EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de Minatitlán

Ingeniería En Sistemas Computacionales

“MANUAL DE PRÁCTICAS DE LA MATERIA DE CONMUTACION Y ENRUTAMIENTO EN REDES DE DATOS”

MINATITLÁN, VER. JULIO 2023

Conmutación y Enrutamiento en Redes de Datos.

Prácticas que se implementan.

Docente: Isaías Torres Martínez.

1. Configuración de los parámetros básicos de un switch

Topología

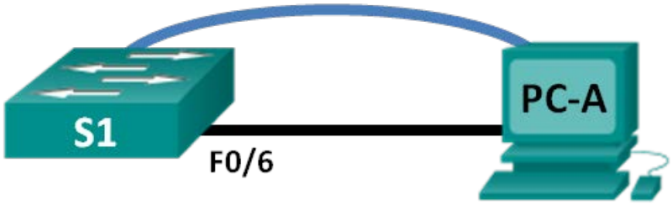


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: tender el cableado de red y verificar la configuración predeterminada del switch

Parte 2: configurar los parámetros básicos de los dispositivos de red

- Configurar los parámetros básicos del switch.
- Configurar la dirección IP de la computadora.

Parte 3: verificar y probar la conectividad de red

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

Parte 4: administrar la tabla de direcciones MAC

- Registrar la dirección MAC del host.
- Determine las direcciones MAC que el switch ha aprendido.
- Enumere las opciones del comando **show mac address-table**.
- Configure una dirección MAC estática.

Información básica/situación

Los switches Cisco se pueden configurar con una dirección IP especial, conocida como “interfaz virtual de switch” (SVI). La SVI o dirección de administración se puede usar para el acceso remoto al switch a fin de ver o configurar parámetros. Si se asigna una dirección IP a la SVI de la VLAN 1, de manera predeterminada, todos los puertos en la VLAN 1 tienen acceso a la dirección IP de administración de SVI.

En esta práctica de laboratorio, armará una topología simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Examinará la configuración predeterminada del switch antes de configurar los parámetros básicos del switch. Esta configuración básica del switch incluye el nombre del dispositivo, la descripción de interfaces, las contraseñas locales, el mensaje del día (MOTD), el direccionamiento IP, la configuración de una dirección MAC estática y la demostración del uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host que solo usa puertos Ethernet y de consola.

Nota: el switch que se utiliza es Cisco Catalyst 2960 con IOS de Cisco versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros 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.

Nota: asegúrese de que el switch se haya borrado y no tenga una configuración de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 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, y capacidad para Telnet)
- Cable de consola para configurar el dispositivo con IOS de Cisco mediante el puerto de consola
- Cable Ethernet, como se muestra en la topología

Parte 1. tender el cableado de red y verificar la configuración predeterminada del switch

En la parte 1, establecerá la topología de la red y verificará la configuración predeterminada del switch.

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

a. Realice el cableado de la conexión de consola tal como se muestra en la topología. En esta instancia, no conecte el cable Ethernet de la PC-A.

   Nota: si utiliza Netlab, puede desactivar F0/6 en el S1, lo que tiene el mismo efecto que no conectar la PC-A al S1.

b. Con Tera Term u otro programa de emulación de terminal, cree una conexión de consola de la PC-A al switch.

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

Paso 2. Verificar la configuración predeterminada del switch.

En este paso, examinará la configuración predeterminada del switch, como la configuración actual del switch, la información de IOS, las propiedades de las interfaces, la información de la VLAN y la memoria flash.

Puede acceder a todos los comandos IOS del switch en el modo EXEC privilegiado. Se debe restringir el acceso al modo EXEC privilