Este sitio se eligió porque se mantiene actualizado. Si el instructor prefiere otro sitio FTP anónimo, encontrará una lista disponible en: <http://www.ftp-sites.org/> o puede realizar una búsqueda de "sitios FTP anónimos".

Nota para el instructor: dado que muchos lugares de estudio no tienen acceso a la petición de entrada C:\> o bien tienen políticas de seguridad que bloquean el protocolo FTP, los instructores podrán asignar esta práctica de laboratorio como tarea para el hogar o hacer una demostración en su PC, si la petición de entrada C:\> y el protocolo FTP están habilitados.

- Haga clic en el botón **Inicio de Windows**, escriba **cmd** en el campo de búsqueda y presione Entrar para abrir una ventana de comandos.
- En la petición de entrada C:\>, escriba **ftp ftp.cdc.gov**. En la petición de entrada que indica **User (ftp.cdc.gov:(none))**: escriba **anonymous**. Para la contraseña, no escriba nada. Presione Entrar para iniciar sesión como usuario anónimo.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Observe que la petición de entrada `C:\>` se reemplazó por la petición de entrada `ftp>`. Escriba **ls** para que aparezca una lista de los archivos y directorios. En el momento en que se creó esta práctica de laboratorio, había un archivo `Readme` (Léame).

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
```

- c. En la petición de entrada, escriba **get Readme**. De esta manera, el archivo se descarga en su equipo local desde el servidor FTP anónimo establecido por el Centro para el Control y la Prevención de Enfermedades. El archivo se copia al directorio que se muestra en la petición de entrada `C:\>` (`C:\Users\User1`, en este ejemplo).

Nota para el instructor: los estudiantes necesitan una carpeta en la que `ftp.exe` tenga acceso de lectura y escritura para descargar y ver el archivo `Readme` del sitio `ftp`. Como ejemplo, se utiliza la carpeta `C:\>Users\User1`.

```
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.00Seconds 1428000.00Kbytes/sec.
ftp>
```

- d. Escriba **quit** para salir del FTP y volver a la petición de entrada `C:\>`. Escriba **more Readme** para ver el contenido del documento.

```
ftp> quit
221

C:\Users\User1>more Readme

Welcome to the Centers for Disease Control and Prevention and Agency for
Toxic Substances and Disease Registry FTP server. Information maintained on
this server is in the public domain and is available at anytime for your use.
CDC/ATSDR requests that you provide a valid e-mail address when responding to
the FTP server's password prompt.

FTP POLICY

CDC/ATSDR's file structure is designed to make information easily accessible
for faster response. All FTP directories and sub-directories should contain
the following files:

      README.TXT          Contains general information and Disclaimer text.
                          <ASCII>
```

- e. ¿Cuál es una desventaja de utilizar el protocolo FTP desde la línea de comandos?

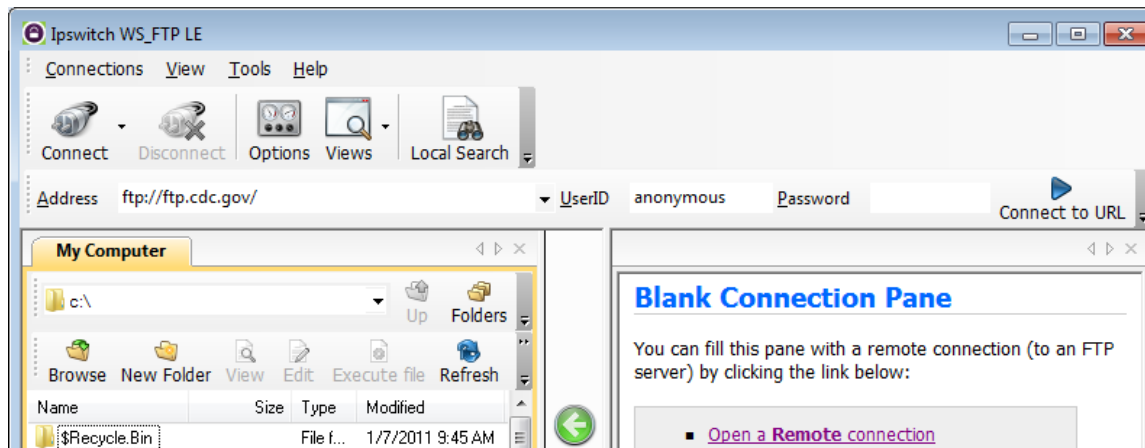
Descargar archivos de esta manera todo el tiempo puede volverse tedioso.

Parte 2: Descargar un archivo FTP usando WS_FTP LE

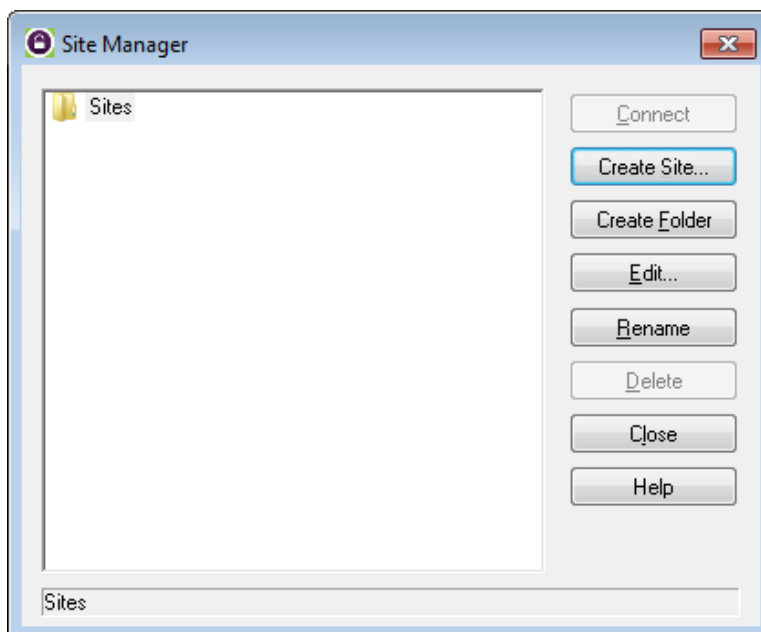
En la parte 2, descargará un archivo utilizando WS_FTP LE (una herramienta de transferencia FTP gratuita).

Nota para el instructor: los instructores deben instalar WS_FTP LE en cada PC de los estudiantes. En el momento en que se creó esta práctica, estaba disponible en: <http://www.wsftple.com/download.aspx>. Si este URL cambió, utilice su motor de búsqueda preferido para buscar “descargar WS_FTP LE” o “descargar FTP gratuito”.

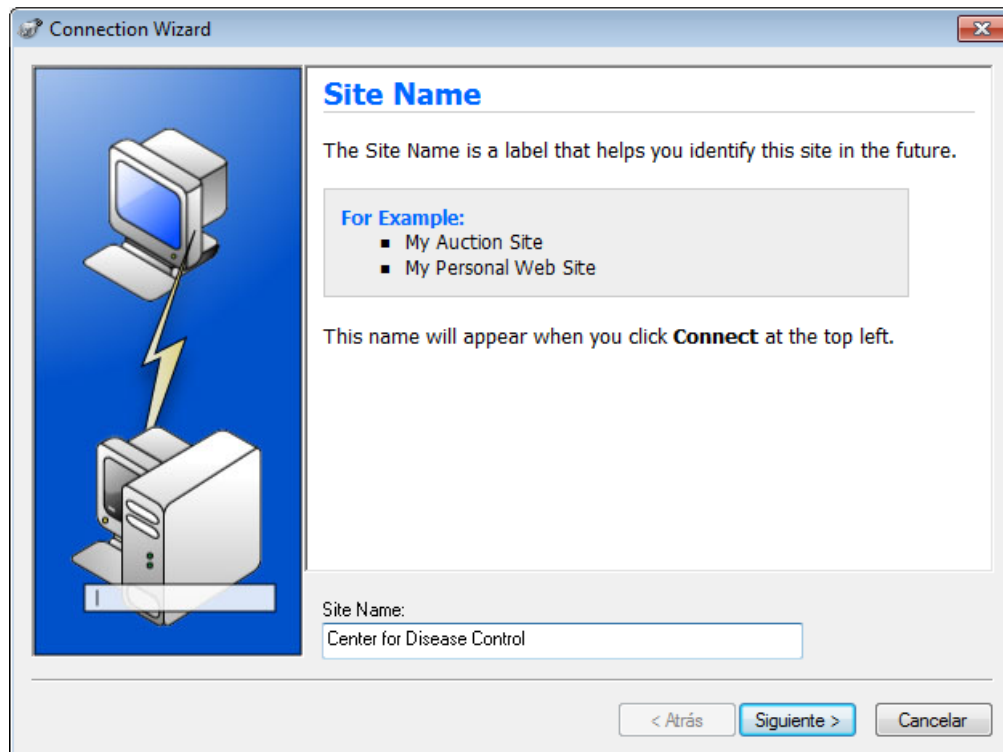
- a. Inicie **WS_FTP LE**. Si aparece la ventana Ipswitch WS_FTP LE, haga clic en **Next** (Siguiente) para continuar y pase al paso C. De lo contrario, haga clic en el enlace **Open a Remote Connection** (Abrir una conexión remota).



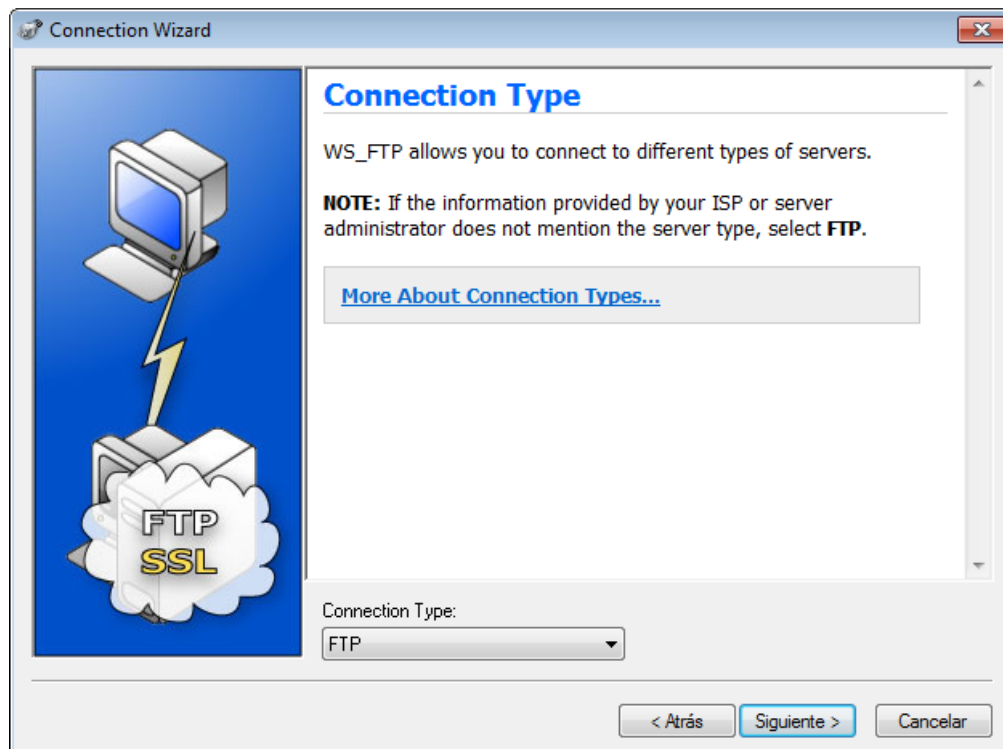
- b. Haga clic en **Create site...** (Crear sitio...).



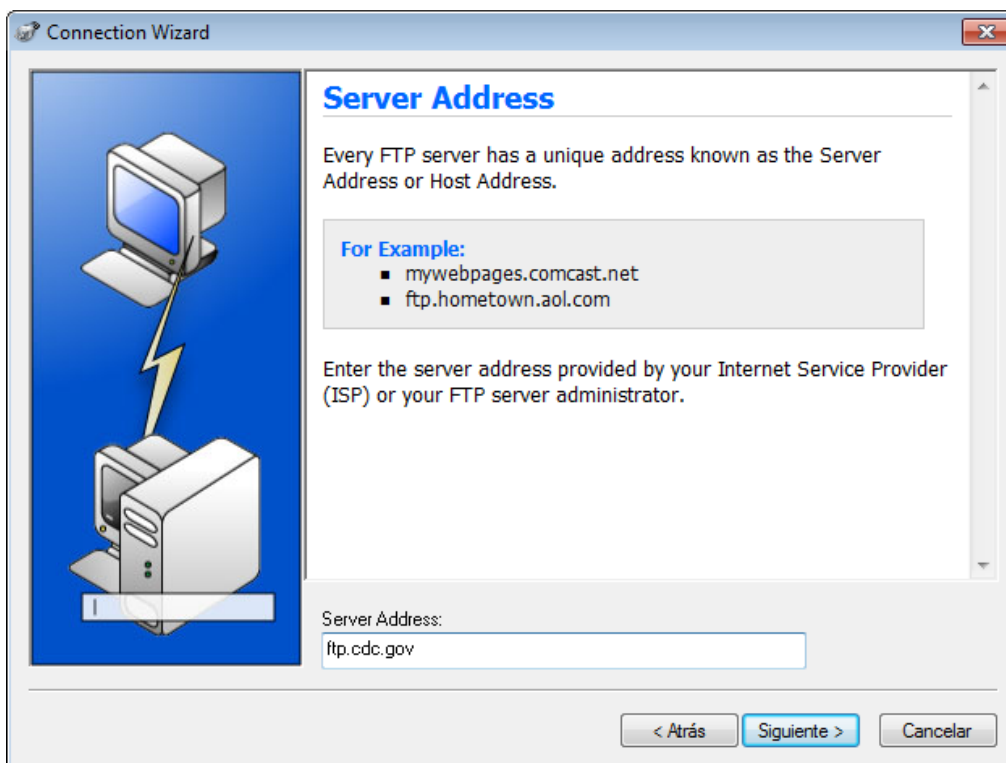
- c. En el campo **Site Name** (Nombre del sitio), escriba **Center for Disease Control** y haga clic en **Next** para continuar.



- d. Haga clic en la lista desplegable **Connection Type** (Tipo de conexión), seleccione **FTP** (el tipo de conexión predeterminado) y haga clic en **Next**.



- e. En el campo **Server Address** (Dirección de servidor), escriba <ftp.cdc.gov> y haga clic en **Next**.



The screenshot shows the 'Connection Wizard' window with the 'Server Address' tab selected. On the left, there is an illustration of a desktop computer connected to a server rack by a lightning bolt. The main text area explains that every FTP server has a unique address and provides two examples: 'mywebpages.comcast.net' and 'ftp.hometown.aol.com'. Below this, it instructs the user to enter the server address provided by their ISP or FTP server administrator. A text input field at the bottom contains 'ftp.cdc.gov'. At the bottom right, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'.

Server Address

Every FTP server has a unique address known as the Server Address or Host Address.

For Example:

- mywebpages.comcast.net
- ftp.hometown.aol.com

Enter the server address provided by your Internet Service Provider (ISP) or your FTP server administrator.

Server Address:
ftp.cdc.gov

< Atrás Siguiente > Cancelar

- f. En el campo **User Name** (Nombre de usuario), escriba **anonymous** y deje el campo de contraseña en blanco. Haga clic en **Next** (Siguiente).



The screenshot shows the 'Connection Wizard' window with the 'User Name and Password' tab selected. On the left, there is an illustration of a desktop computer connected to a server rack by a lightning bolt. The main text area explains that FTP servers require a user name and password and instructs the user to enter the user name and password provided by their ISP or FTP server administrator. A **NOTE** states that entering a password is not required and that WS_FTP will save the password for future connections. Below this, there are two text input fields: 'User Name' containing 'anonymous' and 'Password' which is empty. At the bottom right, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'.

User Name and Password

FTP servers require a user name and password.

Enter the user name and password provided by your Internet Service Provider (ISP) or the FTP server administrator.

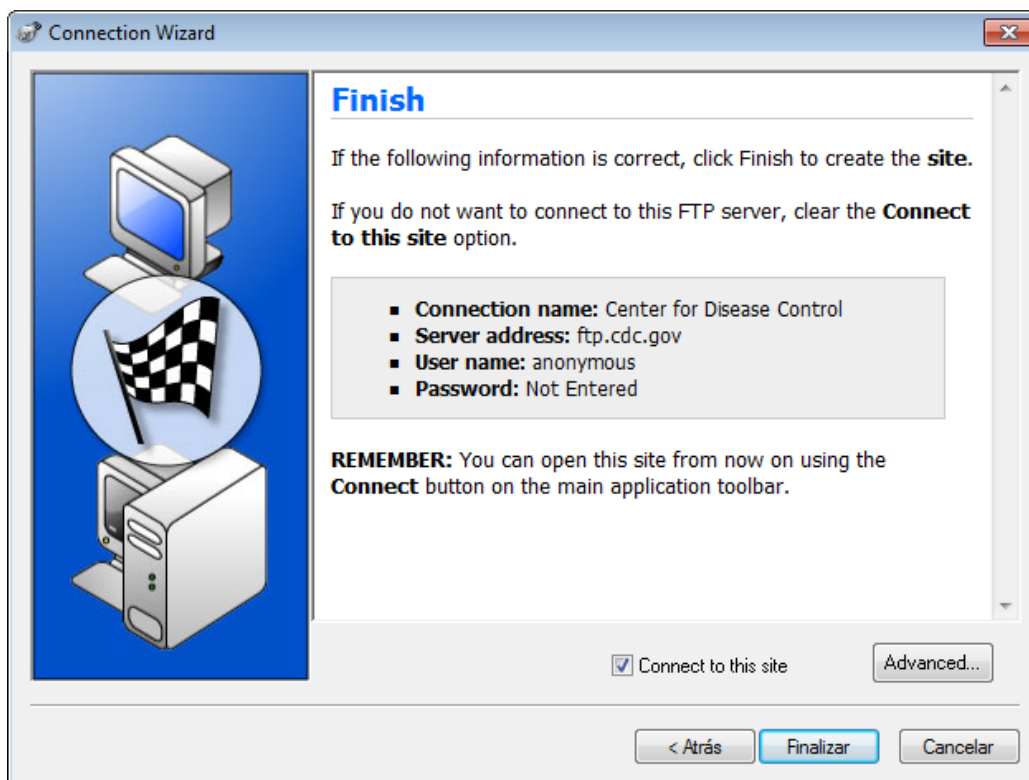
NOTE: Entering a password below is not required. If you choose to enter a password, WS_FTP will safely save that password for future connections to this site.

User Name:
anonymous

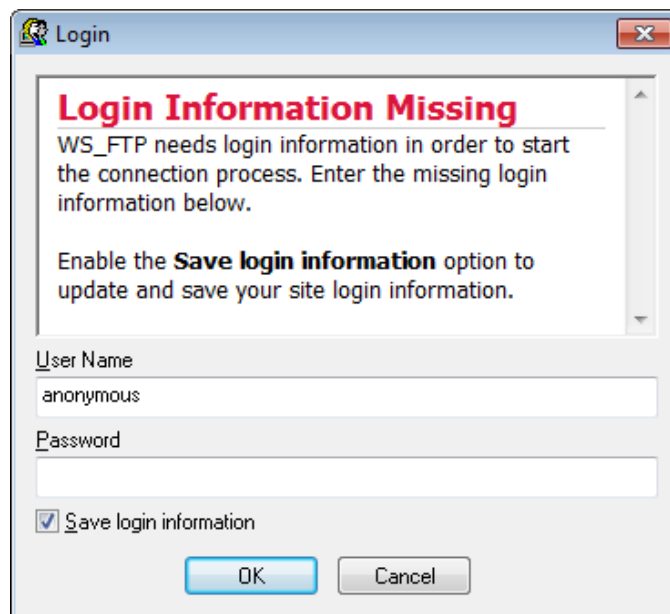
Password:

< Atrás Siguiente > Cancelar

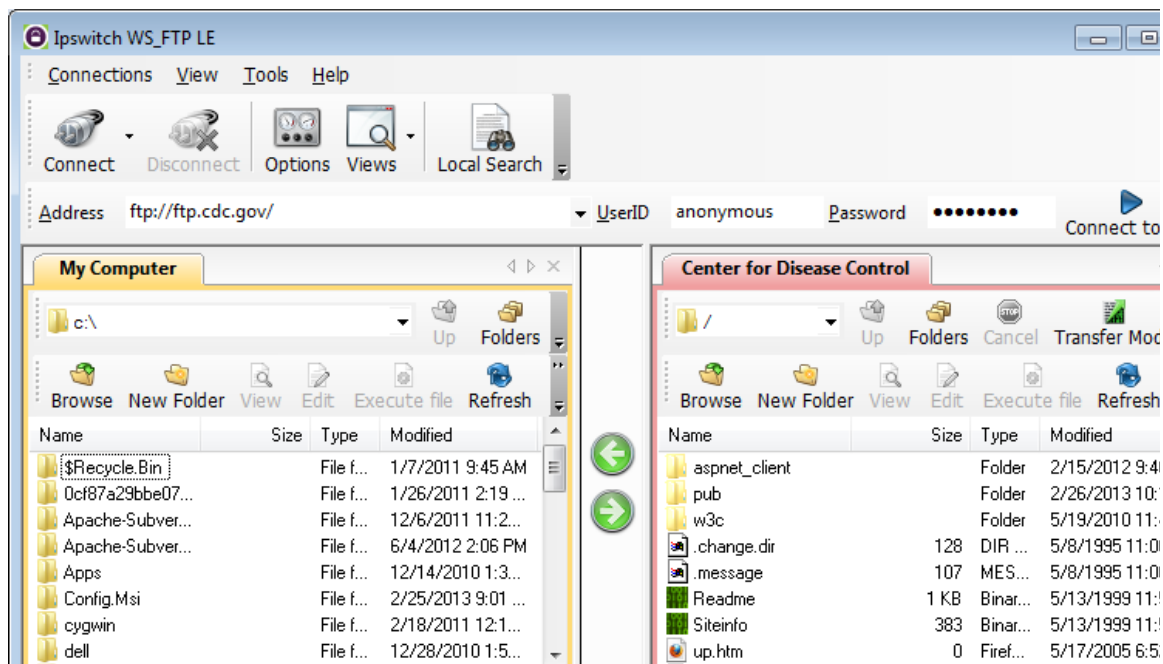
- g. Haga clic en **Finish** (Finalizar).



- h. Cuando aparezca el cuadro de diálogo Login Information Missing (Falta información de inicio de sesión), haga clic en **OK** (Aceptar). No escriba una contraseña en el campo **Password** (Contraseña).

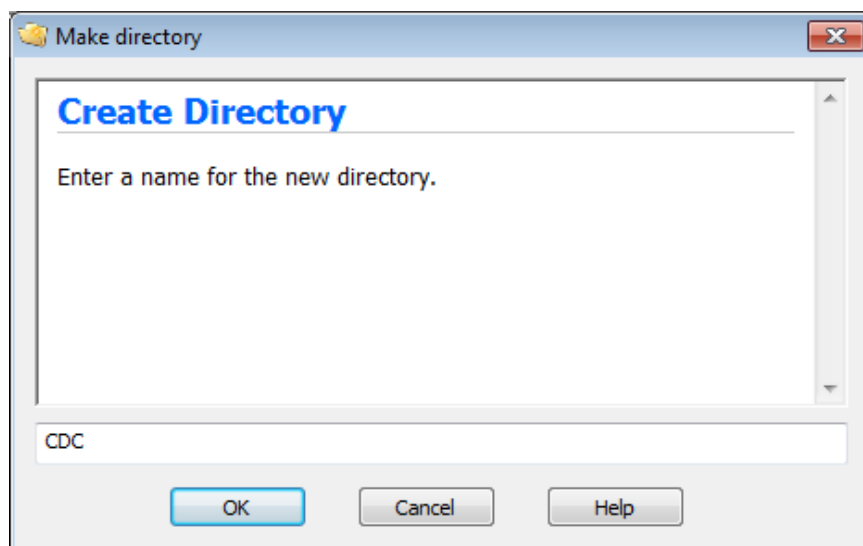


- i. Ahora está conectado al sitio FTP del Centro para el Control y la Prevención de Enfermedades en forma anónima.

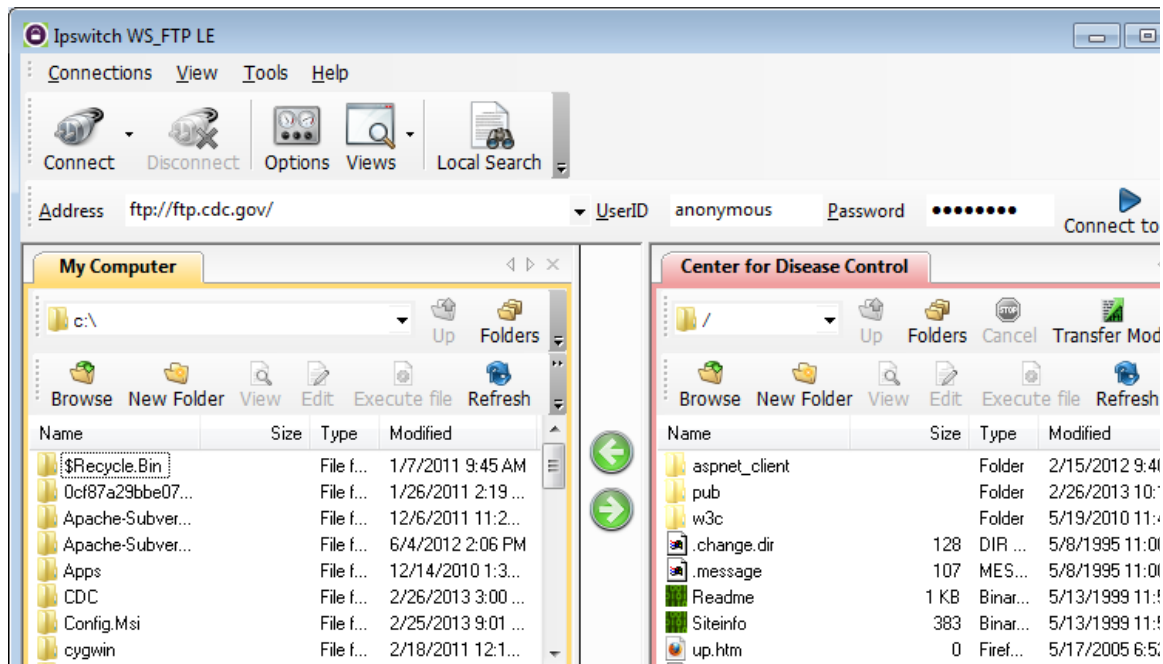


- j. En el menú de barra de herramientas de WS_FTP LE, debajo de Mi Computer (Mi PC), haga clic en **New Folder** (Carpeta nueva) para crear una carpeta en su unidad **C:** local.
- k. En el cuadro de diálogo Make Directory (Crear directorio), nombre la carpeta **CDC** y haga clic en **OK**.

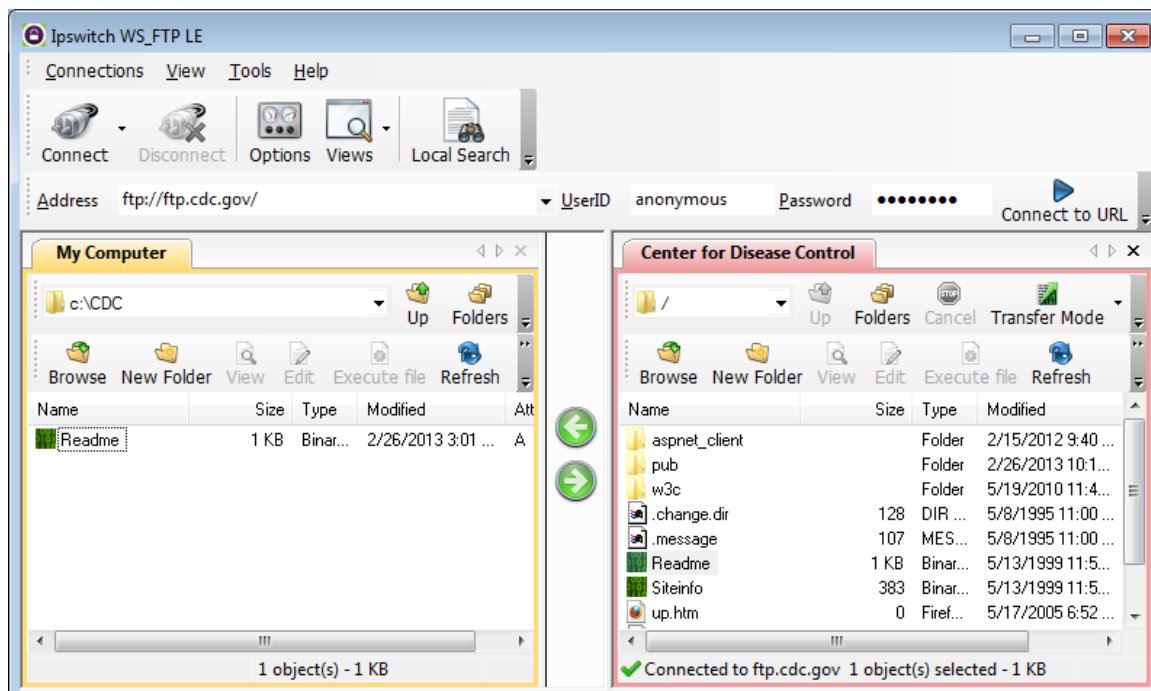
Nota: si la carpeta ya existe, puede usar la misma carpeta o crear otra con un nombre diferente. Si utiliza la misma carpeta CDC, puede reemplazar el archivo Readme existente con el archivo Readme descargado.



- l. Después de crear el directorio, en la página de la ficha **My Computer**, haga doble clic en el directorio para abrirlo.



- m. Arrastre el archivo **Readme** que está a la derecha de la aplicación (en el servidor FTP remoto del CDC) a la carpeta CDC que está en la unidad **C:** local.



- n. Haga doble clic en el archivo **Readme** en la carpeta **C:\CDC** de su unidad local **C:**. Si se le solicita una aplicación para abrir el documento, elija cualquier software de procesamiento de texto. Debería ver un mensaje similar al siguiente:

```
Welcome to the Centers for Disease Control and Prevention and
Agency for Toxic Substances and Disease Registry FTP server.
Information maintained on this server is in the public domain
and is available at anytime for your use.
```

- o. ¿Qué fue más fácil: usar el protocolo FTP desde la petición de entrada del **cmd** o usar WS_FTP LE?

Una vez instalada, es más fácil usar una aplicación FTP de GUI, como WS_FTP LE, en especial si se trabaja con una gran cantidad de archivos grandes.

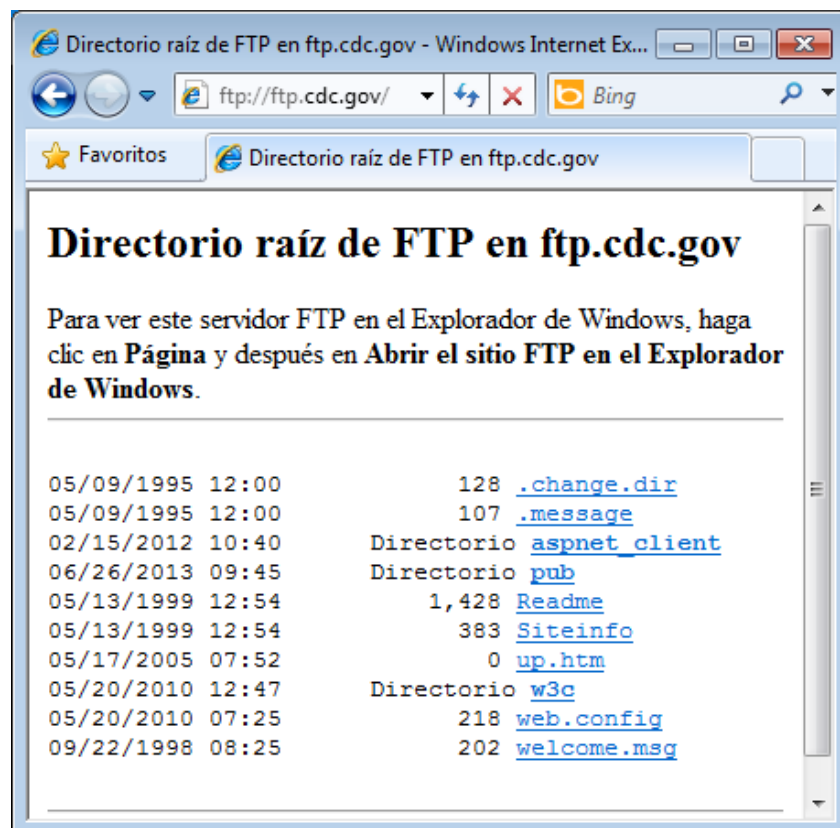
- p. Cuando termine, haga clic en **Disconnect** (Desconectar) para desconectarse del sitio [ftp.cdc.gov](ftp://ftp.cdc.gov).
- q. El sitio remoto se eliminará de la lista guardada de sitios FTP. En la ventana Ipswitch WS_FTP LE, haga clic en el enlace **Open a Remote Connection**. Seleccione el sitio **Center for Disease Control** y haga clic en **Delete** (Eliminar) para eliminar el sitio FTP. Haga clic en **Yes** (Sí) para confirmar la eliminación. Haga clic en **Close** (Cerrar) para salir del administrador de sitios.
- r. Elimine la carpeta **C:\CDC**.

Nota para el instructor: elimine la carpeta **C:\CDC** u otras carpetas que los estudiantes hayan creado en esta práctica de laboratorio.

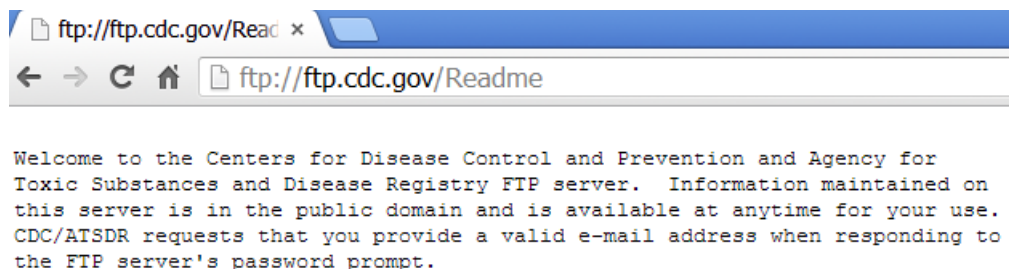
Parte 3: Utilizar el protocolo FTP en un explorador

Es posible utilizar un explorador como cliente FTP anónimo.

- a. En un explorador, escriba <ftp://ftp.cdc.gov/>.



- b. Haga clic en el archivo **Readme**.



Reflexión

1. ¿Qué método FTP fue más fácil de usar?

El explorador.

2. ¿Tuvo alguna ventaja utilizar el protocolo FTP desde el símbolo del sistema o utilizar WS_FTP LE?

Desde una perspectiva de facilidad de uso, el explorador claramente fue superior a los otros dos métodos. La única ventaja de los otros dos métodos es que brindan una vista más detallada de la interacción entre el software de cliente y el servidor FTP remoto. Esto resulta útil para comprender cómo funciona el protocolo FTP, pero no es un argumento convincente para utilizar cualquiera de esos métodos en la práctica.

Hágalo realidad (Versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar el funcionamiento de la capa de aplicación en cuanto a dar soporte a las aplicaciones de usuario final.

- Los estudiantes aplicarán el nuevo conocimiento sobre los protocolos de capa de aplicación y de los métodos de la capa TCP/IP a la optimización de la comunicación de datos y de la red.

Información básica/Situación

Consulte la actividad de creación de modelos que se encuentra al comienzo de este capítulo como base para esta actividad.

Los teléfonos IP se instalaron en media jornada, en lugar de tomar una semana completa como se previó inicialmente. Se restauró la capacidad total de la red, y las aplicaciones de red están disponibles para que las utilice. Tiene los mismos correos electrónicos que enviar y cotizaciones que preparar para obtener la aprobación del gerente.

Utilice la misma situación que completó en la actividad de creación de modelos introductoria para responder las siguientes preguntas:

A. Correos electrónicos

- ¿Qué métodos puede utilizar para enviar correspondencia electrónica ahora que la red funciona?
- ¿En qué formato se enviarán sus correos electrónicos a través de la red?
- ¿Cómo puede enviar el mismo mensaje a varios destinatarios ahora?
- ¿Cómo puede enviar los adjuntos grandes a varios destinatarios usando aplicaciones de red?
- ¿El uso de aplicaciones de red resultaría un método de comunicación rentable para la compañía?

B. Cotización para obtener la aprobación del gerente.

- Dado que tiene programas de aplicaciones de escritorio instalados en su PC, ¿será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? Justifique su respuesta.
- Cuando termine de redactar la cotización, ¿cómo la presentará al gerente para obtener su aprobación? ¿Cómo enviará el gerente la cotización al cliente para que la apruebe?
- ¿El uso de aplicaciones de red constituye un modo rentable de realizar transacciones comerciales? Justifique su respuesta.
- Conserve una copia impresa o una copia electrónica de sus respuestas. Esté preparado para comentar sus respuestas en clase.

Nota para el instructor: el objetivo de esta actividad de creación de modelos es revisar el contenido aprendido en el capítulo 4. El enfoque se centra en la forma en que la capa de aplicación utiliza las aplicaciones de red para funcionar de manera eficaz.

Para destinar tiempo de clase para el debate, se les puede asignar a los estudiantes que solo completen una situación (A. Correos electrónicos, o B. Cotización para obtener la aprobación del gerente).

Destaque que los estudiantes deben leer cuidadosamente el primer párrafo de esta actividad de creación de modelos para conocer los parámetros de la tarea.

Reflexión

1. Tener aplicaciones y servicios de red disponibles puede permitirle aumentar la producción, reducir los costos y ahorrar tiempo. ¿Esta afirmación sería verdadera en la situación que eligió? Justifique su respuesta.

Las respuestas representativas (para el debate) pueden ser similares a las siguientes:

Correos electrónicos:

- ¿Qué métodos puede utilizar para enviar correspondencia electrónica ahora que la red funciona? Probablemente, entrega de correo electrónico POP o IMAP junto con un programa de software de correo electrónico de red.
- ¿En qué formato se enviarán sus correos electrónicos a través de la red? POP o IMAP
- ¿Cómo puede enviar el mismo mensaje a varios destinatarios ahora? La MISMA copia del correo electrónico puede enviarse a varios destinatarios en cuestión de segundos.
- ¿Cómo puede enviar archivos adjuntos grandes a varios destinatarios por medio de las aplicaciones de red? Escribiendo el correo electrónico, dirigiéndolo a los destinatarios y enviando los archivos adjuntos grandes con el correo electrónico (sin necesidad de imprimir).
- ¿El uso de aplicaciones de red resultaría un método de comunicación rentable para la compañía? Este método ahorraría tiempo y recursos, y proporcionaría un producto orientado a la calidad (todos obtienen la misma información).

Cotización para obtener la aprobación del gerente:

- Tiene un procesador de texto, una hoja de cálculo y un programa de base de datos instalado en forma local en su PC. ¿Será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? En esta situación, el software de la estación de trabajo local ayudará a crear la cotización para el gerente sin afectar el costo.
- Cuando termine de redactar la cotización, ¿cómo la presentará al gerente para obtener su aprobación? Por lo general, se enviaría al gerente como correo electrónico con archivos adjuntos.
- ¿Cómo enviará el gerente la cotización al cliente para que la evalúe y la apruebe? Lo más probable es que se envíe un correo electrónico al cliente (aunque, a veces, se envía al cliente una copia adicional impresa o en formato multimedia de la cotización para su firma o aprobación).
- ¿El uso de aplicaciones de red constituye un modo rentable de realizar transacciones comerciales? Usar aplicaciones de red permite optimizar más el tiempo y, definitivamente, ahorrar recursos.

Identifique los elementos del modelo que corresponden a contenido relacionado con TI:

- Los costos asociados con la producción diaria de la empresa disminuyen al utilizar aplicaciones de red.
- Al trabajar con aplicaciones de red, el rendimiento del tiempo mejora.
- La comunicación de calidad mejora al utilizar aplicaciones de red.

¿Se dio cuenta? (Versión para el instructor)

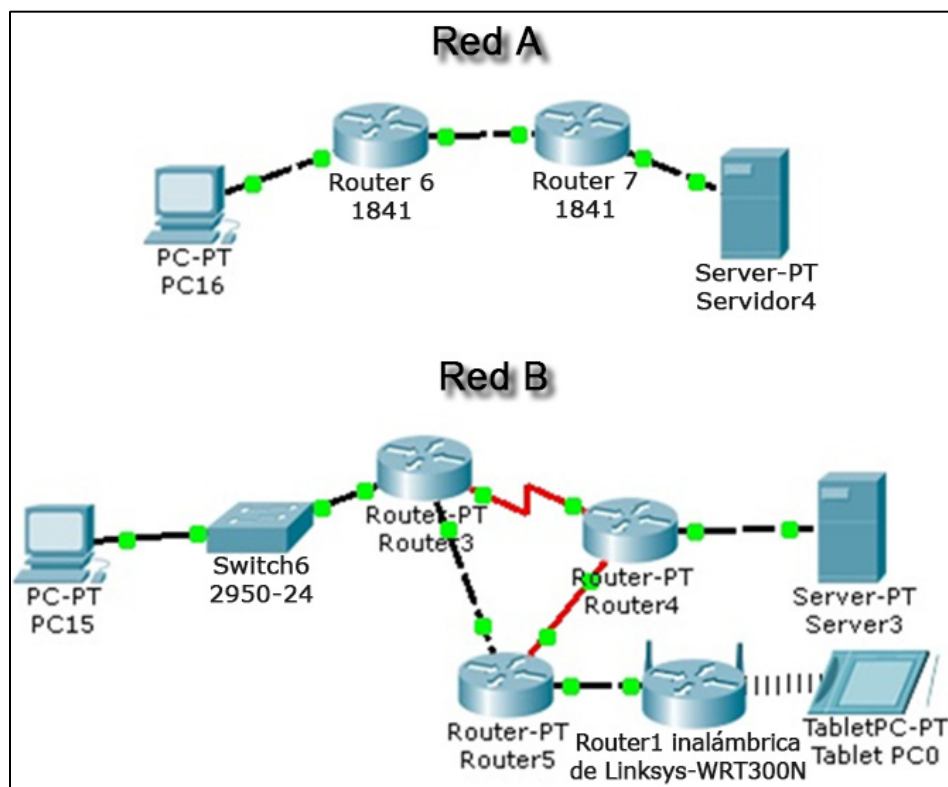
Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que se crea, se configura y se verifica una red pequeña de segmentos conectados directamente.

Los estudiantes observarán de qué manera las redes difieren tanto en tamaño como en función. Identificarán en qué forma las redes proporcionan soluciones diferentes según su costo, velocidad, puertos, capacidad de expansión y facilidad de administración, sobre la base de las necesidades de una pequeña a mediana empresa.

Topología



Información básica/Situación

Observe las dos redes del diagrama de topología. Responda las siguientes preguntas y registre las respuestas para compartirlas con la clase.

- Compare y contraste visualmente las redes A y B. ¿En qué sentido son iguales las dos redes?
- Tome nota de los dispositivos utilizados en cada diseño de red. Como los dispositivos están etiquetados, ya sabe qué tipos de dispositivos finales e intermediarios son. ¿En qué se diferencian las dos redes? ¿La cantidad de dispositivos presentes en una red es el único factor que las diferencia? Justifique su respuesta.
- ¿Qué red seleccionaría si tuviera una empresa de pequeña a mediana? Justifique la elección de la red según el costo, la velocidad, los puertos, la capacidad de expansión y la facilidad de administración.

Notas para el instructor: esta actividad de creación de modelos no tiene como fin ser una asignación con calificación. El objetivo es que los estudiantes observen las similitudes y diferencias con respecto al equipo de red que se muestra y los tipos de redes creados. El direccionamiento de las dos redes también debe ser un factor por considerar en las comparaciones de las dos redes. La facilitación del debate debe incluir conversaciones entre los estudiantes sobre el trabajo de cada uno.

Recursos necesarios

- Capacidades de registro (papel, tablet PC, etc.) para compartir los comentarios de reflexión con la clase.

Reflexión

1. Reflexione sobre sus comparaciones de las dos situaciones de red. ¿Qué elementos observó puntos de interés?

Varios estudiantes pueden seleccionar la red B como mejor red para una pequeña o mediana empresa, pero es posible que esta no sea necesariamente la mejor opción.

La red A es menos costosa en términos de equipos. Además, ofrece un diseño más sencillo, lo que debería contribuir a resolver problemas de velocidad de la red. Puesto que no hay un switch presente en esta red determinada, la capacidad de expansión podría ser un problema y estar limitada a los puertos que tienen los ISR. La administración sería fácil, ya que hay menos dispositivos para mantener actualizados y registrados.

La red B es más costosa que la A solo en términos de equipos. Proporciona redundancia, lo cual es importante para el costo de ejecución de las funciones empresariales. Permite la transmisión inalámbrica y no solo Ethernet, como se muestra en la red A, pero el hecho de incorporar tecnología inalámbrica aumenta la posibilidad de infracciones de seguridad, lo que aumenta las consideraciones de facilidad de administración. La velocidad podría mejorarse si los dispositivos usaran balanceo de carga y rutas estáticas para contribuir a dicha función. No sabemos qué tipos de routers incluye la red B. Si son routers serie 1841, en realidad el tráfico de datos podría lentificarse, pero esto depende de la ruta por la que se transfieren los datos de la red.

Por lo tanto, después de considerar todas las categorías, podría aceptarse el uso de cualquiera de las dos redes para una empresa pequeña o mediana. Las redes A y B ofrecen distintas ventajas y desventajas, y quedaría a consideración de la empresa pequeña o mediana priorizar el costo, la velocidad, los puertos, la capacidad de expansión y la facilidad de administración. Luego, a partir de su lista de prioridades y un plan a futuro, seleccionaría el mejor diseño para la empresa. Esto es similar a separar todas las sesiones en varias salas de conferencia según los temas.

Identifique los elementos del modelo que corresponden a contenido del mundo real:

- El costo, la velocidad, los puertos, la capacidad de expansión y la facilidad de administración son todos factores que se deben tener en cuenta al diseñar una red para una empresa pequeña o mediana.

Práctica de laboratorio: Investigación de amenazas de seguridad de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Explorar el sitio Web de SANS

- Navegar hasta el sitio Web de SANS e identifique los recursos.

Parte 2: Identificar amenazas de seguridad de red recientes

- Identificar diversas amenazas de seguridad de red recientes mediante el sitio de SANS.
- Identificar otros sitios, además de SANS, que proporcionen información sobre amenazas de seguridad de red.

Parte 3: Detallar una amenaza de seguridad de red específica

- Seleccionar y detallar una amenaza de red específica reciente.
- Presentar la información a la clase.

Información básica/Situación

Para defender una red contra ataques, el administrador debe identificar las amenazas externas que representan un peligro para la red. Pueden usarse sitios Web de seguridad para identificar amenazas emergentes y para proporcionar opciones de mitigación para defender una red.

Uno de los sitios más populares y confiables para la defensa contra amenazas de seguridad informática y de redes es el de SANS (SysAdministration, Audit, Networking and Security). El sitio de SANS proporciona varios recursos, incluida una lista de los 20 principales controles de seguridad críticos para una defensa cibernética eficaz y el boletín informativo semanal “@Risk: The Consensus Security Alert”. Este boletín detalla nuevos ataques y vulnerabilidades de red.

En esta práctica de laboratorio, navegará hasta el sitio de SANS, lo explorará y lo utilizará para identificar amenazas de seguridad de red recientes, investigará otros sitios Web que identifican amenazas, e investigará y presentará detalles acerca de un ataque de red específico.

Recursos necesarios

- Dispositivo con acceso a Internet
- PC para la presentación con PowerPoint u otro software de presentación instalado

Parte 1: Explorar el sitio Web de SANS

En la parte 1, navegue hasta el sitio Web de SANS y explore los recursos disponibles.

Paso 1: Localizar recursos de SANS.

Con un explorador Web, navegue hasta www.SANS.org. En la página de inicio, resalte el menú **Resources** (Recursos).

Indique tres recursos disponibles.

Reading Room (Sala de lectura), Webcasts (Transmisiones Web), Newsletters (Boletines informativos), Blogs, Top 25 Programming Errors (Los principales 25 errores de programación), Top 20 Critical Controls (Los principales 20 controles críticos), Security Policy Project (Proyecto de política de seguridad)

Paso 2: Localizar el recurso Top 20 Critical Controls.

El documento **Twenty Critical Security Controls for Effective Cyber Defense** (Los 20 controles de seguridad críticos para una defensa cibernética eficaz), incluido en el sitio Web de SANS, es el resultado de una asociación pública y privada entre el Departamento de Defensa de los EE. UU. (DoD), la National Security Association, el Center for Internet Security (CIS) y el instituto SANS. La lista se desarrolló para establecer el orden de prioridades de los controles de seguridad cibernética y los gastos para el DoD y se convirtió en la pieza central de programas de seguridad eficaces para el gobierno de los Estados Unidos. En el menú **Resources**, seleccione **Top 20 Critical Controls** (Los principales 20 controles críticos).

Seleccione uno de los 20 controles críticos e indique tres de las sugerencias de implementación para ese control.

Las respuestas varían. Critical Control 5: Malware Defenses. (Control crítico 5: Defensas contra malware) Employ automated tools to continuously monitor workstations, servers, and mobile devices. (Utilice herramientas automatizadas para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles). Employ anti-malware software and signature auto-update features. (Emplee software contra malware y funciones de actualización automática de firmas). Configure network computers to not auto-run content from removable media. (Configure equipos de red para que el contenido de los medios extraíbles no se ejecute automáticamente)

Paso 3: Localizar el menú Newsletter.

Resalte el menú **Resources** y seleccione **Newsletter** (Boletín informativo). Describa brevemente cada uno de los tres boletines disponibles.

SANS NewsBites. Resumen de alto nivel de los artículos periodísticos más importantes sobre la seguridad informática. El boletín se publica dos veces por semana e incluye enlaces para obtener más información.

@RISK: The Consensus Security Alert. Resumen semanal de nuevos ataques y vulnerabilidades de red. El boletín también proporciona detalles sobre la forma en que resultaron los ataques más recientes.

Ouch! Documento para despertar conciencia sobre la seguridad que proporciona a los usuarios finales información sobre cómo pueden ayudar a garantizar la seguridad de su red.

Parte 2: Identificar amenazas de seguridad de red recientes

En la parte 2, investigará las amenazas de seguridad de red recientes mediante el sitio de SANS e identificará otros sitios que contienen información de amenazas de seguridad.

Paso 1: Localizar el archivo del boletín informativo @Risk: Consensus Security Alert.

En la página **Newsletter** (Boletín informativo), seleccione **Archive** (Archivo) para acceder al archivo del boletín informativo @RISK: The Consensus Security Alert. Desplácese hasta **Archives Volumes** (Volúmenes de archivo) y seleccione un boletín semanal reciente. Repase las secciones **Notable Recent Security Issues y Most Popular Malware Files** (Problemas de seguridad recientes destacados y Archivos de malware más populares).

Enumere algunos ataques recientes. Examine varios boletines informativos recientes, si es necesario.

Las respuestas varían. Win.Trojan.Quarian, Win.Trojan.Changeup, Andr.Trojan.SMSsend-1, Java.Exploit.Agent-14, Trojan.ADH.

Paso 2: Identificar sitios que proporcionen información sobre amenazas de seguridad recientes.

Además del sitio de SANS, identifique otros sitios Web que proporcionen información sobre amenazas de seguridad recientes.

Las respuestas varían, pero podrían incluir www.mcafee.com/us/mcafee-labs.aspx, www.symantec.com/news.cnet.com/security/, www.sophos.com/en-us/threat-center/, us.norton.com/security_response/.

Enumere algunas de las amenazas de seguridad recientes detalladas en esos sitios Web.

Las respuestas varían. Trojan.Ransomlock, Inostealer.Vskim, Troyano, Fareit, Backdoor.Sorosk, Android.Boxer, W32.Changeup!gen35.

Parte 3: Detallar un ataque de seguridad de red específico

En la parte 3, investigará un ataque de red específico que haya ocurrido y creará una presentación basada en sus conclusiones. Complete el formulario que se encuentra a continuación con sus conclusiones.

Paso 1: Completar el siguiente formulario para el ataque de red seleccionado.

Nombre del ataque:	Code Red (Código rojo)
Tipo de ataque:	Gusano
Fechas de ataques:	Julio de 2001

Computadoras/organizaciones afectadas:	Se infectaron unas 359 000 computadoras en un día.
Cómo funciona y qué hizo:	
Nota para el instructor: la mayor parte de lo que sigue se extrajo de la versión en inglés de Wikipedia. El gusano “código rojo” se aprovechó de las vulnerabilidades de desbordamiento del búfer en Microsoft Internet Information Servers sin parches de revisión aplicados. Inició un código troyano en un ataque por negación de servicio contra direcciones IP fijas. El gusano se propagó utilizando un tipo común de vulnerabilidad conocida como desbordamiento del búfer. Utilizó una cadena larga que repetía el carácter “N” para desbordar un búfer, lo que luego permitía que el gusano ejecutara un código arbitrario e infectara la máquina. El contenido del gusano incluía lo siguiente: • Vandalizar el sitio Web afectado con el mensaje: HELLO! Welcome to http://www.worm.com! Hacked By Chinese! (¡HOLA! Bienvenido a http://www.worm.com. Pirateado por los chinos). • Intentó propagarse buscando más servidores IIS en Internet. • Esperó entre 20 y 27 días desde que se instaló para iniciar ataques DoS en varias direcciones IP fijas. Una de ellas fue la dirección IP del servidor Web de la Casa Blanca. • Mientras buscaba máquinas vulnerables, el gusano no revisaba si el servidor en ejecución en una máquina remota ejecutaba una versión vulnerable de IIS o si IIS se ejecutaba.	
Opciones de mitigación:	
Para evitar la explotación de la vulnerabilidad del IIS, las organizaciones necesitaron aplicar el parche de Microsoft para el IIS.	
Referencias y enlaces de información:	
CERT Advisory CA-2001-19 eEye Code Red advisory Code Red II analysis	

Paso 2: Siga las pautas para instructores para completar la presentación.

Reflexión

1. ¿Qué medidas puede tomar para proteger su propia PC?

Las respuestas varían, pero podrían incluir: mantener actualizados el sistema operativo y las aplicaciones con parches y paquetes de servicios mediante un firewall personal; configurar contraseñas para acceder al sistema y al BIOS; configurar protectores de pantalla con un tiempo de espera y con solicitud de contraseña; proteger los archivos importantes guardándolos como archivos de solo lectura; encriptar los archivos confidenciales y los archivos de respaldo para mantenerlos seguros.

2. ¿Cuáles son algunas medidas importantes que las organizaciones pueden seguir para proteger sus recursos?

Las respuestas varían, pero podrían incluir: el uso de firewalls, la detección y prevención de intrusiones, la protección de dispositivos de red y de terminales, herramientas de vulnerabilidad de red, educación del usuario y desarrollo de políticas de seguridad.

Práctica de laboratorio: Acceso a dispositivos de red mediante SSH (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Configurar el router para el acceso por SSH

Parte 3: Examinar una sesión de Telnet con Wireshark

Parte 4: Examinar una sesión de SSH con Wireshark

Parte 5: Configurar el switch para el acceso por SSH

Parte 6: Ejecutar SSH desde la CLI del switch

Información básica/Situación

En el pasado, Telnet era el protocolo de red más común utilizado para configurar dispositivos de red de manera remota. Sin embargo, los protocolos como Telnet no autentican ni encriptan la información entre el cliente y el servidor. Esto permite que un programa detector de redes intercepte contraseñas y la información de configuración.

Shell seguro (SSH) es un protocolo de red que establece una conexión de emulación de terminal segura a un router u otro dispositivo de red. SSH encripta toda la información que atraviesa el enlace de red y proporciona autenticación de la computadora remota. SSH está reemplazando rápidamente a Telnet como la herramienta de conexión remota preferida por los profesionales de red. SSH se utiliza con mayor frecuencia para conectarse a un dispositivo remoto y ejecutar comandos. Sin embargo, también puede transferir archivos mediante los protocolos de transferencia segura de archivos (SFTP) o de copia segura (SCP) asociados.

Para que SSH funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En esta práctica de laboratorio, habilitará el servidor SSH en un router y luego se conectará a ese router mediante una PC con un cliente SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP.

En esta práctica de laboratorio, configurará un router para que acepte conectividad de SSH y utilizará Wireshark para capturar y ver sesiones de Telnet y SSH. Esto demostrará la importancia de la encriptación con SSH. También se lo desafiará a que configure un switch para que tenga conectividad de SSH.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con Wireshark y programa de emulación de terminal — por ejemplo, Tera Term — instalados)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar el router.

- Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- Entre al modo de configuración.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configurar la PC-A

- Configure la PC-A con una dirección IP y una máscara de subred.
- Configure un gateway predeterminado para la PC-A.

Paso 5: Verificar la conectividad de la red.

Haga ping a R1 desde PC-A. Si el ping falla, resuelva los problemas en la conexión.

Parte 2: Configurar el router para el acceso por SSH

Usar Telnet para conectarse a un dispositivo de red es un riesgo de seguridad, porque toda la información se transmite en formato de texto no cifrado. SSH encripta los datos de sesión y proporciona autenticación del dispositivo, por lo que se recomienda SSH para las conexiones remotas. En la parte 2, configurará el router para que acepte conexiones SSH por las líneas VTY.

Paso 1: Configurar la autenticación del dispositivo

El nombre del dispositivo y el dominio se utilizan como parte de la clave de encriptación, cuando se genera. Por lo tanto, estos nombres deben introducirse antes de emitir el comando **crypto key**.

- Configure el nombre del dispositivo.

```
Router(config)# hostname R1
```

- Configure el dominio para el dispositivo.

```
R1(config)# ip domain-name ccna-lab.com
```

Paso 2: Configurar el método de la clave de encriptación

```
R1(config)# crypto key generate rsa modulus 1024
```

```
The name for the keys will be: R1.ccna-lab.com
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 1 seconds)
```

```
R1(config)#
```

```
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Paso 3: Configurar el nombre de usuario de una base de datos local

```
R1(config)# username admin privilege 15 secret adminpass
```

```
R1(config)#
```

```
*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjTlHbmYxZigc
```

```
R1(config)#
```

Nota: el nivel de privilegio 15 otorga al usuario derechos de administrador.

Paso 4: Habilitar SSH en las líneas VTY

- Habilite Telnet y SSH en las líneas VTY entrantes mediante el comando **transport input**.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input telnet ssh
```

- b. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Paso 5: Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Parte 3: Examinar una sesión de Telnet con Wireshark

En la parte 3, utilizará Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder al R1 mediante Telnet, se registrará y luego emitirá el comando show run en el router.

Nota: si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, debe instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) y PuTTY (www.putty.org).

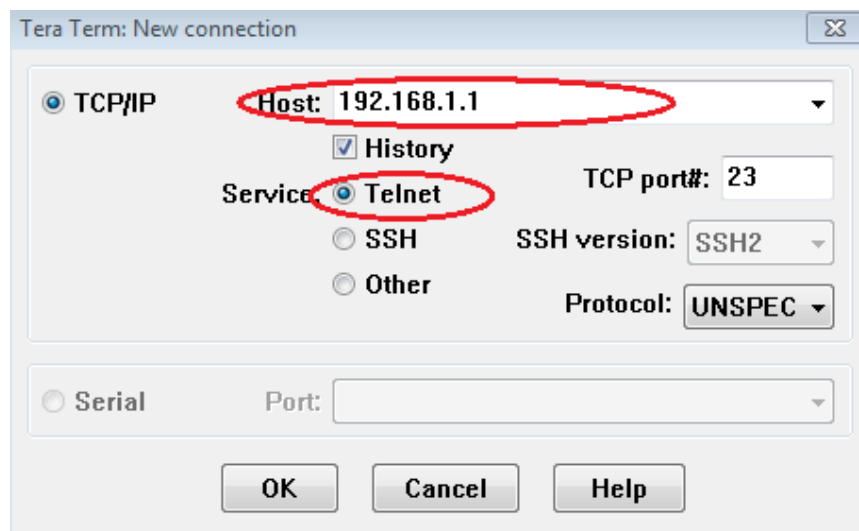
Nota: Telnet no está disponible de manera predeterminada mediante el símbolo del sistema de Windows 7. Para habilitar Telnet a fin de utilizarlo en la ventana del símbolo del sistema, haga clic en **Inicio > Panel de control > Programas > Programas y características > Activar o desactivar las características de Windows**. Haga clic en la casilla de verificación **Client Telnet** y, a continuación, haga clic en **Aceptar**.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

Nota: si no puede comenzar la captura en la interfaz LAN, necesitará abrir Wireshark mediante la opción **Run as Administrator** (Ejecutar como administrador).

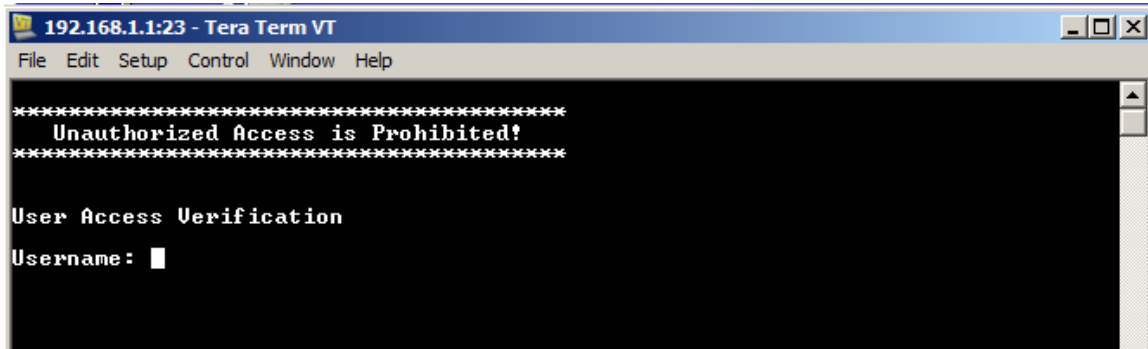
Paso 2: Iniciar una sesión de Telnet en el router

- a. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, introduzca **192.168.1.1**.



¿Cuál es el puerto TCP predeterminado para las sesiones de Telnet? _____ Puerto 23

- b. En la petición de entrada Username: (Nombre de usuario:), introduzca **admin**, y en la petición de entrada Password: (Contraseña:), introduzca **adminpass**. Estas peticiones de entrada se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando **login local**.



- c. Emita el comando **show run**.

R1# **show run**

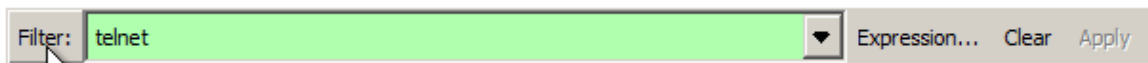
- d. Introduzca **exit** para salir de la sesión de Telnet y de Tera Term.

R1# **exit**

Paso 3: Detener la captura de Wireshark



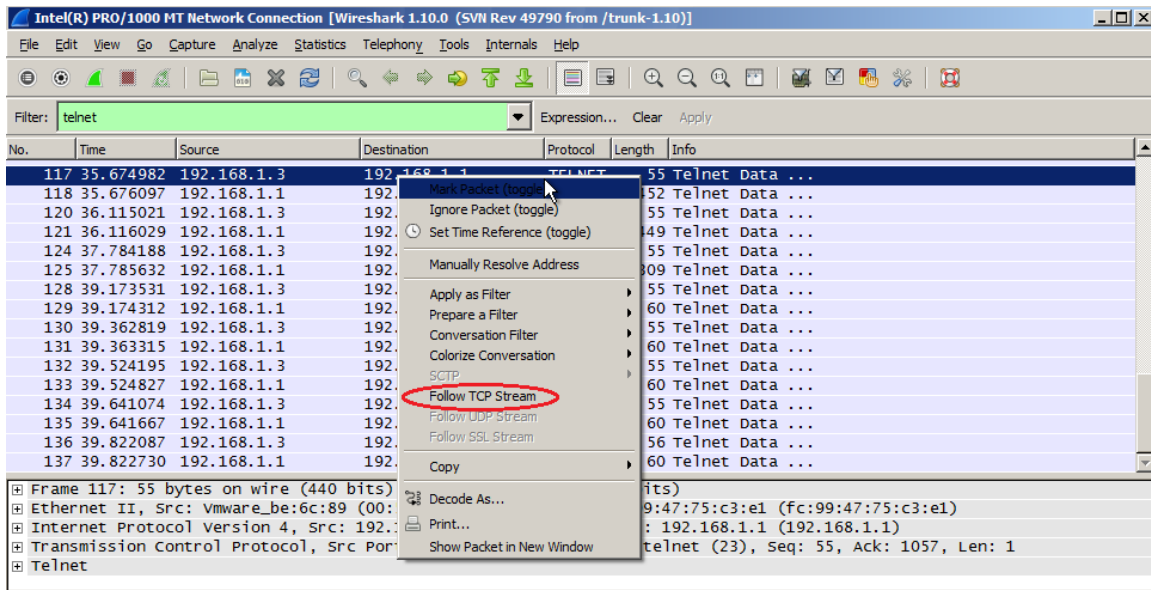
Paso 4: Aplicar un filtro de Telnet a los datos de captura de Wireshark



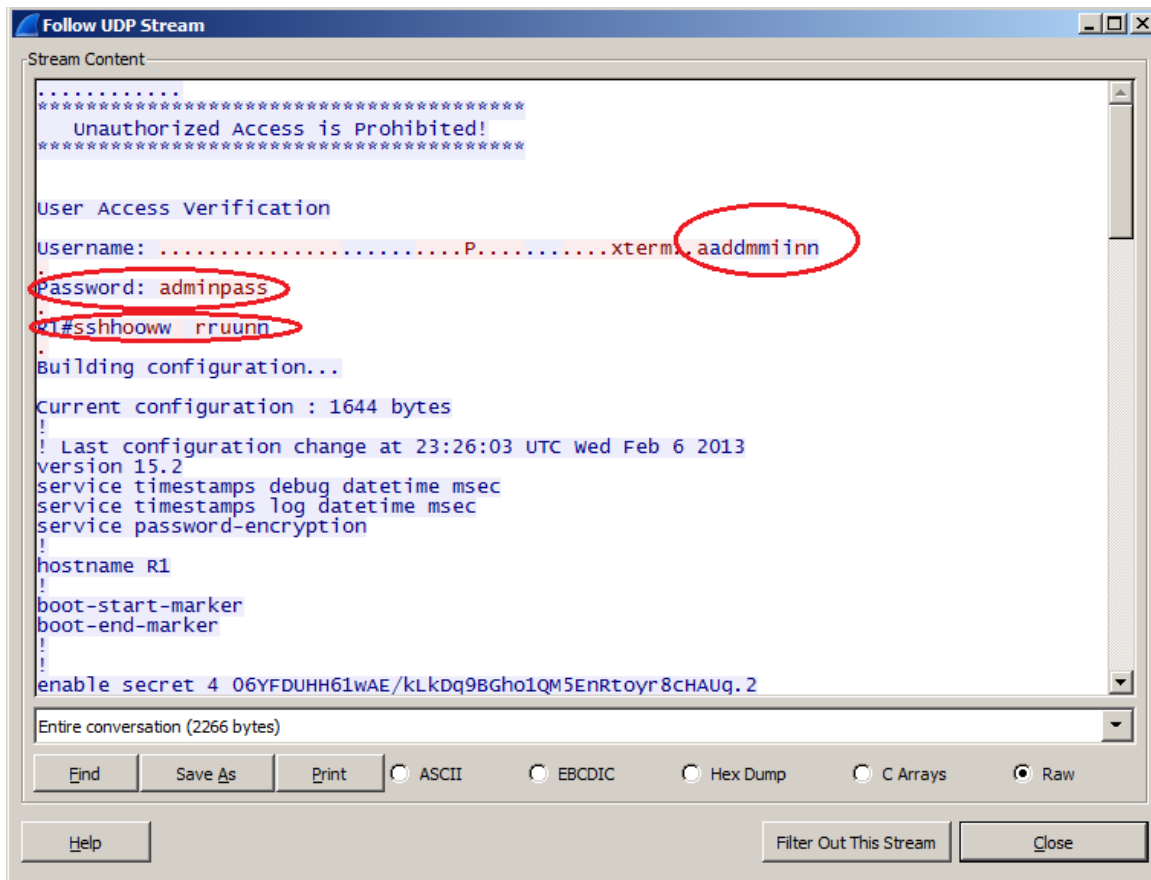
Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

- a. Haga clic con el botón secundario en una de las líneas **Telnet** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).

Práctica de laboratorio: Acceso a dispositivos de red mediante SSH



- b. En la ventana Follow TCP Stream, se muestran los datos para su sesión de Telnet con el router. Toda la sesión, incluida la contraseña, se muestra como texto no cifrado. Observe que el nombre de usuario y el comando **show run** que introdujo se muestran con caracteres duplicados. Esto lo causa el ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.



- c. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream**, haga clic en **Close** (Cerrar).

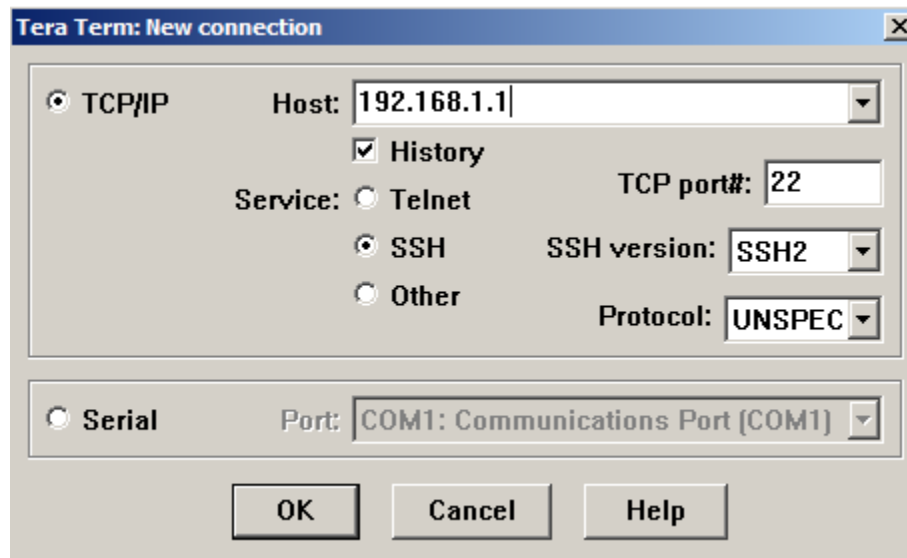
Parte 4: Examinar una sesión de SSH con Wireshark

En la parte 4, utilizará el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

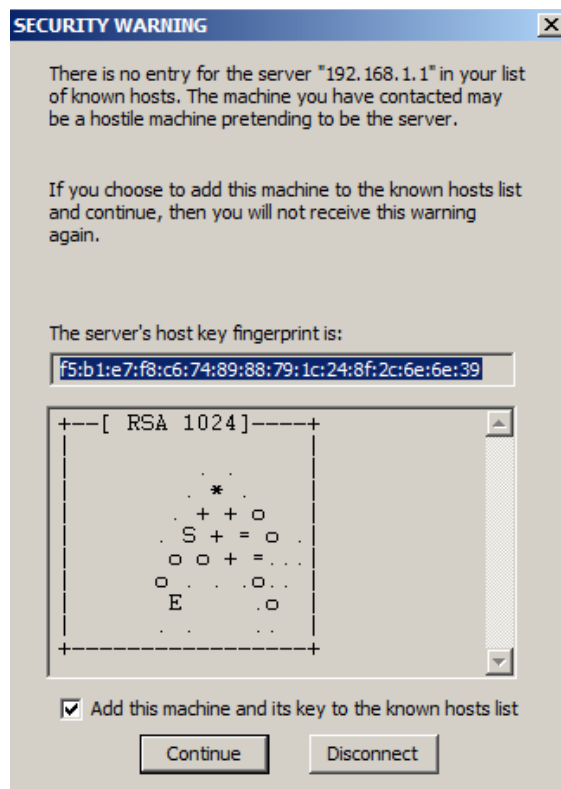
Paso 2: Iniciar una sesión de SSH en el router

- a. Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **SSH** esté seleccionado y, a continuación, haga clic en **OK** (Aceptar) para conectarse al router.

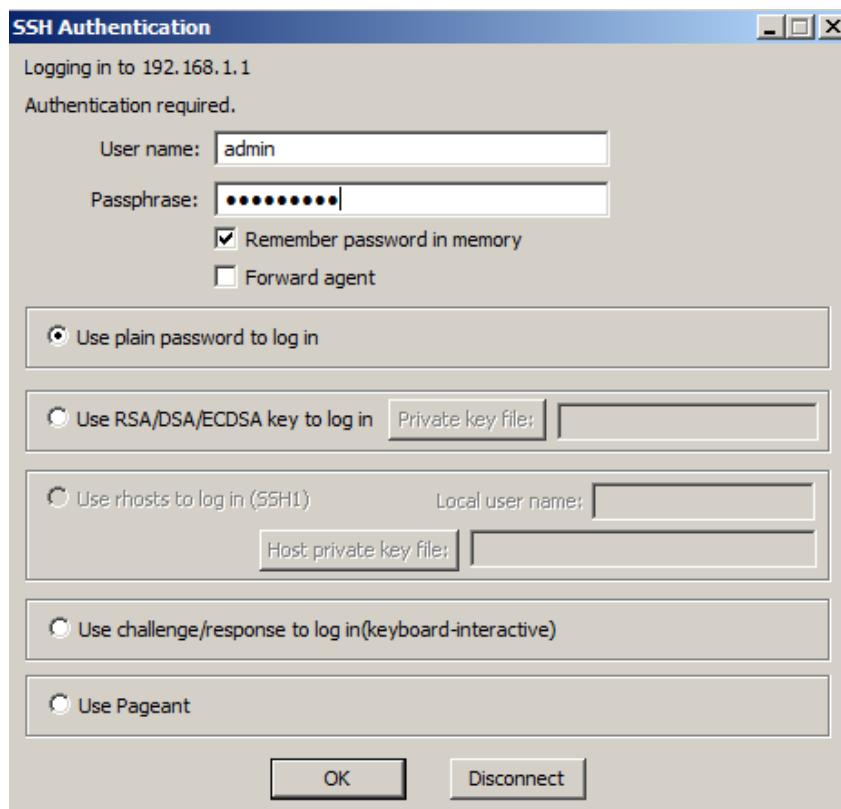


¿Cuál es el puerto TCP predeterminado que se utiliza para las sesiones de SSH? _____
Puerto 22

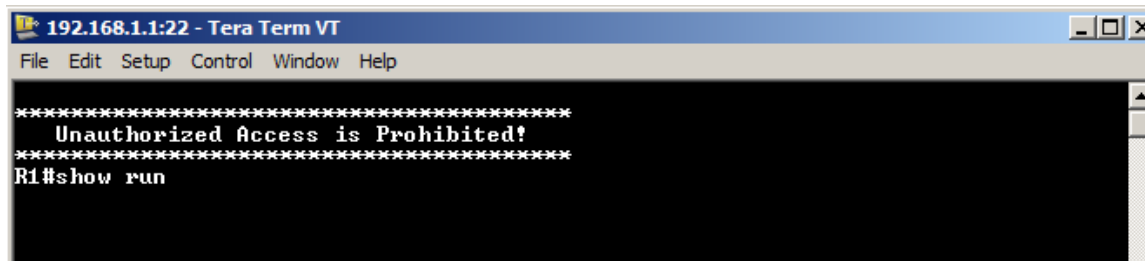
- b. La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (ADVERTENCIA DE SEGURIDAD) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y, luego, haga clic en **Continue** (Continuar).



- c. En la ventana de la autenticación de SSH, introduzca **admin** en User name (Nombre de usuario) y **adminpass** en Passphrase (Frase de contraseña). Haga clic en **OK** (Aceptar) para registrarse en el router.



- d. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En la petición de entrada, emita el comando **show version**.



- e. Salga de la sesión de SSH y de Tera Term emitiendo el comando **exit**.

R1# **exit**

Paso 3: Detener la captura de Wireshark

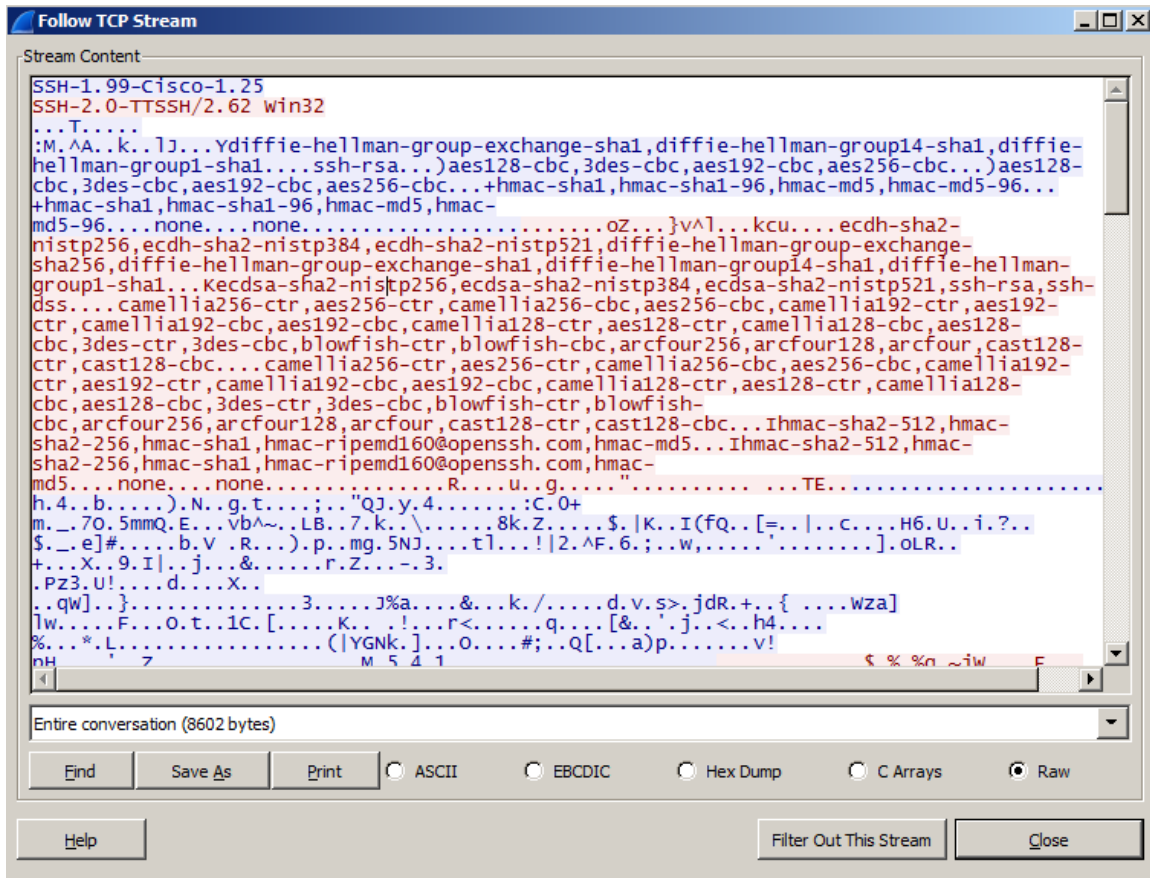


Paso 4: Aplicar un filtro de SSH a los datos de captura de Wireshark



Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

- Haga clic con el botón secundario en una de las líneas **SSHv2** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).
- Examine la ventana **Follow TCP Stream** de la sesión de SSH. Los datos se encriptaron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.



¿Por qué se prefiere SSH a Telnet para las conexiones remotas?

Las respuestas pueden variar. SSH lleva a cabo una autenticación con un dispositivo y le hace saber si es la primera vez que se conecta al dispositivo. También protege la sesión al encriptar todos los datos.

- Después de analizar la sesión de SSH, haga clic en **Close** (Cerrar).
- Cierre Wireshark.

Parte 5: Configurar el switch para el acceso por SSH

En la parte 5, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH en él utilizando Tera Term.

Paso 1: Configurar los parámetros básicos en el switch

Paso 2: Configurar el switch para que tenga conectividad de SSH

A fin de configurar SSH para el switch, utilice los mismos comandos que usó para configurar SSH en el router en la parte 2.

Paso 3: Establecer una conexión SSH al switch

Inicie Tera Term desde la PC-A y, luego, acceda a la interfaz SVI en el S1 mediante SSH.

Paso 4: Resuelva cualquier problema que se presente.

¿Puede establecer una sesión de SSH con el switch?

Sí. SSH se puede configurar en un switch mediante los mismos comandos que se usaron en el router.

Parte 6: Ejecutar SSH desde la CLI del switch

El cliente de SSH está incorporado en Cisco IOS y puede ejecutarse desde la CLI. En la parte 6, ejecutará una conexión SSH al router desde la CLI del switch.

Paso 1: Ver los parámetros disponibles para el cliente de SSH de Cisco IOS

Utilice el signo de interrogación (?) para mostrar las opciones de parámetros disponibles con el comando **ssh**.

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
  -p      Connect to this port
  -v      Specify SSH Protocol Version
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

Paso 2: Acceder al router R1 mediante SSH desde el S1

- a. Cuando accede al R1 mediante SSH, debe utilizar la opción **-l admin**. De esta manera, podrá iniciar sesión como usuario **admin**. Cuando se le solicite, introduzca **adminpass** en el campo Password (contraseña).

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****
```

```
R1#
```

- b. Para volver al S1 sin cerrar la sesión de SSH para el R1, presione las teclas **Ctrl+Mayús+6**. Suelte las teclas **Ctrl+Mayús+6** y presione **x**. Debería ver la ventana de petición de entrada del modo EXEC privilegiado del switch.

```
R1#
S1#
```

- c. Para volver a la sesión de SSH en el R1, presione Entrar en una línea en blanco de la CLI. Es posible que deba presionar Entrar por segunda vez para ver la petición de entrada de la CLI del router.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

- d. Para finalizar la sesión de SSH en el R1, escriba **exit** en la petición de entrada del router.

```
R1# exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
S1#
```

¿Qué versiones de SSH se admiten en la CLI?

Las respuestas pueden variar, pero se puede determinar al introducir **ssh -v ?** en la línea de comandos. La versión 15.0(2) del IOS que se ejecuta en el switch 2960 admite SSH v1 y V2.

```
S1# ssh -v ?
```

```
1 Protocol Version 1
```

```
2 Protocol Version 2
```

Reflexión

¿Cómo proporcionaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?

Las respuestas pueden variar. Se agregaría el nombre de usuario y la contraseña de cada usuario a la base de datos local mediante el comando **username**. También es posible utilizar un servidor RADIUS o TACACS, pero este tema aún no se analizó.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos, final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Connection to S1-F0/5.
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
```

```
no ip http secure-server
!
control-plane
!
!
banner motd ^C
*****
  Unauthorized Access is Prohibited!
*****
^C
!
line con 0
  password 7 00071A150754
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0
  password 7 110A1016141D
  login local
  transport input telnet ssh
line vty 1 4
  login local
  transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMivyLkyjTlHbmYxZigc
no aaa new-model
system mtu routing 1500
```

```
!  
!  
no ip domain-lookup  
ip domain-name ccna-lab.com  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20
```

```
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
 ip address 192.168.1.11 255.255.255.0  
!  
ip http server  
ip http secure-server  
!  
!  
banner motd ^C  
*****  
  Unauthorized Access is Prohibited!  
*****  
^C  
!  
line con 0  
 password 7 060506324F41  
 login  
line vty 0 4  
 password 7 060506324F41  
 login local  
 transport input telnet ssh  
line vty 5 15  
 password 7 00071A150754  
 login local  
 transport input telnet ssh  
!  
end
```


Práctica de laboratorio: Protección de dispositivos de red

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Configurar medidas básicas de seguridad en el router

Parte 3: Configurar medidas básicas de seguridad en el switch

Información básica/Situación

Se recomienda que todos los dispositivos de red se configuren, al menos, con un conjunto mínimo de comandos de seguridad conforme a las prácticas recomendadas. Esto incluye dispositivos para usuarios finales, servidores y dispositivos de red, como routers y switches.

En esta práctica de laboratorio, configurará los dispositivos de red en la topología a fin de que acepten sesiones de SSH para la administración remota. También utilizará la CLI del IOS para configurar medidas de seguridad básicas conforme a las prácticas recomendadas. Luego, probará las medidas de seguridad para verificar que estén implementadas de manera apropiada y que funcionen correctamente.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son ISR Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con software Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos que se muestran en la topología y realice el cableado según sea necesario.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar el router.

Consulte la práctica de laboratorio anterior para obtener ayuda con los comandos necesarios para SSH.

- Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- Entre al modo de configuración.
- Asigne el nombre R1 al router.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configure el switch.

- Acceda al switch mediante el puerto de consola y habilite al modo EXEC privilegiado.
- Entre al modo de configuración.
- Asigne el nombre S1 al switch.
- Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

- g. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- h. Encripte las contraseñas de texto no cifrado.
- i. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- j. Configure la SVI predeterminada con la información de dirección IP incluida en la tabla de direccionamiento.
- k. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Configurar medidas básicas de seguridad en el router

Paso 1: Aportar seguridad a las contraseñas

Un administrador debe asegurar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Entre estas pautas, se podría incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

Nota: las pautas de prácticas recomendadas requieren el uso de contraseñas seguras, como las que se muestran aquí, en ambientes de producción. Sin embargo, las otras prácticas de laboratorio en este curso utilizan las contraseñas cisco y class para facilitar la realización de las prácticas.

- a. Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas.

```
R1(config)# enable secret Enablep@55
```

- b. Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas.

```
R1(config)# security passwords min-length 10
```

Paso 2: Habilitar conexiones SSH

- a. Asigne el nombre **CCNA-lab.com** al dominio.

```
R1(config)# ip domain-name CCNA-lab.com
```

- b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

- c. Configure la entrada de transporte para las líneas vty de modo que acepten conexiones SSH, pero no permitan conexiones Telnet.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input ssh
```

- d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
R1(config-line)# login local
```

```
R1(config-line)# exit
```

- e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
```

```
The name for the keys will be: R1.CCNA-lab.com
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 2 seconds)
```

```
R1(config)#  
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

- a. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante el lapso especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra la sesión del usuario en forma automática después de un tiempo especificado. Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad.

```
R1(config)# line console 0  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# line vty 0 4  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# exit  
R1(config)#
```

- b. El comando siguiente impide los intentos de inicio de sesión por fuerza bruta. Si alguien falla en dos intentos en un período de 120 segundos, el router bloquea los intentos de inicio de sesión por 30 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
R1(config)# login block-for 30 attempts 2 within 120
```

¿Qué significa **2 within 120** en el comando anterior?

Si se realizan dos intentos fallidos en un período de dos minutos (120 segundos), el acceso de inicio de sesión se bloquea.

¿Qué significa **block-for 30** en el comando anterior?

Si el acceso de inicio de sesión se bloquea, el dispositivo esperará 30 segundos antes de volver a permitir el acceso.

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

Los puertos del router están deshabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado administrativamente inactivo. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en el estado administratively down (administrativamente inactivo) se deben deshabilitar por medio del comando **shutdown** en el modo de configuración de interfaz.

```
R1# show ip interface brief  


| Interface                  | IP-Address  | OK? | Method | Status                | Protocol |
|----------------------------|-------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned  | YES | NVRAM  | administratively down | down     |
| GigabitEthernet0/0         | unassigned  | YES | NVRAM  | administratively down | down     |
| GigabitEthernet0/1         | 192.168.1.1 | YES | manual | up                    | up       |
| Serial0/0/0                | unassigned  | YES | NVRAM  | administratively down | down     |
| Serial0/0/1                | unassigned  | YES | NVRAM  | administratively down | down     |

  
R1#
```

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

- a. Utilice Tera Term para acceder al R1 mediante Telnet.

¿R1 acepta la conexión Telnet? _____ No, la conexión se rechaza.

¿Por qué o por qué no?

Telnet se deshabilitó con el comando **transport input ssh**.

- b. Utilice Tera Term para acceder al R1 mediante SSH.

¿R1 acepta la conexión SSH? _____ Si

- c. Escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea después de dos intentos.

¿Qué ocurrió después del segundo inicio de sesión fallido?

La conexión al R1 se desconectó. Si intenta volver a conectarse dentro de los siguientes 30 segundos, la conexión será rechazada.

- d. Desde su sesión de consola en el router, emita el comando **show login** para ver el estado de inicio de sesión. En el siguiente ejemplo, el comando **show login** se emitió dentro del período de bloqueo de inicio de sesión de 30 segundos y muestra que el router está en modo silencioso. El router no aceptará ningún intento de inicio de sesión por 14 segundos más.

R1# **show login**

```
A default login delay of 1 second is applied.  
No Quiet-Mode access list has been configured.
```

```
Router enabled to watch for login Attacks.  
If more than 2 login failures occur in 120 seconds or less,  
logins will be disabled for 30 seconds.
```

```
Router presently in Quiet-Mode.  
Will remain in Quiet-Mode for 14 seconds.  
Denying logins from all sources.
```

R1#

- e. Cuando hayan pasado los 30 segundos, vuelva a acceder al R1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.

Una vez que inició sesión correctamente, ¿qué se mostró? _____

El aviso de inicio de sesión del R1.

- f. Ingrese al modo EXEC privilegiado y utilice la contraseña **Enablep@55**.

Si escribe esta contraseña incorrectamente, ¿se desconectará la sesión de SSH después de dos intentos fallidos en el lapso de 120 segundos? _____ No.

¿Por qué o por qué no?

El comando **login block-for 30 attempts 2 within 120** solo controla los intentos de inicio de sesión de las sesiones.

- g. Emita el comando **show running-config** en la petición de entrada del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Parte 3: Configurar medidas básicas de seguridad en el switch

Paso 1: Aportar seguridad a las contraseñas en el switch

Cambie la contraseña encriptada del modo EXEC privilegiado conforme a las pautas de contraseña segura.

```
S1(config)# enable secret Enablep@55
```

Nota: el comando de seguridad **password min-length** no está disponible en el switch 2960.

Paso 2: Habilitar conexiones SSH

- a. Asigne el nombre **CCNA-lab.com** al dominio.

```
S1(config)# ip domain-name CCNA-lab.com
```

- b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

- c. Configure la entrada de transporte para las líneas vty para permitir las conexiones SSH, pero no las conexiones Telnet.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh
```

- d. Las líneas vty deben utilizar la base de datos de usuarios local para realizar la autenticación.

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

- e. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Paso 3: Implementar medidas de seguridad en las líneas de consola y vty

- a. Haga que el switch cierre sesión en una línea que haya estado inactiva durante 10 minutos.

```
S1(config)# line console 0
```

```
S1(config-line)# exec-timeout 10 0
```

```
S1(config-line)# line vty 0 15
```

```
S1(config-line)# exec-timeout 10 0
```

```
S1(config-line)# exit
```

```
S1(config)#
```

- b. Para impedir intentos de inicio de sesión por fuerza bruta, configure el switch para que bloquee el acceso de inicio de sesión por 30 segundos en caso de que haya dos intentos fallidos en un período de 120 segundos. Este temporizador se establece en un valor especialmente bajo para esta práctica de laboratorio.

```
S1(config)# login block-for 30 attempts 2 within 120
```

```
S1(config)# end
```

Paso 4: Verifique que todos los puertos sin utilizar estén deshabilitados.

Los puertos del switch están habilitados de manera predeterminada. Desactive todos los puertos que no estén en uso en el switch.

- a. Para verificar el estado de los puertos del switch, utilice el comando **show ip interface brief**.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

S1#

- b. Utilice el comando **interface range** para desactivar varias interfaces a la vez.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- c. Verifique que todas las interfaces inactivas tengan un estado administrativamente inactivo.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
FastEthernet0/8	unassigned	YES	unset	administratively down	down

FastEthernet0/9	unassigned	YES	unset	administratively	down	down
FastEthernet0/10	unassigned	YES	unset	administratively	down	down
FastEthernet0/11	unassigned	YES	unset	administratively	down	down
FastEthernet0/12	unassigned	YES	unset	administratively	down	down
FastEthernet0/13	unassigned	YES	unset	administratively	down	down
FastEthernet0/14	unassigned	YES	unset	administratively	down	down
FastEthernet0/15	unassigned	YES	unset	administratively	down	down
FastEthernet0/16	unassigned	YES	unset	administratively	down	down
FastEthernet0/17	unassigned	YES	unset	administratively	down	down
FastEthernet0/18	unassigned	YES	unset	administratively	down	down
FastEthernet0/19	unassigned	YES	unset	administratively	down	down
FastEthernet0/20	unassigned	YES	unset	administratively	down	down
FastEthernet0/21	unassigned	YES	unset	administratively	down	down
FastEthernet0/22	unassigned	YES	unset	administratively	down	down
FastEthernet0/23	unassigned	YES	unset	administratively	down	down
FastEthernet0/24	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively	down	down

S1#

Paso 5: Verificar que las medidas de seguridad se hayan implementado correctamente

- Verifique que Telnet esté deshabilitado en el switch.
- Acceda al switch mediante SSH y escriba incorrectamente a propósito la información de usuario y contraseña para ver si el acceso de inicio de sesión se bloquea.
- Cuando hayan pasado los 30 segundos, vuelva a acceder al S1 mediante SSH e inicie sesión utilizando el nombre de usuario **admin** y la contraseña **Admin15p@55**.
¿Apareció el anuncio después de iniciar sesión correctamente? _____ **Sí**
- Ingresa al modo EXEC privilegiado utilizando la contraseña **Enablep@55**.
- Emita el comando **show running-config** en la petición de entrada del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Reflexión

- En la configuración básica de la parte 1, se introdujo el comando **password cisco** para las líneas de consola y vty. ¿Cuándo se utiliza esta contraseña después de haberse aplicado las medidas de seguridad conforme a las prácticas recomendadas?

Esta contraseña no se vuelve a utilizar. Aunque el comando **password** todavía aparece en las secciones de línea de la configuración en ejecución, el comando se deshabilitó no bien se introdujo el comando **login local** para esas líneas.

- ¿Se vieron afectadas por el comando **security passwords min-length 10** las contraseñas configuradas previamente con menos de 10 caracteres?

No. El comando `security passwords min-length` solo afecta las contraseñas que se introducen después de emitir el comando. Todas las contraseñas preexistentes permanecen vigentes. Si se cambian, deberán tener una longitud mínima de 10 caracteres.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

Configuraciones de dispositivos, final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 4 jowh6xYPeJucL2dB/ulkSjK2YGee/Usr./fiqFhbxTQ
no aaa new-model
!
no ip domain lookup
ip domain name CCNA-lab.com
ip cef
```

```
login block-for 30 attempts 2 within 120
no ipv6 cef
!
username admin privilege 15 secret 4 iAAXTYNDMJ03iHURmpY85S.NR4m72e1HMyRxq9kPN0g
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
banner motd ^C

  Unauthorized Access is Prohibited!

^C
!
line con 0
exec-timeout 5 0
password 7 094F471A1A0A57
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
```

```
exec-timeout 5 0
password 7 104D000A0618
login local
transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 jowh6xYPeJucL2dB/ulkSjK2YGee/Usr./fiqFhbxTQ
!
username admin privilege 15 secret 4 iAAxTYNDMJ03iHURmpY85S.NR4m72e1HMyRxq9kPN0g
!
system mtu routing 1500
!
no ip domain-lookup
ip domain-name CCNA-lab.com
login block-for 30 attempts 2 within 120
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
```

```
!  
interface FastEthernet0/7  
shutdown  
!  
interface FastEthernet0/8  
shutdown  
!  
interface FastEthernet0/9  
shutdown  
!  
interface FastEthernet0/10  
shutdown  
!  
interface FastEthernet0/11  
shutdown  
!  
interface FastEthernet0/12  
shutdown  
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown  
!  
interface FastEthernet0/16  
shutdown  
!  
interface FastEthernet0/17  
shutdown  
!  
interface FastEthernet0/18  
shutdown  
!  
interface FastEthernet0/19  
shutdown  
!  
interface FastEthernet0/20  
shutdown  
!  
interface FastEthernet0/21  
shutdown  
!  
interface FastEthernet0/22  
shutdown  
!
```

```
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C

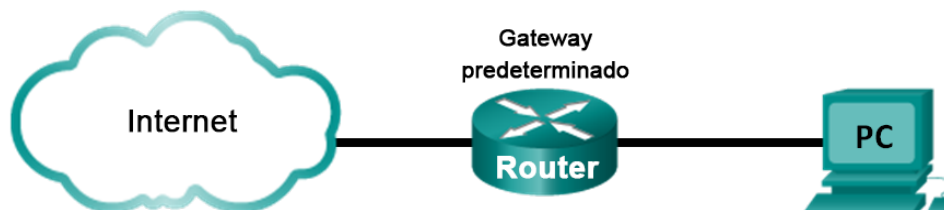
  Unauthorized Access is Prohibited!

^C
!
line con 0
 password 7 110A1016141D
 login
line vty 0 4
 password 7 110A1016141D
 login local
 transport input ssh
line vty 5 15
 login local
!
end
```

Práctica de laboratorio: Prueba de la latencia de red con los comandos ping y traceroute (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

Parte 1: Utilizar el comando ping para registrar la latencia de red

Parte 2: Utilizar el comando traceroute para registrar la latencia de red

Información básica/Situación

Para obtener estadísticas reales sobre latencia, se debe realizar esta actividad en una red activa. Consulte con su instructor si existen restricciones locales de seguridad para el uso del comando **ping** en la red.

Nota para el instructor: algunas instituciones deshabilitan las respuestas de eco ICMP a través de la red. Antes de que los estudiantes comiencen esta actividad, asegúrese de que no haya restricciones locales sobre datagramas ICMP. En esta actividad se da por sentado que los datagramas ICMP no están restringidos por ninguna política de seguridad local.

El objetivo de esta actividad de laboratorio es medir y evaluar la latencia de red en el tiempo y durante diferentes momentos del día para capturar una muestra representativa de la actividad típica de la red. Esto se logrará mediante el análisis del retardo del retorno desde una computadora remota con el comando **ping**. El tiempo de retraso del retorno, medido en milisegundos, se resume calculando la latencia promedio (media) y el intervalo (máximo y mínimo) del tiempo de retraso.

Recursos necesarios

- 1 PC (Windows 7, Vista o XP, con acceso a Internet)

Parte 1: Utilizar el comando ping para registrar la latencia de red

En la parte 1, examinará la latencia de red a varios sitios Web en distintas partes del mundo. Este proceso se puede utilizar en una red de producción empresarial para crear una línea de base de rendimiento.

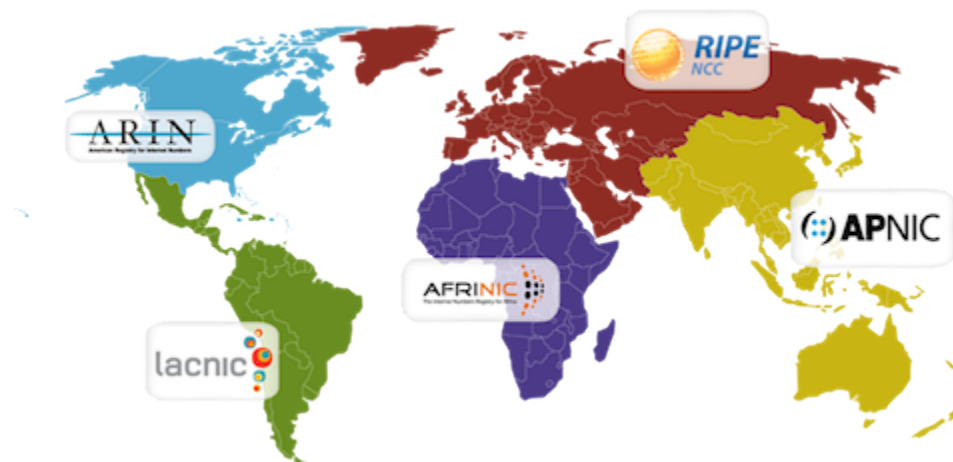
Paso 1: Verificar la conectividad

Haga ping a los siguientes sitios Web de registros regionales de Internet (RIR) para verificar la conectividad:

```

C:\Users\User1> ping www.arin.net
C:\Users\User1> ping www.lacnic.net
C:\Users\User1> ping www.afrinic.net
C:\Users\User1> ping www.apnic.net
  
```

Nota: www.ripe.net no responde a solicitudes de ICMP, por lo que no puede utilizarse para esta práctica de laboratorio.



Paso 2: Recopilar los datos de red

Recopilará una cantidad de datos suficiente para calcular estadísticas sobre el resultado del comando **ping** mediante el envío de 25 solicitudes de eco a cada dirección del paso 1. Registre los resultados para cada sitio Web en archivos de texto.

- a. En el símbolo del sistema, escriba **ping** para enumerar las opciones disponibles.

```
C:\Users\User1> ping
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated

<resultado omitido>

- b. Si utiliza el comando **ping** con la opción de cuenta, podrá enviar 25 solicitudes de eco al destino, como se muestra a continuación. Además, creará un archivo de texto con el nombre **arin.txt** en el directorio actual. Este archivo de texto contendrá los resultados de las solicitudes de eco.

```
C:\Users\User1> ping -n 25 www.arin.net > arin.txt
```

Nota: la terminal permanecerá en blanco hasta que el comando haya finalizado, porque en este ejemplo el resultado se redirigió a un archivo de texto: **arin.txt**. El símbolo > se utiliza para redirigir el resultado de pantalla al archivo y para sobrescribir el archivo, si ya existe. Si se desean añadir más resultados al archivo, reemplace > por >> en el comando.

- c. Repita el comando **ping** para los otros sitios Web.

```
C:\Users\User1> ping -n 25 www.afrinic.net > afrinic.txt
```

```
C:\Users\User1> ping -n 25 www.apnic.net > apnic.txt
```

```
C:\Users\User1> ping -n 25 www.lacnic.net > lacnic.txt
```

Paso 3: Verificar la recopilación de datos

Para ver los resultados en el archivo creado, introduzca el comando **more** en el símbolo del sistema.

```
C:\Users\User1> more arin.txt
```

```
Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
```

```
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
```

```
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
```

```
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
```

```
<resultado omitido>
```

```
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
```

```
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
```

```
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
```

```
Ping statistics for 192.149.252.75:
```

```
Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Nota: presione la barra espaciadora para mostrar el resto del archivo o presione **q** para salir.

Para verificar que los archivos se crearon, utilice el comando **dir** para enumerar los archivos en el directorio. También se puede utilizar el carácter comodín ***** para filtrar solo los archivos de texto.

```
C:\Users\User1> dir *.txt
```

```
Volume in drive C is OS
```

```
Volume Serial Number is 0A97-D265
```

```
Directory of C:\Users\User1
```

```
02/07/2013  12:59 PM                1,642 afrinic.txt
```

```
02/07/2013  01:00 PM                1,615 apnic.txt
```

```
02/07/2013  12:40 PM                1,641 arin.txt
```

```
02/07/2013  12:58 PM                1,589 lacnic.txt
```

```
         4 File(s)                6,487 bytes
```

```
         0 Dir(s)  34,391,453,696 bytes free
```


Registre sus resultados en la siguiente tabla:

	Mínimo	Máximo	Promedio
www.afrinic.net	359 ms	389 ms	369 ms
www.apnic.net	201	210	204
www.arin.net	107	121	112
www.lacnic.net	216	226	218

Compare los resultados de retardo. ¿De qué manera afecta el retardo la ubicación geográfica?

En la mayoría de los casos, el tiempo de respuesta es más extenso cuando se compara con la distancia física al destino.

Parte 2: Utilizar el comando traceroute para registrar la latencia de red

Según cuál sea el tamaño del ISP y la ubicación de los hosts de origen y destino, las rutas rastreadas pueden atravesar muchos saltos y una cantidad de ISP diferentes. Los comandos **traceroute** también pueden utilizarse para observar la latencia de red. En la parte 2, se utiliza el comando **tracert** para rastrear la ruta a los destinos utilizados en la parte 1.

El comando **tracert** utiliza paquetes ICMP de TTL superado y respuestas de eco ICMP para rastrear la ruta.

Paso 1: Utilizar el comando tracert y registrar el resultado en archivos de texto

Copie los siguientes comandos para crear los archivos de traceroute:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Paso 2: Utilizar el comando more para examinar la ruta rastreada

a. Utilice el comando **more** para acceder al contenido de estos archivos:

```
C:\Users\User1> more traceroute_arin.txt
```

```
Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:
```

```
  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    11 ms    12 ms    11 ms    10.39.0.1
  3    10 ms    15 ms    11 ms    172.21.0.116
  4    19 ms    10 ms    11 ms    70.169.73.90
  5    13 ms    10 ms    11 ms    chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]
  6    72 ms    71 ms    70 ms    mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
  7    72 ms    71 ms    72 ms    68.100.0.146
  8    74 ms    83 ms    73 ms    172.22.66.29
  9    75 ms    71 ms    73 ms    172.22.66.29
```

```
10    74 ms    75 ms    73 ms    wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]
11    71 ms    71 ms    71 ms    host-252-131.arin.net [192.149.252.131]
12    73 ms    71 ms    71 ms    www.arin.net [192.149.252.75]
```

Trace complete.

En este ejemplo, demoró menos de 1 ms recibir una respuesta del gateway predeterminado (192.168.1.1). En el conteo de saltos 6, la ida y vuelta a 68.1.1.7 requirió un promedio de 71 ms. Para la ida y vuelta al destino final en www.arin.net, se requirió un promedio de 72 ms.

Entre las líneas 5 y 6, el retardo de red es mayor, según lo indica el aumento del tiempo de ida y vuelta de un promedio de 11 a 71 ms

- b. Realice el mismo análisis con el resto de los resultados del comando tracert.

¿A qué conclusión puede llegar con respecto a la relación entre el tiempo de ida y vuelta y la ubicación geográfica?

En la mayoría de los casos, el tiempo de respuesta es más extenso cuando se compara con la distancia física al destino.

Reflexión

1. Los resultados de **tracert** y **ping** pueden proporcionar información importante sobre la latencia de red. ¿Qué debe hacer si desea una representación precisa de la línea de base de la latencia de su red?

Las respuestas varían. Debe realizar un análisis cuidadoso del retraso en varios días consecutivos y en momentos diferentes del día.

2. ¿Cómo puede utilizar la información de línea de base?

Puede comparar los datos de línea de base con los datos actuales para determinar si hubo un cambio en los tiempos de respuesta de la red. Este análisis puede ayudarlo a resolver problemas de red y a programar la transferencia de datos de rutina durante las horas no pico.

Práctica de laboratorio: Uso de la CLI para recopilar información sobre dispositivos de red (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

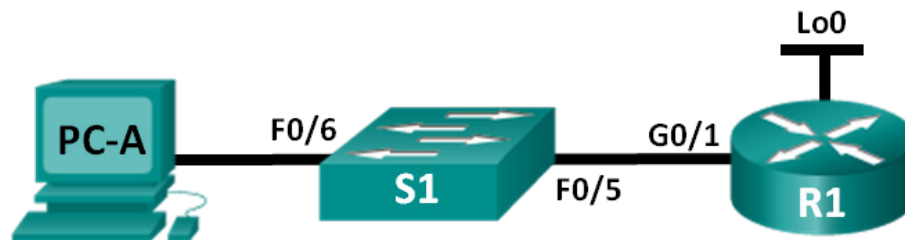


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Establecer la topología e inicializar los dispositivos

- Configurar los equipos para que coincidan con la topología de la red.
- inicializar y volver a cargar el router y el switch.

Parte 2: Configurar dispositivos y verificar la conectividad

- Asignar una dirección IP estática a la NIC de la PC-A.
- configurar los parámetros básicos en el R1.
- configurar los parámetros básicos en el S1.
- Verificar la conectividad de la red.

Parte 3: Recopilar información sobre los dispositivos de red

- Recopilar información sobre el R1 mediante los comandos de CLI del IOS.
- Recopilar información sobre el S1 mediante los comandos de CLI del IOS.
- Recopilar información sobre la PC-A mediante la CLI del símbolo del sistema.

Información básica/situación

La documentación de una red en funcionamiento es una de las tareas más importantes que puede realizar un profesional de red. Tener la documentación correspondiente de las direcciones IP, los números de modelo, las versiones del IOS y los puertos utilizados, así como probar la seguridad, puede resultar muy útil para resolver los problemas de una red.

En esta práctica de laboratorio, armará una red pequeña, configurará los dispositivos, implementará seguridad básica y documentará las configuraciones mediante la emisión de diversos comandos en el router, el switch y la PC para recopilar la información.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red, borrará cualquier configuración, de ser necesario, y configurará los parámetros básicos del router y el switch.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

- a. Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.
- b. Encienda todos los dispositivos de la topología.

Paso 2: inicializar y volver a cargar el router y el switch.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, establecerá la topología de la red y configurará los parámetros básicos del router y el switch. Consulte la topología y la tabla de direccionamiento que se encuentran al principio de esta práctica de laboratorio para obtener información sobre nombres de dispositivos y direcciones.

Nota: en el apéndice A, se proporcionan detalles de configuración para los pasos de la parte 2. Antes de consultar el apéndice, intente completar la parte 2.

Paso 1: Configurar la dirección IPv4 para la PC

Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A según la tabla de direccionamiento.

Paso 2: Configurar el router.

Si necesita ayuda para realizar el paso 2, consulte el apéndice A.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- b. Configure la hora correcta en el router.
- c. Ingrese al modo de configuración global.
 - 1) Asigne un nombre de dispositivo al router según la topología y la tabla de direccionamiento.
 - 2) Desactive la búsqueda del DNS.
 - 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
 - 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.
 - 5) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.
 - 6) Encripte las contraseñas de texto no cifrado.
 - 7) Cree un nombre de dominio **cisco.com** para el acceso por SSH.
 - 8) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.
 - 9) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.
- d. Configure el acceso a las líneas VTY.
 - 1) Use la base de datos local para la autenticación de SSH.
 - 2) Habilite SSH solo para el acceso de inicio de sesión.
- e. Vuelva al modo de configuración global.
 - 1) Cree la interfaz Loopback 0 y asigne la dirección IP según la tabla de direccionamiento.
 - 2) Configure y habilite la interfaz G0/1 en el router.
 - 3) Configure las descripciones de interfaz para G0/1 y L0.
 - 4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

Paso 3: Configurar el switch.

Si necesita ayuda para realizar el paso 3, consulte el apéndice A.

- a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- b. Configure la hora correcta en el switch.
- c. Ingrese al modo de configuración global.
 - 1) Asigne un nombre de dispositivo al switch según la topología y la tabla de direccionamiento.
 - 2) Desactive la búsqueda del DNS.
 - 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
 - 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.
 - 5) Cifre las contraseñas de texto no cifrado.

- 6) Cree un nombre de dominio **cisco.com** para el acceso por SSH.
 - 7) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.
 - 8) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.
 - 9) Cree y active una dirección IP en el switch según la topología y la tabla de direccionamiento.
 - 10) Configure el gateway predeterminado en el switch.
 - 11) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.
- d. Configure el acceso a las líneas VTY.
- 1) Use la base de datos local para la autenticación de SSH.
 - 2) Habilite SSH solo para el acceso de inicio de sesión.
 - 3) Ingrese al modo correspondiente para configurar las descripciones de interfaz de F0/5 y F0/6.
 - 4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Verificar la conectividad de la red.

- a. Desde el símbolo del sistema en la PC-A, haga ping a la dirección IP de la VLAN 1 del S1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
- b. En el símbolo del sistema de la PC-A, haga ping a la dirección IP del gateway predeterminado en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
- c. En el símbolo del sistema de la PC-A, haga ping a la interfaz loopback en R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
- d. Vuelva a acceder al switch mediante la consola y haga ping a la dirección IP de G0/1 en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.

Parte 3: Recopilar información sobre los dispositivos de red

En la parte 3, utilizará una variedad de comandos para recopilar información sobre los dispositivos en la red, así como algunas características de rendimiento. La documentación de la red es un componente muy importante de la administración de una red. La documentación de la topología física y lógica es importante, al igual que la verificación de los modelos de plataforma y las versiones del IOS de los dispositivos de red. Tener conocimientos de los comandos adecuados para recopilar esta información es fundamental para los profesionales de red.

Paso 1: Recopilar información sobre el R1 mediante los comandos del IOS.

Uno de los pasos más básicos consiste en recopilar información sobre el dispositivo físico, así como la información del sistema operativo.

- a. Emita el comando adecuado para obtener la siguiente información:

Nota para el instructor: las respuestas para todo el paso 1 varían según el modelo de router y el IOS. Tenga en cuenta que la respuesta para el paquete de tecnología se aplica solo a los routers que ejecutan el IOS 15.0 y posterior.

Modelo de router: _____
router Cisco 1941

Versión del IOS: _____
15.2(4)M3

RAM total: _____

512 MB

NVRAM total: _____

255 KB

Memoria flash total: _____

250880 KB

Archivo de imagen de IOS: _____

c1900-universalk9-mz.SPA.152-4.M3.bin

Registro de configuración: _____

0x2102

Paquete de tecnología: _____

ipbasek9

¿Qué comando emitió para recopilar la información?

Se puede usar el comando **show version** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

- b. Emita el comando adecuado para mostrar un resumen de la información importante sobre las interfaces del router. Escriba el comando y registre sus resultados a continuación.

Nota: registre solo las interfaces que tengan direcciones IP.

Se puede usar el comando **show ip interface brief** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/1	192.168.1.1	YES	NVRAM	up	up
Loopback0	209.165.200.225	YES	NVRAM	up	up

<some output omitted>

- c. Emita el comando adecuado para mostrar la tabla de enrutamiento. Escriba el comando y registre sus resultados a continuación.

Se puede usar el comando **show ip route** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/27 is directly connected, Loopback0
L    209.165.200.225/32 is directly connected, Loopback0

```

- d. ¿Qué comando usaría para mostrar la asignación de direcciones de capa 2 y capa 3 en el router? Escriba el comando y registre sus resultados a continuación.

Se puede usar el comando **show arp** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	30f7.0da3.1821	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	0	c80a.a9fa.de0d	ARPA	GigabitEthernet0/1
Internet	192.168.1.11	2	0cd9.96d2.34c0	ARPA	GigabitEthernet0/1

- e. ¿Qué comando usaría para ver información detallada sobre todas las interfaces en el router o sobre una interfaz específica? Escriba el comando a continuación.

Se puede usar el comando **show interfaces** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

- f. Cisco tiene un protocolo muy eficaz que funciona en la capa 2 del modelo OSI. Este protocolo puede ayudarlo a delinear la forma en que se conectan físicamente los dispositivos Cisco, así como a determinar los números de modelo e incluso el direccionamiento IP y las versiones del IOS. ¿Qué comandos usaría en el router R1 para obtener información sobre el switch S1 que le ayude a completar la siguiente tabla?

Identificador del dispositivo	Interfaz local	Capacidad	N.º de modelo	ID del puerto remoto	Dirección IP	Versión del IOS
S1.cisco.com	G 0/1	Switch	WS-2960-24TT-L	F 0/5	192.168.1.11	15.0(2)SE1

Se puede usar el comando **show cdp neighbors detail** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

- g. Una prueba muy simple de los dispositivos de red consiste en ver si se puede acceder a estos mediante Telnet. No obstante, tenga en cuenta que Telnet no es un protocolo seguro. No se debe habilitar en la mayoría de los casos. Con un cliente Telnet, como Tera Term o PuTTY, intente acceder al R1 mediante Telnet con la dirección IP del gateway predeterminado. Registre sus resultados a continuación.

Tera Term Output: Connection refused. (Resultado de Tera Term: conexión denegada).

- h. En la PC-A, realice pruebas para asegurar que SSH funcione correctamente. Con un cliente SSH, como Tera Term o PuTTY, acceda al R1 mediante SSH desde la PC-A. Si recibe un mensaje de advertencia con respecto a otra clave, haga clic en **Continue** (Continuar). Inicie sesión con el nombre de usuario y la contraseña correspondientes que creó en la parte 2. ¿Tuvo éxito?

Sí.

Las distintas contraseñas configuradas en el router deben ser tan seguras y protegidas como sea posible.

Nota: las contraseñas utilizadas para la práctica de laboratorio (**cisco** y **class**) no cumplen con las prácticas recomendadas para las contraseñas seguras. Estas contraseñas se usan simplemente por cuestiones de practicidad para realizar las prácticas de laboratorio. De manera predeterminada, la contraseña de consola y todas las contraseñas de vty configuradas se muestran como texto no cifrado en el archivo de configuración.

- i. Verifique que todas las contraseñas en el archivo de configuración estén encriptadas. Escriba el comando y registre sus resultados a continuación.

Comando: _____

Se puede usar el comando **show running-config** o **show run** en la petición de entrada de EXEC privilegiado.

¿Está encriptada la contraseña de consola? _____ Sí

¿Está encriptada la contraseña de SSH? _____ Sí

Paso 2: Recopilar información sobre el S1 mediante los comandos del IOS.

Muchos de los comandos que usó en R1 se pueden utilizar con el switch. Sin embargo, existen algunas diferencias con algunos de los comandos.

Nota para el instructor: las respuestas para todo el paso 2 varían según el modelo de switch, los puertos utilizados y las direcciones MAC.

- a. Emita el comando adecuado para obtener la siguiente información:

Modelo de switch: _____ WS-C2960-24TT-L

Versión del IOS: _____ 15.0(2)SE1

NVRAM total: _____ 64 K

Archivo de imagen de IOS: _____ c2960-lanbasek9-mz.150-2.SE1.bin

¿Qué comando emitió para recopilar la información?

Se puede usar el comando **show version** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

- b. Emita el comando adecuado para mostrar un resumen de la información clave sobre las interfaces del switch. Escriba el comando y registre sus resultados a continuación.

Nota: registre solo las interfaces activas.

Se puede usar el comando **show ip interface brief** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

```
Interface          IP-Address      OK? Method Status        Protocol
Vlan1              192.168.1.11   YES NVRAM    up            up
FastEthernet0/5    unassigned      YES unset    up            up
FastEthernet0/6    unassigned      YES unset    up            up
<some output omitted>
```

- c. Emita el comando adecuado para mostrar la tabla de direcciones MAC del switch. Registre solo las direcciones MAC dinámicas en el siguiente espacio.

Se puede usar el comando **show mac address-table** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

```
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       30f7.0da3.1821   DYNAMIC   Fa0/5
1       c80a.a9fa.de0d   DYNAMIC   Fa0/6
```

- d. Verifique que el acceso a VTY por Telnet esté deshabilitado en el S1. Con un cliente Telnet, como Tera Term o PuTTY, intente acceder al S1 mediante Telnet con la dirección 192.168.1.11. Registre sus resultados a continuación.

Tera Term Output: Connection refused. (Resultado de Tera Term: conexión denegada).

- e. En la PC-A, realice pruebas para asegurar que SSH funcione correctamente. Con un cliente SSH, como Tera Term o PuTTY, acceda al S1 mediante SSH desde la PC-A. Si recibe un mensaje de advertencia con respecto a otra clave, haga clic en **Continue**. Inicie sesión con un nombre de usuario y una contraseña adecuados. ¿Tuvo éxito?

Sí.

- f. Complete la siguiente tabla con información sobre el router R1 utilizando los comandos adecuados en el S1.

Id. del dispositivo	Interfaz local	Capacidad	N.º de modelo	ID del puerto remoto	Dirección IP	Versión del IOS
R1.cisco.com	F 0/5	Router	CISCO1941/K9	G 0/1	192.168.1.1	15.2(4)M3

Se puede usar el comando **show cdp neighbors detail** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

- g. Verifique que todas las contraseñas en el archivo de configuración estén encriptadas. Escriba el comando y registre sus resultados a continuación.

Comando: _____

Se puede usar el comando **show running-config** o **show run** en la petición de entrada de EXEC privilegiado.

¿Está encriptada la contraseña de consola? _____ Sí

Paso 3: Recopilar información sobre la PC-A.

Mediante diversos comandos de utilidades de Windows, recopilará información sobre la PC-A.

- a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** y registre sus respuestas a continuación.

```
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : 
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : C8-0A-A9-FA-DE-0D
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.3 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
<output omitted>
```

¿Cuál es la dirección IP de la PC-A?

192.168.1.3

¿Cuál es la máscara de subred de la PC-A?

255.255.255.0

¿Cuál es la dirección de gateway predeterminado de la PC-A?

192.168.1.1

¿Cuál es la dirección MAC de la PC-A?

Las respuestas varían.

- b. Emita el comando adecuado para probar el stack de protocolos TCP/IP con la NIC. ¿Qué comando utilizó?

```
C:\> ping 127.0.0.1
```

```
Pinging 127.0.0.1 with 32 bytes of data:  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

- c. Haga ping a la interfaz loopback del R1 desde el símbolo del sistema de la PC-A. ¿El ping se realizó correctamente?

Sí.

- d. Emita el comando adecuado en la PC-A para rastrear la lista de saltos de router para los paquetes provenientes de la PC-A a la interfaz loopback en R1. Registre el comando y el resultado a continuación. ¿Qué comando utilizó?

```
C:\> tracert 209.165.200.225
```

```
Traza a 209.165.200.225 sobre caminos de 30 saltos como máximo  
 1      1 ms      1 ms      1 ms  209.165.200.225  
Trace complete.
```

- e. Emita el comando adecuado en la PC-A para buscar las asignaciones de direcciones de capa 2 y capa 3 que se realizaron en la NIC. Registre sus respuestas a continuación. Registre solo las respuestas para la red 192.168.1.0/24. ¿Qué comando utilizó?

```
C:\> arp -a
```

```
Interfaz: 192.168.1.3 --- 0xb  
Dirección de Internet      Dirección física      Tipo  
192.168.1.1                30-f7-0d-a3-18-21    dinámico  
192.168.1.11              0c-d9-96-d2-34-c0    dinámico  
192.168.1.255             ff-ff-ff-ff-ff-ff    estático
```

Reflexión

¿Por qué es importante registrar los dispositivos de red?

Tener la información adecuada, incluidas las direcciones IP, las conexiones de puertos físicos, las versiones del IOS, las copias de los archivos de configuración y la cantidad de almacenamiento de memoria, puede ayudarlo en gran medida al realizar la resolución de problemas y las pruebas de línea de base de red. Tener una buena documentación también le permite recuperarse de las interrupciones de la red y reemplazar equipos cuando sea necesario.

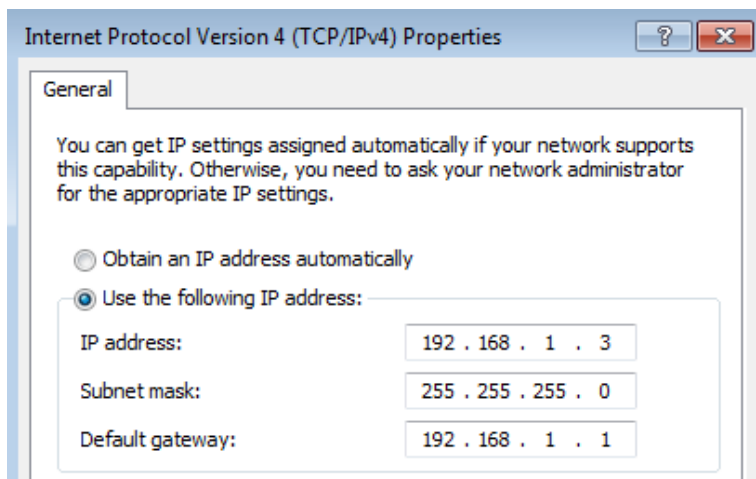
Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Ethernet Interface #1	Interfaz Ethernet n.º 2	Serial Interface #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Apéndice A: Detalles de configuración para los pasos de la parte 2

Paso 1: Configurar la dirección IPv4 para la PC.

Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A según la tabla de direccionamiento que se encuentra al principio de esta práctica de laboratorio.



Paso 2: Configurar el router.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Router> enable
Router#
```

- b. Configure la hora correcta en el router.

```
Router# clock set 10:40:30 6 February 2013
Router#
```

- c. Ingrese al modo de configuración global.

```
Router# config t
Router(config)#
```

- 1) Asigne un nombre de host al router. Use la topología y la tabla de direccionamiento como pautas.

```
Router(config)# hostname R1
R1(config)#
```

- 2) Desactive la búsqueda del DNS.

```
R1(config)# no ip domain-lookup
```

- 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd #Warning! Unauthorized Access is prohibited.#
```

- 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.

```
R1(config)# enable secret class
```

- 5) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.

```
R1(config)# line con 0
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

6) Encripte las contraseñas de texto no cifrado.

```
R1(config)# service password-encryption
```

7) Cree un nombre de dominio **cisco.com** para el acceso por SSH.

```
R1(config)# ip domain-name cisco.com
```

8) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.

```
R1(config)# username admin secret cisco
```

9) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.

```
R1(config)# crypto key generate rsa modulus 512
```

d. Configure el acceso a las líneas VTY.

1) Use la base de datos local para la autenticación de SSH.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# login local
```

2) Habilite SSH solo para el acceso de inicio de sesión.

```
R1(config-line)# transport input ssh
```

e. Vuelva al modo de configuración global.

```
R1(config-line)# exit
```

1) Cree la interfaz Loopback 0 y asigne la dirección IP según la tabla de direcciones.

```
R1(config)# interface loopback 0
```

```
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

2) Configure y habilite la interfaz G0/1 en el router.

```
R1(config-if)# int g0/1
```

```
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)# no shut
```

3) Configure las descripciones de interfaz para G0/1 y L0.

```
R1(config-if)# description Connected to LAN
```

```
R1(config-if)# int lo0
```

```
R1(config-if)# description Emulate ISP Connection
```

4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

```
R1(config-if)# end
```

```
R1# copy run start
```

Paso 3: Configurar el switch.

a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
```

```
Switch#
```

b. Configure la hora correcta en el switch.

```
Switch# clock set 10:52:30 6 February 2013
```

- c. Ingrese al modo de configuración global.

```
Switch# config t
```

- 1) Asigne un nombre de host al switch según la topología y la tabla de direccionamiento.

```
Switch(config)# hostname S1
```

- 2) Desactive la búsqueda del DNS.

```
S1(config)# no ip domain-lookup
```

- 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited.#
```

- 4) Asigne **class** como la contraseña encriptada del modo EXEC privilegiado.

```
S1(config)# enable secret class
```

- 5) Cifre las contraseñas de texto no cifrado.

```
S1(config)# service password-encryption
```

- 6) Cree un nombre de dominio **cisco.com** para el acceso por SSH.

```
S1(config)# ip domain-name cisco.com
```

- 7) Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.

```
S1(config)# username admin secret cisco
```

- 8) Genere una clave de módulo RSA. Use **512** para la cantidad de bits.

```
S1(config)# crypto key generate rsa modulus 512
```

- 9) Cree y active una dirección IP en el switch según la topología y la tabla de direccionamiento.

```
S1(config)# interface vlan 1
```

```
S1(config-if)# ip address 192.168.1.11 255.255.255.0
```

```
S1(config-if)# no shut
```

- 10) Configure el gateway predeterminado en el switch.

```
S1(config)# ip default-gateway 192.168.1.1
```

- 11) Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.

```
S1(config-if)# line con 0
```

```
S1(config-line)# password cisco
```

```
S1(config-line)# login
```

- d. Configure el acceso a las líneas VTY.

- 1) Use la base de datos local para la autenticación de SSH.

```
S1(config-line)# line vty 0 15
```

```
S1(config-line)# login local
```

- 2) Habilite SSH solo para el acceso de inicio de sesión.

```
S1(config-line)# transport input ssh
```

- 3) Ingrese al modo de configuración correspondiente para configurar las descripciones de interfaz de F0/5 y F0/6.

```
S1(config-line)# int f0/5
```

```
S1(config-if)# description Connected to R1
```



```
S1(config-if)# int f0/6
```

```
S1(config-if)# description Connected to PC-A
```

4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

```
S1(config-if)# end
```

```
S1# copy run start
```

Configuraciones de dispositivos

Router R1

```
R1#sh run
```

```
Building configuration...
```

```
Current configuration : 1545 bytes
```

```
!
```

```
version 15.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname R1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
```

```
!
```

```
no aaa new-model
```

```
no ip domain lookup
```

```
ip domain name cisco.com
```

```
ip cef
```

```
no ipv6 cef
```

```
multilink bundle-name authenticated
```

```
!
```

```
!
```

```
username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

```
!
```

```
!
```

```
ip ssh version 1
```

```
!
```

```
interface Loopback0
```

```
description Emulate ISP Connection
```

```
ip address 209.165.200.225 255.255.255.224
```

```
!
```

```
interface Embedded-Service-Engine0/0
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  description Connected to LAN
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
banner motd ^CWarning! Unauthorized access is prohibited.^C
!
line con 0
  password 7 060506324F41
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  login local
  transport input ssh
!
scheduler allocate 20000 1000
```

```
!  
End
```

Switch S1

```
S1#sh run  
Building configuration...  
  
Current configuration : 1752 bytes  
!  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY  
no aaa new-model  
system mtu routing 1500  
!  
!  
no ip domain-lookup  
ip domain-name cisco.com  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
ip ssh version 1  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
description Connected to R1
```

```
!  
interface FastEthernet0/6  
  description Connected to PC-A  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  ip address 192.168.1.11 255.255.255.0  
!  
ip default-gateway 192.168.1.1  
ip http server
```

```
ip http secure-server
!
banner motd ^CWarning! Unauthorized access is prohibited.^C
!
line con 0
  password 7 00071A150754
  login
line vty 0 4
  login local
  transport input ssh
line vty 5 15
  login local
  transport input ssh
!
end
```

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Configurar parámetros básicos de los dispositivos

Parte 2: Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

Parte 3: Utilizar un archivo de configuración de respaldo para restaurar un router

Información básica/Situación

Se recomienda mantener archivos de configuración de respaldo de routers y switches en caso de que sea necesario restaurar una configuración anterior. El software de emulación de terminal puede utilizarse para realizar una copia de seguridad o para restaurar fácilmente un archivo de configuración de router o switch.

En esta práctica de laboratorio, utilizará Tera Term para realizar una copia de seguridad de un archivo de configuración en ejecución del router, eliminar el archivo de configuración de inicio del router, volver a cargar el router y, luego, restaurar la configuración del router faltante a partir del archivo de configuración de respaldo.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: en esta práctica de laboratorio, se utiliza Tera Term 4.75. Se debe instalar Tera Term en la PC antes de comenzar la práctica de laboratorio. Puede descargar la versión más reciente de diversos sitios de Internet. Simplemente, busque una descarga de Tera Term.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP con un programa de emulación de terminal, por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.

Paso 2: Configurar los parámetros de red de la PC-A según la tabla de direccionamiento

Paso 3: Inicialice y vuelva a cargar el router y el switch.

Paso 4: Configurar el router.

- Acceda al router mediante el puerto de consola e introduzca el modo de configuración global.
- Establezca R1 como nombre del router.
- Desactive la búsqueda del DNS.
- Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- Encripte las contraseñas de texto no cifrado.
- Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- Configure y active la interfaz G0/1 en el router utilizando la información contenida en la Tabla de direccionamiento.
- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 5: Configure el switch.

- Acceda al switch mediante el puerto de consola e ingrese al modo de configuración global.
- Establezca S1 como nombre del switch.
- Desactive la búsqueda del DNS.

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal

- d. Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- e. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.
- f. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.
- g. Encripte las contraseñas de texto no cifrado.
- h. Cree un mensaje de aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- i. Configure la interfaz de administración predeterminada SVI con la información de dirección IP incluida en la tabla de direccionamiento.
- j. Configure el gateway predeterminado del switch.
- k. Guarde la configuración en ejecución en el archivo de configuración de inicio.

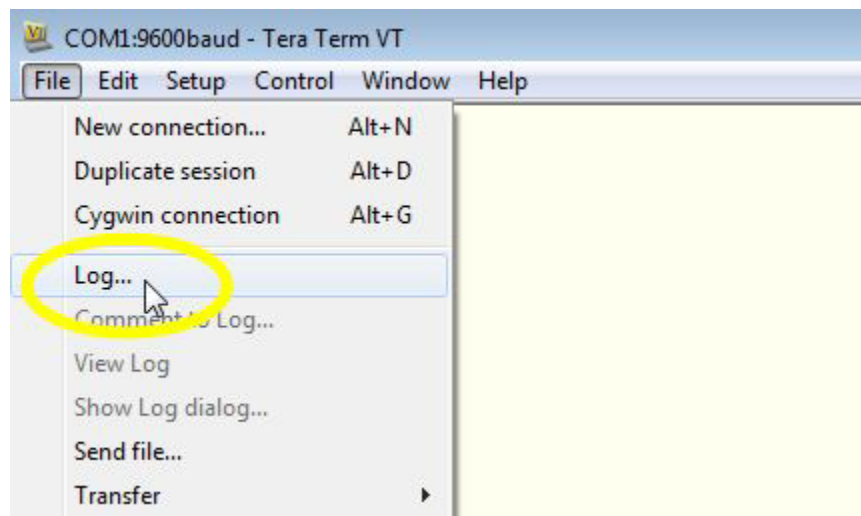
Parte 2: Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

Paso 1: Establecer una sesión de consola de Tera Term con el router

Inicie el programa Tera Term y, en la ventana New Connection (Conexión nueva), seleccione el botón de opción **Serial** y el puerto de comunicaciones apropiado para su PC (es decir, COM1).

Nota: si Tera Term no está instalado, puede descargar la versión más reciente de diversos sitios de Internet. Simplemente, busque una descarga de Tera Term.

- a. En Tera Term, presione Entrar para conectarse al router.
- b. En el menú **File** (Archivo), seleccione **Log...** (Registrar...) y guarde el archivo **teraterm.log** en el escritorio. Asegúrese de que las casillas de verificación **Append** (Anexar) y **Plain text** (Texto sin formato) estén activadas (marcadas).

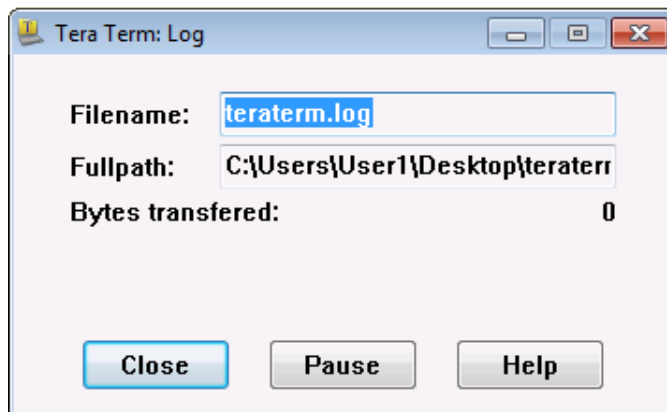


- c. El archivo de registro de Tera Term creará un registro de cada comando emitido y de cada resultado visualizado.

Nota: puede utilizar esta característica para capturar el resultado de varios comandos en secuencia y utilizarlo para fines de registro de la red. Por ejemplo, podría emitir los comandos **show version**, **show ip interface brief** y **show running-config** para capturar información sobre el router.

Paso 2: Mostrar la configuración en ejecución del router

- Utilice la contraseña de consola para iniciar sesión en el router.
- Ingresa al modo EXEC privilegiado.
- Ingresa el comando **show running-config**.
- Continúe presionando la barra espaciadora cuando se muestre **--More--** (Más), hasta que vuelva a ver la petición de entrada R1# del router.
- Haga clic en el ícono **Tera Term: Log** (Tera Term: registro) en la barra de tareas. Haga clic en **Close** (Cerrar) para finalizar la sesión de registro.



Nota: también puede copiar el texto de la ventana de Tera Term y pegarlo directamente en un editor de texto.

Parte 3: Utilizar un archivo de configuración de respaldo para restaurar un router

Paso 1: Borrar la configuración de inicio del router y volver a cargar

- En el modo EXEC privilegiado, elimine la configuración de inicio.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```
- Recargue el router.

```
R1# reload
Proceed with reload? [confirm]
```
- En la petición de entrada System Configuration Dialog (Cuadro de diálogo de configuración del sistema), escriba **no**. Aparecerá una petición de entrada de router que indica que hay un router sin configurar.

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!
<resultado omitido>
Router>
```

- d. Ingrese al modo EXEC privilegiado e introduzca un comando **show running-config** para verificar que todas las configuraciones anteriores se hayan borrado.

Paso 2: Editar el archivo de configuración de respaldo guardado a fin de prepararlo para restablecer la configuración del router

Para restaurar la configuración del router desde un archivo de configuración en ejecución de respaldo guardado, debe editar el texto.

- a. Abra el archivo de texto **teraterm.log**.
- b. Elimine cada aparición de **--More--** en el archivo de texto.

Nota: **--More--** se generó al presionar la barra espaciadora mientras se mostraba la configuración en ejecución.

- c. Elimine las líneas iniciales del archivo de configuración de respaldo, de modo que la primera línea comience con el primer comando de configuración, como se muestra a continuación.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

- d. Reemplace la contraseña secreta encriptada.

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

Cambie a:

```
enable secret class
```

- e. En las líneas para la interfaz GigabitEthernet0/1, inserte una línea nueva para habilitar la interfaz.

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
```

Cambie a:

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
no shutdown
```

- f. Cambie la configuración del anuncio del mensaje del día (MOTD) para insertar caracteres delimitadores como si introdujera el comando en la línea de comandos.

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

Change to:

```
banner motd " Unauthorized Access is Prohibited! "
```

- g. En las secciones line con 0 y vty 0 4, reemplace la contraseña encriptada.

```
line con 0
password 7 104D000A0618
line vty 0 4
password 7 104D000A0618
```

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal

Cambie a:

```
line con 0
  password cisco
line vty 0 4
  password cisco
```

- h. Después de realizar todas las ediciones al archivo de configuración de respaldo, guarde los cambios con el nombre de archivo **R1-config-backup**.

Nota: al guardar el archivo, es posible que se agregue automáticamente una extensión, como **.txt**, al nombre de archivo.

Paso 3: Restaurar la configuración del router

Puede restaurar la configuración en ejecución editada directamente en la terminal de consola en el modo de configuración global del router; las configuraciones se introducen como si fueran comandos escritos de forma individual en la petición de entrada de comandos.

- a. Ingrese al modo de configuración global desde la conexión de consola de Tera Term al router.
- b. En el menú **File** (Archivo), seleccione **Send file...** (Enviar archivo).
- c. Localice **R1-config-backup** y seleccione **Open** (Abrir).
- d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copy running-config startup-config
```

- e. Verifique la nueva configuración en ejecución.

Paso 4: Realizar una copia de seguridad y restaurar el switch

Vuelva al comienzo de la parte 2 y siga los mismos pasos para realizar una copia de seguridad de la configuración del switch y restaurarla.

Reflexión

¿Por qué cree que es importante utilizar un editor de texto en lugar de un procesador de textos para copiar y guardar las configuraciones de los comandos?

Un procesador de textos posiblemente añada caracteres de control especiales al texto, lo que dificultaría su uso para restaurar el router.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos, final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ipv6 cef
!
no ip domain lookup
ip cef
multilink bundle-name authenticated
!
!
```

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal

```
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 104D000A0618
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 104D000A0618
  login
  transport input all
```

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal

```
!  
scheduler allocate 20000 1000  
!  
end
```

Switch S1

```
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
system mtu routing 1500  
!  
no ip domain-lookup  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11
```

Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal

```
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
 ip address 192.168.1.11 255.255.255.0  
!  
ip default-gateway 192.168.1.1  
ip http server  
ip http secure-server  
banner motd ^C Unauthorized access is prohibited! ^C  
!  
line con 0  
 password 7 070C285F4D06  
 login  
line vty 0 4  
 password 7 070C285F4D06  
 login  
line vty 5 15  
 login  
!  
end
```

Práctica de laboratorio: Administración de archivos de configuración de dispositivos con TFTP, flash y USB (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

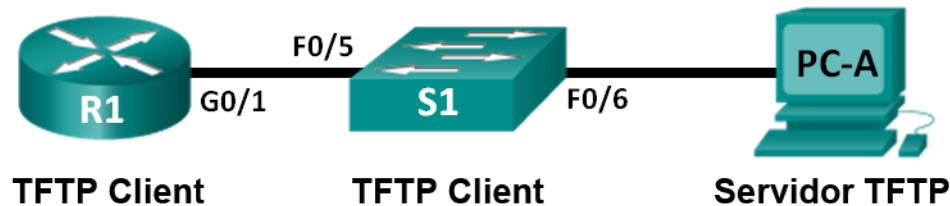


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Descargar software de servidor TFTP (optativo)

Parte 3: Utilizar TFTP para realizar una copia de seguridad de la configuración en ejecución del switch y restaurarla

Parte 4: Utilizar TFTP para realizar una copia de seguridad de la configuración en ejecución del router y restaurarla

Parte 5: Realizar copias de seguridad de las configuraciones en ejecución y restaurarlas mediante la memoria flash del router

Parte 6: Utilizar una unidad USB para realizar una copia de seguridad de la configuración en ejecución y restaurarla (optativo)

Información básica/Situación

Los dispositivos de red de Cisco a menudo se actualizan o intercambian por varios motivos. Es importante mantener copias de seguridad de las configuraciones más recientes de los dispositivos, así como un historial de los cambios de configuración. Se suele utilizar un servidor TFTP para realizar copias de seguridad de los archivos de configuración y de las imágenes del IOS en las redes de producción. Los servidores TFTP constituyen un método centralizado y seguro que se utiliza para almacenar las copias de seguridad de los archivos y para restaurarlos según sea necesario. Con un servidor TFTP centralizado, puede realizar copias de seguridad de archivos de numerosos dispositivos Cisco diferentes.

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

Además de un servidor TFTP, la mayoría de los routers Cisco actuales pueden realizar copias de seguridad de los archivos y restaurarlos localmente desde la memoria CompactFlash (CF) o desde una unidad flash USB. CF es un módulo de memoria extraíble que reemplazó la memoria flash interna limitada de los modelos de routers anteriores. La imagen del IOS para el router reside en la memoria CF, y el router utiliza dicha imagen para el proceso de arranque. Gracias al mayor tamaño de la memoria CF, es posible almacenar más archivos para propósitos de respaldo. También se puede utilizar una unidad flash USB extraíble para propósitos de respaldo.

En esta práctica de laboratorio, utilizará un software de servidor TFTP para realizar una copia de seguridad de la configuración en ejecución del dispositivo Cisco en el servidor TFTP o la memoria flash. Puede editar el archivo mediante un editor de texto y volver a copiar la nueva configuración en un dispositivo Cisco.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Nota para el instructor: si el tiempo es limitado, la práctica de laboratorio se puede dividir y realizar en varias sesiones. Por ejemplo, después de crear la red en la parte 1, se puede realizar cualquier combinación de las partes restantes de la práctica de laboratorio en cualquier orden.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS, versión 15.0(2), imagen lanbasek9 o similar)
- 1 PC (Windows 7, Vista o XP, con un servidor TFTP y un programa de emulación de terminal —por ejemplo, Tera Term)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.
- Unidad flash USB (optativa)

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y los parámetros básicos de configuración, como las direcciones IP de interfaz para el router R1, el switch S1 y la PC-A.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y realice el cableado según sea necesario.

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar los parámetros básicos para cada dispositivo

- a. Configure los parámetros básicos del dispositivo como se muestra en la tabla de direccionamiento.
- b. Para evitar que el router y el switch intenten traducir comandos introducidos de manera incorrecta como si fueran nombres de host, desactive la búsqueda de DNS.

- c. Asigne **class** como la contraseña encriptada de EXEC privilegiado.
- d. Configure las contraseñas y permita conectarse a las líneas de consola y vty utilizando **cisco** como la contraseña.
- e. Configure el gateway predeterminado para el switch.
- f. Encripte las contraseñas de texto no cifrado.
- g. Configure la dirección IP, la máscara de subred y el gateway predeterminado para la PC-A.

Paso 4: Verificar la conectividad desde PC-A

- a. Haga ping desde PC-A hasta S1.
- b. Haga ping desde PC-A hasta R1.

Si los pings no se realizan correctamente, lleve a cabo la resolución de problemas de las configuraciones básicas del dispositivo antes de continuar.

Parte 2: Descargar software de servidor TFTP (optativo)

Se encuentra disponible una serie de servidores TFTP gratuitos para descargar de Internet. En esta práctica de laboratorio, se utiliza el servidor Tftpd32.

Nota: para descargar un servidor TFTP de un sitio Web, se requiere acceso a Internet.

Paso 1: Verificar la disponibilidad de un servidor TFTP en la PC-A

- a. Haga clic en el menú **Inicio** y seleccione **Todos los programas**.
- b. Busque un servidor TFTP en la PC-A.
- c. Si no encuentra ninguno, puede descargar uno de Internet.

Paso 2: Descargar un servidor TFTP

- a. En esta práctica de laboratorio, se utiliza el servidor Tftpd32, que puede descargarse del siguiente enlace:
http://tftpd32.jounin.net/tftpd32_download.html
- b. Elija la versión adecuada para el sistema e instale el servidor.

Parte 3: Utilizar TFTP para realizar una copia de seguridad de la configuración en ejecución del switch y restaurarla

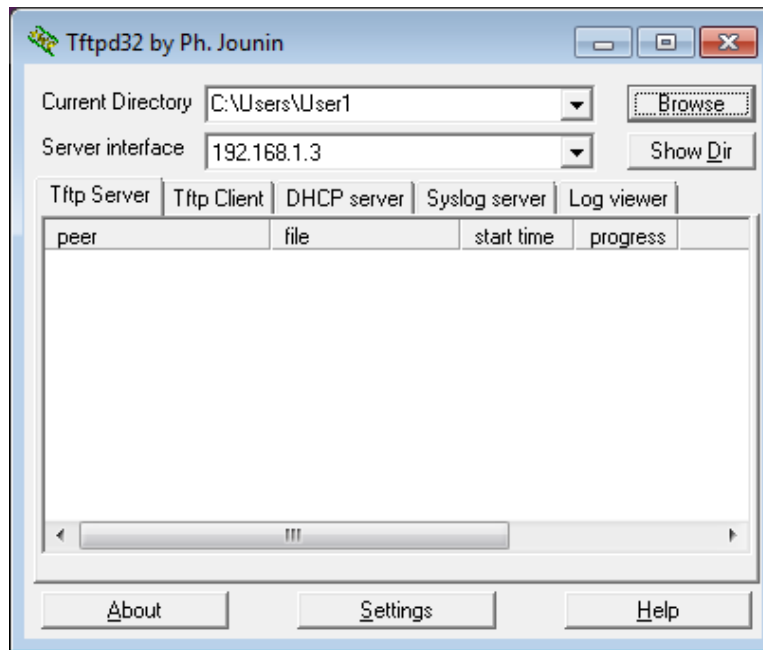
Paso 1: Verificar la conectividad al switch S1 desde PC-A

La aplicación TFTP utiliza el protocolo de transporte de capa 4 UDP, que está encapsulado en un paquete IP. Para que las transferencias de archivo TFTP funcionen, debe haber conectividad de capa 1 y capa 2 (Ethernet, en este caso) y capa 3 (IP) entre el cliente TFTP y el servidor TFTP. En la topología de la LAN en esta práctica de laboratorio solo se utiliza Ethernet en las capas 1 y 2. Sin embargo, las transferencias TFTP también pueden realizarse mediante enlaces WAN que utilizan otros enlaces físicos de capa 1 y protocolos de capa 2. La transferencia TFTP puede ocurrir siempre que haya conectividad IP entre el cliente y el servidor, la que se demuestra mediante el ping. Si los pings no se realizan correctamente, lleve a cabo la resolución de problemas de las configuraciones básicas del dispositivo antes de continuar.

Nota: un concepto erróneo habitual es que puede realizar una transferencia TFTP de un archivo mediante la conexión de consola. Pero esto no es así, dado que la conexión de consola no utiliza IP. La transferencia TFTP puede iniciarse en el dispositivo cliente (router o switch), mediante la conexión de consola, pero debe haber conectividad IP entre el cliente y el servidor para que se produzca la transferencia de archivos.

Paso 2: Iniciar el servidor TFTP

- Haga clic en el menú **Inicio** y seleccione **Todos los programas**.
- Busque y seleccione **Tftpd32** o **Tftpd64**. La ventana siguiente muestra que el servidor TFTP está listo.



- Haga clic en **Browse** (Examinar) para elegir un directorio en el que tenga permiso de escritura, como C:\Users\User1, o el escritorio.

Paso 3: Explorar el comando copy en un dispositivo Cisco

- Acceda al switch S1 mediante el puerto de consola y, en la petición de entrada del modo EXEC privilegiado, introduzca **copy ?** para que se muestren las opciones para la ubicación source (origen) o "from" ("desde") y otras opciones de copy disponibles. Puede especificar **flash:** o **flash0:** como la ubicación de origen; sin embargo, si simplemente proporciona un nombre de archivo como origen, se supone que la ubicación del archivo es **flash0:**, dado que es la ubicación predeterminada. Observe que **running-config** también es una opción para ubicar el origen.

```
S1# copy ?
/erase          Erase destination file system.
/error          Allow to copy error file.
/noverify       Don't verify image signature before reload.
/verify         Verify image signature before reload.
archive:        Copy from archive: file system
cns:            Copy from cns: file system
flash0:         Copy from flash0: file system
flash1:         Copy from flash1: file system
flash:          Copy from flash: file system
ftp:            Copy from ftp: file system
http:           Copy from http: file system
https:          Copy from https: file system
null:           Copy from null: file system
nvram:          Copy from nvram: file system
```

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
rcp:          Copy from rcp: file system
running-config Copy from current system configuration
scp:          Copy from scp: file system
startup-config Copy from startup configuration
system:       Copy from system: file system
tar:          Copy from tar: file system
tftp:         Copy from tftp: file system
tmpsys:       Copy from tmpsys: file system
xmodem:       Copy from xmodem: file system
ymodem:       Copy from ymodem: file system
```

- b. Después de seleccionar una ubicación de archivo de origen, utilice **?** para que se muestren las opciones de destino. En este ejemplo, el sistema de archivos de origen es el sistema de archivos **flash:** del S1.

```
S1# copy flash: ?
```

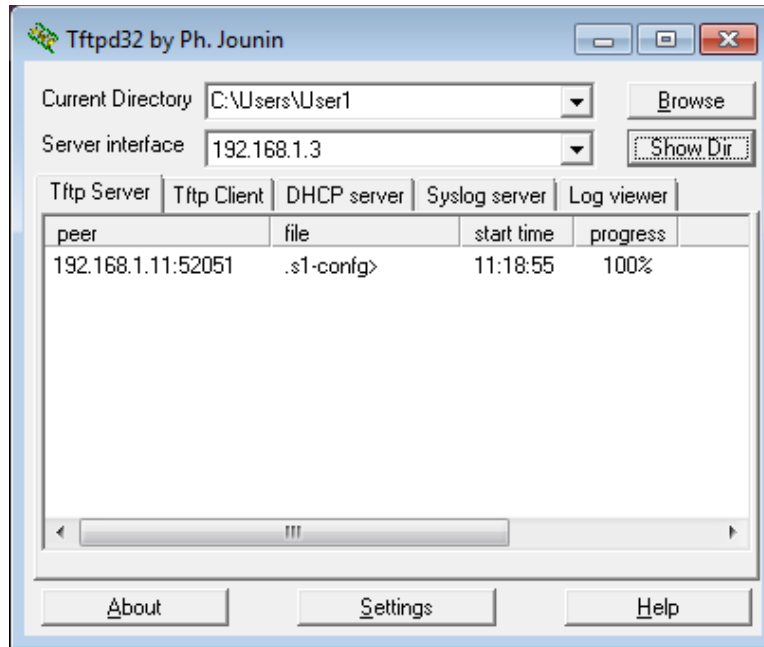
```
archive:      Copy to archive: file system
flash0:       Copy to flash0: file system
flash1:       Copy to flash1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
http:         Copy to http: file system
https:        Copy to https: file system
idconf        Load an IDConf configuration file
null:         Copy to null: file system
nvram:        Copy to nvram: file system
rcp:          Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
startup-config Copy to startup configuration
syslog:       Copy to syslog: file system
system:       Copy to system: file system
tftp:         Copy to tftp: file system
tmpsys:       Copy to tmpsys: file system
xmodem:       Copy to xmodem: file system
ymodem:       Copy to ymodem: file system
```

Paso 4: Transferir el archivo running-config del switch S1 al servidor TFTP en la PC-A

- a. Desde el modo EXEC privilegiado del switch, introduzca el comando **copy running-config tftp:**. Proporcione la dirección de host remoto del servidor TFTP (PC-A), 192.168.1.3. Presione Entrar para aceptar el nombre de archivo de destino predeterminado (**s1-config**) o proporcione otro nombre. Los signos de exclamación (!!) indican que el proceso de transferencia está en curso y que se realiza correctamente.

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-config]?
!!
1465 bytes copied in 0.663 secs (2210 bytes/sec)
S1#
```

El servidor TFTP también muestra el progreso durante la transferencia.



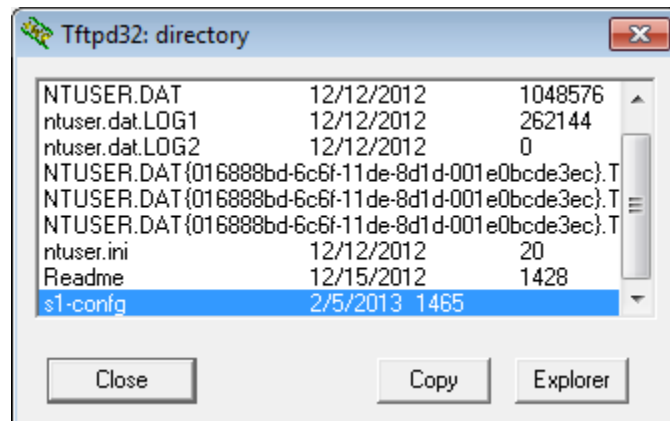
Nota: si no tiene permiso de escritura en el directorio actual que utiliza el servidor TFTP, aparece el siguiente mensaje de error:

```
S1# copy running-config tftp:  
Address or name of remote host []? 192.168.1.3  
Destination filename [s1-config]?  
%Error opening tftp://192.168.1.3/s1-config (Permission denied)
```

Para cambiar el directorio actual en el servidor TFTP, haga clic en **Browse** (Explorar) y seleccione otra carpeta.

Nota: otros problemas, como un firewall que bloquee el tráfico de TFTP, pueden impedir la transferencia TFTP. Si necesita mayor asistencia, consulte con el instructor.

- b. En la ventana del servidor Tftpd32, haga clic en **Show Dir** (Mostrar directorio) para verificar que el archivo **s1-config** se transfirió a su directorio actual. Al terminar, haga clic en **Close** (Cerrar).



Paso 5: Crear un archivo de configuración en ejecución del switch modificado

El archivo de configuración en ejecución guardado (**s1-config**) también se puede restaurar en el switch si se emite el comando **copy** en el switch. La versión original o modificada del archivo se puede copiar al sistema de archivos flash del switch.

- Navegue hasta el directorio de TFTP en la PC-A mediante el sistema de archivos de la PC-A y localice el archivo **s1-config**. Abra este archivo con un programa editor de textos, como WordPad.
- Una vez abierto el archivo, localice la línea **hostname S1**. Reemplace **S1** por **Switch1**. Elimine todas las claves de encriptación autogeneradas, según sea necesario. A continuación se muestra un ejemplo de las claves. Estas claves no se pueden exportar y pueden causar errores cuando se actualiza la configuración en ejecución.

```
crypto pki trustpoint TP-self-signed-1566151040
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1566151040
  revocation-check none
  rsakeypair TP-self-signed-1566151040
!
!
crypto pki certificate chain TP-self-signed-1566151040
certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
<resultado omitido>
  E99574A6 D945014F B6FE22F3 642EE29A 767EABF7 403930CA D2C59E23 102EC12E
  02F9C933 B3296D9E 095EBDAF 343D17F6 AF2831C7 6DA6DFE3 35B38D90 E6F07CD4
  40D96970 A0D12080 07A1C169 30B9D889 A6E2189C 75B988B9 0AF27EDC 6D6FA0E5
  CCFA6B29 729C1E0B 9DADACD0 3D7381
quit
```

- Guarde este archivo como un archivo de texto sin formato con un nombre nuevo (en este ejemplo, **Switch1-config.txt**).

Nota: al guardar el archivo, es posible que se agregue automáticamente una extensión, como **.txt**, al nombre de archivo.

- En la ventana del servidor Tftpd32, haga clic en **Show Dir** para verificar que el archivo **Switch1-config.txt** se encuentra en el directorio actual.

Paso 6: Subir el archivo de configuración en ejecución del servidor TFTP al switch S1

- Desde el modo EXEC privilegiado del switch, introduzca el comando **copy tftp running-config**. Proporcione la dirección de host remoto del servidor TFTP, 192.168.1.3. Introduzca el nombre de archivo nuevo, **Switch1-config.txt**. El signo de exclamación (!) indica que el proceso de transferencia está en curso y que se realiza correctamente.

```
S1# copy tftp: running-config
Address or name of remote host []? 192.168.1.3
Source filename []? Switch1-config.txt
Destination filename [running-config]?
Accessing tftp://192.168.1.3/Switch1-config.txt...
Loading Switch1-config.txt from 192.168.1.3 (via Vlan1): !
[OK - 1580 bytes]
[OK]
```

```
1580 bytes copied in 9.118 secs (173 bytes/sec)
*Mar  1 00:21:16.242: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new certificate
*Mar  1 00:21:16.251: %SYS-5-CONFIG_I: Configured from tftp://192.168.1.3/Switch1-
cfg.txt by console
```

Switch1#

Una vez finalizada la transferencia, la petición de entrada cambia de S1 a Switch1, porque la configuración en ejecución se actualizó con el comando **hostname Switch1** en la configuración en ejecución modificada.

- b. Introduzca el comando **show running-config** para examinar el archivo de configuración en ejecución.

Switch1# **show running-config**

Building configuration...

```
Current configuration : 3062 bytes
!
! Last configuration change at 00:09:34 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch1
!
boot-start-marker
boot-end-marker
<resultado omitido>
```

Nota: este procedimiento combina la configuración en ejecución del servidor TFTP con la configuración en ejecución actual en el switch o el router. Si se realizaron cambios a la configuración en ejecución actual, se agregan los comandos en la copia de TFTP. Como otra alternativa, si se emite el mismo comando, el comando correspondiente se actualiza en la configuración en ejecución actual del switch o el router.

Si desea reemplazar por completo la configuración en ejecución actual con la del servidor TFTP, debe eliminar la configuración de inicio del switch y volver a cargar el dispositivo. A continuación, necesitará configurar la dirección de administración de VLAN 1 para que haya conectividad IP entre el servidor TFTP y el switch.

Parte 4: Utilizar TFTP para realizar una copia de seguridad de la configuración en ejecución del router y restaurarla

El procedimiento de copia de seguridad y restauración de la parte 3 también se puede realizar en un router. En la parte 4, se realizará una copia de seguridad del archivo de configuración en ejecución y se restaurará mediante un servidor TFTP.

Paso 1: Verificar la conectividad al router R1 desde la PC-A

Si los pings no se realizan correctamente, lleve a cabo la resolución de problemas de las configuraciones básicas del dispositivo antes de continuar.

Paso 2: Transferir la configuración en ejecución del router R1 al servidor TFTP en la PC-A

- Desde el modo EXEC privilegiado en el R1, introduzca el comando **copy running-config tftp**. Proporcione la dirección de host remoto del servidor TFTP, 192.168.1.3, y acepte el nombre de archivo predeterminado.
- Verifique que el archivo se haya transferido al servidor TFTP.

Paso 3: Restaurar el archivo de configuración en ejecución en el router.

- Elimine el archivo de configuración de inicio del router.
- Recargue el router.
- Configure la interfaz G0/1 en el router con una dirección IP 192.168.1.1.
- Verifique la conectividad entre el router y la PC-A.
- Utilice el comando **copy** para transferir el archivo de configuración en ejecución del servidor TFTP al router. Utilice **running-config** como destino.
- Verifique que el router haya actualizado la configuración en ejecución.

Parte 5: Realizar copias de seguridad de las configuraciones y restaurarlas mediante la memoria flash del router

En el router 1941 y otros routers Cisco más nuevos, no hay memoria flash interna. La memoria flash de estos routers es memoria CompactFlash (CF). El uso de memoria CF proporciona una mayor disponibilidad de memoria flash y permite actualizaciones más sencillas, sin necesidad de abrir el gabinete del router. Además de almacenar los archivos necesarios, como las imágenes del IOS, la memoria CF puede almacenar otros archivos, como una copia de la configuración en ejecución. En la parte 5, creará una copia de seguridad del archivo de configuración en ejecución y la guardará en la memoria CF del router.

Nota: si el router no utiliza CF, es posible que no tenga memoria flash suficiente para almacenar la copia de seguridad del archivo de configuración en ejecución. Aun así, debe leer las instrucciones detenidamente y familiarizarse con los comandos.

Paso 1: Mostrar los sistemas de archivos del router

El comando **show file systems** muestra los sistemas de archivos disponibles en el router. El sistema de archivos **flash0:** es el sistema de archivos predeterminado de este router, como lo indica el asterisco (*) al comienzo de la línea. El signo de almohadilla (#) al final de la línea resaltada indica que la unidad es un disco de arranque. También se puede hacer referencia al sistema de archivos **flash0:** utilizando el nombre **flash:**. El tamaño total de **flash0:** es 256 MB, con 62 MB disponible. Actualmente, la ranura de **flash1:** está vacía, como lo indica el guión — debajo de los encabezados Size (b) (Tamaño [b]) y Free (b) (Libre [b]). Actualmente, **flash0:** y **nvrn:** son los únicos sistemas de archivos disponibles.

```
R1# show file systems
```

```
File Systems:
```

Size (b)	Free (b)	Type	Flags	Prefixes
-	-	opaque	rw	archive:
-	-	opaque	rw	system:
-	-	opaque	rw	tmpsys:
-	-	opaque	rw	null:
-	-	network	rw	tftp:
* 260153344	64499712	disk	rw	flash0: flash:#
-	-	disk	rw	flash1:
262136	242776	nvrn	rw	nvrn:

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
-          -   opaque    wo   syslog:
-          -   opaque    rw   xmodem:
-          -   opaque    rw   ymodem:
-          -   network    rw   rcp:
-          -   network    rw   http:
-          -   network    rw   ftp:
-          -   network    rw   scp:
-          -   opaque     ro   tar:
-          -   network    rw   https:
-          -   opaque     ro   cns:
```

¿Dónde se encuentra el archivo de configuración de inicio?

nvram:

Nota: verifique que haya, al menos, 1 MB (1 048 576 bytes) de espacio libre. Si no hay espacio suficiente en la memoria flash, consulte con el instructor para obtener instrucciones. Puede determinar el tamaño de la memoria flash y el espacio disponible mediante el comando **show flash** o **dir flash:** en la petición de entrada del modo EXEC privilegiado.

Paso 2: Copiar la configuración en ejecución del router a la memoria flash

Se puede copiar un archivo en la memoria flash introduciendo el comando **copy** en la petición de entrada del modo EXEC privilegiado. En este ejemplo, el archivo se copia en **flash0:** porque hay una sola unidad flash disponible, como se mostró en el paso anterior, y además es el sistema de archivos predeterminado. El archivo **R1-running-config-backup** se utiliza como nombre de archivo para el archivo de configuración en ejecución de respaldo.

Nota: recuerde que en el sistema de archivos del IOS los nombres de archivo distinguen mayúsculas de minúsculas.

- a. Copiar la configuración en ejecución a la memoria flash

```
R1# copy running-config flash:
Destination filename [running-config]? R1-running-config-backup
2169 bytes copied in 0.968 secs (2241 bytes/sec)
```

- b. Utilice el comando **dir** para verificar que la configuración en ejecución se haya copiado a la memoria flash.

```
R1# dir flash:
Directory of flash0:/

   1  drw-          0  Nov 15 2011 14:59:04 +00:00  ipsdir
<resultado omitido>
  20  -rw-      67998028  Aug 7 2012 17:39:16 +00:00  c1900-universalk9-mz.SPA.152-
4.M3.bin
  22  -rw-       2169   Feb 4 2013 23:57:54 +00:00  R1-running-config-backup
  24  -rw-       5865   Jul 10 2012 14:46:22 +00:00  lpnat
  25  -rw-       6458   Jul 17 2012 00:12:40 +00:00  lpIPSec

260153344 bytes total (64503808 bytes free)
```

- c. Utilice el comando **more** para ver el archivo de configuración en ejecución en la memoria flash. Examine el resultado del archivo y desplácese hasta la sección Interface (Interfaz). Observe que el comando **no shutdown** no se incluyó con GigabitEthernet0/1. Cuando se utiliza este archivo para actualizar la configuración en ejecución en el router, la interfaz se desactiva.

```
R1# more flash:R1-running-config-backup
<resultado omitido>
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
<resultado omitido>
```

Paso 3: Borrar la configuración de inicio y volver a cargar el router

Paso 4: Restaurar la configuración en ejecución desde la memoria flash

- a. Verifique que el router tenga la configuración inicial predeterminada.
- b. Copie el archivo de configuración en ejecución guardado en la memoria flash para actualizar la configuración en ejecución.

```
Router# copy flash:R1-running-config-backup running-config
```

- c. Use el comando **show ip interface brief** para ver el estado de las interfaces. La interfaz GigabitEthernet0/1 no se activó cuando se actualizó la configuración en ejecución, porque está administrativamente inactiva.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

La interfaz se puede activar mediante el comando **no shutdown** en el modo de configuración de interfaz en el router.

Otra opción es agregar el comando **no shutdown** para la interfaz GigabitEthernet0/1 en el archivo guardado antes de actualizar el archivo de configuración en ejecución del router. Esto se hará en la parte 6, en la que se utilizará un archivo guardado en una unidad flash USB.

Nota: dado que la dirección IP se configuró mediante una transferencia de archivos, se incluye el protocolo TFTP debajo del encabezado Method (Método) del resultado del comando **show ip interface brief**.

Parte 6: Utilizar una unidad USB para realizar una copia de seguridad de la configuración en ejecución y restaurarla (optativo)

Se puede utilizar una unidad flash USB para realizar copias de seguridad de los archivos de un router con un puerto USB disponible y también para restaurarlos. En los routers 1941, hay dos puertos USB disponibles.

Nota: no hay puertos USB disponibles en todos los routers, pero igualmente debe familiarizarse con los comandos.

Nota: dado que algunos routers ISR G1 (1841, 2801 o 2811) utilizan sistemas de archivos de tabla de asignación de archivos (FAT), hay un límite de tamaño máximo para las unidades flash USB que pueden usarse en esta parte de la práctica de laboratorio. El tamaño máximo recomendado para un ISR G1 es 4 GB. Si recibe el siguiente mensaje, es posible que el sistema de archivos de la unidad flash USB no sea compatible con el router o que la capacidad de la unidad haya excedido el tamaño máximo del sistema de archivos FAT en el router.

```
*Feb  8 13:51:34.831: %USBFLASH-4-FORMAT: usbflash0 contains unexpected values in
partition table or boot sector. Device needs formatting before use!
```

Paso 1: Insertar una unidad flash USB en un puerto USB del router

Observe el mensaje de la terminal al insertar la unidad flash USB.

```
R1#  
* *Feb  5 20:38:04.678: %USBFLASH-5-CHANGE: usbflash0 has been inserted!
```

Paso 2: Verificar que el sistema de archivos flash USB esté disponible

```
R1# show file systems
```

File Systems:

	Size(b)	Free(b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	260153344	64512000	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	244676	nvr	rw	nvr
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	opaque	ro	tar:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:
	7728881664	7703973888	usbflash	rw	usbflash0:

Paso 3: Copiar el archivo de configuración en ejecución a la unidad flash USB

Utilice el comando **copy** para copiar el archivo de configuración en ejecución a la unidad flash USB.

```
R1# copy running-config usbflash0:
```

Destination filename [running-config]? **R1-running-config-backup.txt**

2198 bytes copied in 0.708 secs (3105 bytes/sec)

Paso 4: Enumerar los archivos en la unidad flash USB

Utilice el comando **dir** (o el comando **show**) en el router para enumerar los archivos en la unidad flash USB. En este ejemplo, la unidad flash se insertó en el puerto USB 0 del router.

```
R1# dir usbflash0:
```

Directory of usbflash0:/

1	-rw-	16216	Nov 15 2006 09:34:04 +00:00	ConditionsFR.txt
2	-rw-	2462	May 26 2006 21:33:40 +00:00	Nlm.ico
3	-rw-	24810439	Apr 16 2010 10:28:00 +00:00	Twice.exe
4	-rw-	71	Jun 4 2010 11:23:06 +00:00	AUTORUN.INF

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
5 -rw-          65327  Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt
6 -rw-           2198   Feb 5 2013 21:36:40 +00:00  R1-running-config-backup.txt
```

7728881664 bytes total (7703973888 bytes free)

Paso 5: Borrar la configuración de inicio y volver a cargar el router

Paso 6: Modificar el archivo guardado

- a. Quite la unidad USB del router.

```
Router#
*Feb  5 21:41:51.134: %USBFLASH-5-CHANGE: usbflash0 has been removed!
```

- b. Introduzca la unidad USB en el puerto USB de una PC.

- c. Modifique el archivo mediante un editor de texto. El comando **no shutdown** se agrega a la interfaz GigabitEthernet0/1. Guarde el archivo como archivo de texto sin formato en la unidad flash USB.

```
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
no shutdown
duplex auto
speed auto
!
```

- d. Quite la unidad flash USB de la PC en forma segura.

Paso 7: Restaurar el archivo de configuración en ejecución en el router.

- a. Inserte la unidad flash USB en un puerto USB del router. Tenga en cuenta el número de puerto en el que se insertó la unidad USB si hay más de un puerto USB disponible en el router.

```
*Feb  5 21:52:00.214: %USBFLASH-5-CHANGE: usbflash1 has been inserted!
```

- b. Enumere los archivos en la unidad flash USB.

```
Router# dir usbflash1:
Directory of usbflash1:/
```

```
1 -rw-          16216  Nov 15 2006 09:34:04 +00:00  ConditionsFR.txt
2 -rw-           2462   May 26 2006 21:33:40 +00:00  Nlm.ico
3 -rw-       24810439   Apr 16 2010 10:28:00 +00:00  Twice.exe
4 -rw-            71    Jun 4 2010 11:23:06 +00:00  AUTORUN.INF
5 -rw-          65327   Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt
6 -rw-           2344   Feb 6 2013 14:42:30 +00:00  R1-running-config-backup.txt
```

7728881664 bytes total (7703965696 bytes free)

- c. Copie el archivo de configuración en ejecución en el router.

```
Router# copy usbflash1:R1-running-config-backup.txt running-config
Destination filename [running-config]?
2344 bytes copied in 0.184 secs (12739 bytes/sec)
R1#
```

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

- d. Verifique que la interfaz GigabitEthernet0/1 esté activada.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

La interfaz G0/1 está activada porque la configuración en ejecución modificada incluía el comando **no shutdown**.

Reflexión

1. ¿Qué comando utiliza para copiar un archivo de la memoria flash a una unidad USB?

```
copy flash:filename usbflash0:
```

2. ¿Qué comando utiliza para copiar un archivo de la unidad flash USB a un servidor TFTP?

```
copy usbflash0:filename tftp:
```

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.				

Configuraciones de dispositivos

Router R1

```
R1# show run
Building configuration...

Current configuration : 1283 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
```

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
 password 14141B180F0B
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 070C285F4D06
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#show run
Building configuration...

Current configuration : 1498 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
```


Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
```

Práctica de laboratorio: Administración de archivos de configuración de dispositivos mediante TFTP, flash y USB

```
!  
!  
line con 0  
  password 045802150C2E  
  login  
line vty 0 4  
  password 045802150C2E  
  login  
line vty 5 15  
  password 045802150C2E  
  login  
!  
end
```

Práctica de práctica de laboratorio: Investigación de procedimientos de recuperación de contraseña (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Parte 1: Investigar el registro de configuración

- Identificar el propósito del registro de configuración.
- Describir el comportamiento del router para distintos valores del registro de configuración.

Parte 2: Registrar el procedimiento de recuperación de contraseña para un router Cisco específico

- Investigar y registrar el proceso de recuperación de contraseñas en un router Cisco específico.
- Responder las preguntas sobre la base del procedimiento investigado.

Información básica/Situación

El propósito de esta práctica de laboratorio es investigar el procedimiento para recuperar o restablecer la contraseña de enable en un router Cisco específico. La contraseña de enable protege el acceso al modo EXEC privilegiado y al modo de configuración en los dispositivos Cisco. La contraseña de enable se puede recuperar, pero la contraseña secreta de enable está encriptada y debe reemplazarse por una contraseña nueva.

Para omitir una contraseña, el usuario debe estar familiarizado con el modo monitor ROM (ROMMON), así como con los parámetros del registro de configuración para los routers Cisco. ROMMON es el software básico de CLI almacenado en la ROM, que se puede utilizar para resolver problemas de errores de arranque y para recuperar un router cuando no se encuentra un IOS.

En esta práctica de laboratorio, comenzará investigando el propósito del registro de configuración para los dispositivos Cisco y los parámetros de dicho registro. Luego, investigará y detallará el procedimiento exacto para la recuperación de la contraseña en un router Cisco específico.

Recursos necesarios

- Dispositivo con acceso a Internet

Parte 1: Investigar el registro de configuración

Para recuperar o restablecer una contraseña de enable, un usuario utiliza la interfaz ROMMON para instruir al router que omita la configuración de inicio durante el arranque. Una vez que se arranca el dispositivo, el usuario accede al modo EXEC privilegiado, sobrescribe la configuración en ejecución con la configuración de inicio guardada, recupera o restablece la contraseña, y restaura el proceso de arranque del router para que incluya la configuración de inicio.

El registro de configuración del router desempeña un papel fundamental en el proceso de recuperación de contraseñas. En la primera parte de esta práctica de laboratorio, investigará el propósito del registro de configuración de un router y el significado de ciertos valores de dicho registro.

Nota para el instructor: los estudiantes deben visitar la página **Use of Configuration Register on All Cisco Routers** (Uso del registro de configuración en todos los routers Cisco) en el sitio Web de Cisco http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a008022493f.shtml.

Paso 1: Describir el propósito del registro de configuración

¿Cuál es el propósito del registro de configuración?

El registro de configuración se puede utilizar para cambiar la forma en que arranca el router, las opciones de arranque y la velocidad de la consola.

¿Qué comando cambia el registro de configuración en el modo de configuración?

config-register

¿Qué comando cambia el registro de configuración en la interfaz ROMMON?

confreg

Paso 2: Determinar los valores del registro de configuración y sus significados

Investigue y detalle el comportamiento del router para los siguientes valores del registro de configuración.

0x2102

Para el valor 0x2102 del registro de configuración, un router carga el IOS desde memoria flash y después carga la configuración de inicio desde la NVRAM, si estuviera presente. Si no se encuentra ningún sistema operativo, el router arranca en ROMMON.

0x2142

Para el valor 0x2142 del registro de configuración, un router carga el IOS desde la memoria flash, omite la configuración de inicio en la NVRAM y proporciona una petición de entrada para el cuadro de diálogo de configuración inicial. Si no se encuentra ningún sistema operativo, el router arranca en ROMMON.

¿Cuál es la diferencia entre estos dos valores del registro de configuración?

El parámetro 0x2102 es para el funcionamiento normal del router. El parámetro 0x2142 omite la configuración de inicio al permitirle a un usuario recuperar o restablecer la contraseña de enable.

Parte 2: Registrar el procedimiento de recuperación de contraseña para un router Cisco específico

En la parte 2, describirá el procedimiento exacto para recuperar o restablecer una contraseña de un router Cisco específico y responderá preguntas sobre la base de la investigación realizada. El instructor le proporcionará el modelo exacto de router que debe investigar.

Nota para el instructor: los estudiantes deben visitar la página **Password Recovery Procedures** (Procedimientos de recuperación de contraseñas) en el sitio Web de Cisco http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml para conocer los procedimientos pertinentes para una variedad de dispositivos Cisco.

Paso 1: Detallar el proceso de recuperación de una contraseña en un router Cisco específico

Investigue y detalle los pasos y los comandos que necesita para recuperar o restablecer la contraseña de enable o la contraseña secreta de enable en su router Cisco. Resuma los pasos con sus propias palabras.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

Para recuperar o restablecer la contraseña de enable en el router Cisco serie 1900, se deben seguir estos pasos:

1. Establecer una conexión de terminal con el router utilizando Tera Term u otro emulador de terminal.
2. Arrancar en modo ROMMON, ya sea por medio de eliminar la memoria flash y reiniciar, o presionando Alt-b durante el reinicio.
3. Escribir **confreg 0x2142** en la petición de entrada de ROMMON.
4. Escribir **reset** en la siguiente petición de entrada de ROMMON.
5. Escribir **no** en el cuadro de diálogo de configuración inicial.
6. Escribir **enable** en la petición de entrada del router.
7. Escribir **copy startup-config running-config** para cargar la configuración de inicio.
8. Escribir **show running-config**.
9. Registrar una contraseña de enable sin encriptar. Restablecer una contraseña de enable encriptada.
10. En el modo de configuración, escribir **config-register 0x2102**.
11. En el modo privilegiado, escribir **copy running-config startup-config** para guardar la configuración.
12. Utilizar el comando **show version** para verificar los parámetros del registro de configuración.

Paso 2: Responder las preguntas sobre el procedimiento de recuperación de contraseñas

Utilice el proceso de recuperación de contraseñas para responder las siguientes preguntas.

Describa cómo buscar los parámetros actuales del registro de configuración.

El comando **show version** proporciona los parámetros actuales del registro de configuración.

Describa el proceso para ingresar al modo ROMMON.

Un usuario puede quitar la memoria flash y reiniciar el router para que arranque en la utilidad ROMMON. El usuario también puede arrancar el router y presionar **alt+b** si utiliza Tera Term.

¿Qué comandos necesita para acceder a la interfaz de ROMMON?

Un usuario debe introducir **confreg 0x2142** para cambiar los parámetros de configuración, seguido por **reset** para reiniciar el router.

¿Qué mensaje esperarías ver cuando arranque el router?

Si un router no carga la configuración de inicio, el usuario debería esperar ver el mensaje “Continue with configuration dialog?” (“¿Desea continuar con el cuadro de diálogo de configuración?”).

¿Por qué es importante cargar la configuración de inicio en la configuración en ejecución?

Cargar la configuración de inicio en la configuración en ejecución asegura que la configuración de inicio original permanezca intacta si el usuario realiza un guardado durante el proceso de recuperación de contraseña.

¿Por qué es importante volver a cambiar el registro de configuración al valor original después de recuperar la contraseña?

Devolver el registro de configuración a su valor original asegura que el router cargue la configuración de inicio durante la recarga siguiente.

Reflexión

1. ¿Por qué es de suma importancia que un router esté protegido físicamente para impedir el acceso no autorizado?

El procedimiento de recuperación de contraseñas se basa en una conexión de consola, lo que requiere acceso físico directo al dispositivo. Por esta razón, impedir el acceso de usuarios no autorizados al dispositivo físico es una parte fundamental del plan de seguridad general.

Diseño y armado de una red de pequeña empresa (proyecto final)

(versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

Explicar la forma en que se crea, se configura y se verifica una red pequeña de segmentos conectados directamente.

Los estudiantes demostrarán que saben cómo diseñar, configurar, verificar y hacer segura una red muy pequeña. El registro y la presentación también son componentes fundamentales de este proyecto final.

Información básica/Situación

Nota: conviene realizar esta actividad en grupos de dos a tres estudiantes.

Diseñe y arme una red desde cero.

- El diseño debe incluir, como mínimo, un router, un switch y una PC.
- Configure completamente la red y utilice IPv4 o IPv6 (debe incluirse la división en subredes como parte del esquema de direccionamiento).
- Revise la red mediante, por lo menos, cinco comandos show.
- Proteja la red con SSH, contraseñas seguras y contraseñas de consola (como mínimo).

Cree una tabla de evaluación para utilizarla en la calificación informal de pares. En forma alternativa, el instructor puede elegir usar la tabla de evaluación que se proporciona con esta actividad.

Presente su proyecto final a la clase y esté preparado para responder las preguntas de sus pares y del instructor.

Notas para el instructor: se sugiere que esta actividad de creación de modelos sea una asignación con calificación para realizar después de completar los capítulos del 1 al 11. Los estudiantes deben ser capaces de mostrar cómo se diseñan, configuran, verifican y protegen las redes pequeñas. El registro es un factor importante de este proyecto, y los estudiantes deben poder explicar el diseño y la verificación de la red mediante el uso de los comandos **show**.

Recursos necesarios

- Packet Tracer
- Tabla de evaluación creada por el estudiante o el grupo para evaluar la asignación

Reflexión

1. ¿Cuál fue la parte más difícil de esta actividad?

Las respuestas varían.

2. ¿Por qué piensa que el registro de la red es tan importante en esta actividad y en el mundo real?

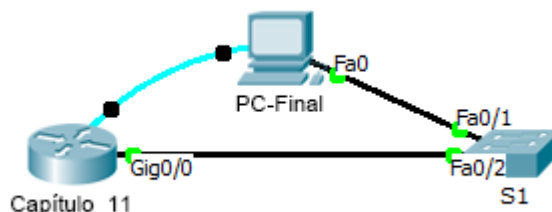
El registro es fundamental para una buena administración de red. Sin él, los administradores de red tienen que recrear topologías y verificar físicamente el direccionamiento, entre otras tareas. Esto toma tiempo, que podría dedicarse a cualquier otro asunto.

A continuación, se proporciona una tabla de evaluación sugerida y ejemplos de registro:

Nota: esta tabla de evaluación incluye un total de 100 puntos para la categoría de puntos obtenidos (si se cumplen los estándares mínimos). Los instructores podrán considerar agregar puntos extra por trabajo adicional o avanzado en cualquier categoría de requisitos.

Requisito	Puntos obtenidos
Topología física: mínimo un router, un switch, una PC	(20 sugeridos)
Direccionamiento lógico: ¿se utiliza la división en subredes?	(20 sugeridos)
Prueba de conectividad: hacer ping al router	(20 sugeridos)
Comandos show (por lo menos, cinco comandos registrados como línea de base)	(20 sugeridos)
Seguridad (SSH, contraseñas seguras, seguridad de la consola); documentada mediante el comando show running-configuration	(20 sugeridos)

Cree una red pequeña de segmentos conectados directamente, con un mínimo de un router, un switch y una PC, e incluya una captura de pantalla de la red en el documento de registro final.



Configure la red de modo de incluir switches, routers y dispositivos finales y utilice su propio direccionamiento de red. Debe utilizar división en subredes de algún tipo y puede usar direccionamiento lógico IPv4 o IPv6. Cree una tabla que muestre el esquema de direccionamiento físico para el router, el switch y la PC, e inclúyala en el documento de registro final.

Nombre del dispositivo	Dirección IP	Máscara de subred
Capítulo_11	Gig0/0 – 192.168.1.30	255.255.255.224
S1	VLAN1 – 192.168.1.20	255.255.255.224
PC_Capstone	Fa0 – 192.168.1.10	255.255.255.224

Verifique la red mediante los comandos show (por lo menos, cinco) para proporcionar una línea de base de rendimiento. Debe poder argumentar por qué eligió los comandos show que seleccionó y qué significa el resultado (utilice todas las actividades de Packet Tracer para los capítulos del 1 al 11). Conserve capturas de pantalla de los resultados e inclúyalas en el documento de registro final.

```
Chapter_11# show arp
Protocol Address           Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.10          42         0006.2AAC.4D31  ARPA   GigabitEthernet0/0
Internet 192.168.1.20          15         0006.2A79.8B1E  ARPA   GigabitEthernet0/0
Internet 192.168.1.30          -          0060.7032.3601  ARPA   GigabitEthernet0/0
Chapter_11#
```

```
S1#show arp
Protocol Address           Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.10          13         0006.2AAC.4D31  ARPA   Vlan1
Internet 192.168.1.20          -          0006.2A79.8B1E  ARPA   Vlan1
Internet 192.168.1.30          13         0060.7032.3601  ARPA   Vlan1
S1#
```

```
Chapter_11#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.30/27
GigabitEthernet0/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
```

```
Chapter_11#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.30/32 is directly connected, GigabitEthernet0/0
Chapter_11#
```

```
S1#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
S1#			

Chapter_11#show int

GigabitEthernet0/0 is up, line protocol is up (connected)

Hardware is CN Gigabit Ethernet, address is 0060.7032.3601 (bia 0060.7032.3601)
Internet address is 192.168.1.30/27
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
7 packets input, 196 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
9 packets output, 252 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
Hardware is CN Gigabit Ethernet, address is 0060.7032.3602 (bia 0060.7032.3602)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Vlan1 is administratively down, line protocol is down
Hardware is CPU Interface, address is 000b.be45.b842 (bia 000b.be45.b842)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
Chapter_11#

```
Chapter_11#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, REL
EASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 hours, 47 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-----
Device#      PID                      SN
-----
*0           CISC01941/K9             FTX152453SZ

Technology Package License Information for Module:'c1900'

-----
Technology    Technology-package      Technology-package
              Current          Type                Next reboot
-----
ipbase        ipbasek9               Permanent           ipbasek9
security      None                   None                None
data          None                   None                None

Configuration register is 0x2102

Chapter_11#
```

Proteja la red mediante configuración común para incluir SSH, contraseñas seguras, seguridad de la consola, entre otros, y muestre los comandos configurados recreando una pantalla del comando show running-configuration como resultado. Inclúyala en el documento de registro final.

Chapter_11#show run	
Building configuration...	
Current configuration : 842 bytes	
!	
version 15.1	
no service timestamps log datetime msec	
no service timestamps debug datetime msec	
service password-encryption	
security passwords min-length 8	
!	
hostname Chapter_11	
!	
login block-for 120 attempts 3 within 60	
!	
license udi pid CISCO1941/K9 sn FTX152453SZ	
!	
spanning-tree mode pvst	
!	
interface GigabitEthernet0/0	interface GigabitEthernet0/1
ip address 192.168.1.30 255.255.255.224	no ip address
duplex auto	duplex auto
speed auto	speed auto
!	shutdown
	!
	interface Vlan1
	no ip address
	shutdown
	!
	ip classless
	!
	line con 0
	password 7 0822455D0A16
	login
	!
	line aux 0
	!
	line vty 0 4
	password 7 0822455D0A165445415F5952
	login
	!
	end

Identifique los elementos del modelo que corresponden a aplicaciones del mundo real:

Todas las facetas de esta actividad corresponden a contenido relacionado con TI y a aplicaciones del mundo reales, dado que se trata de una actividad de culminación para los 11 capítulos.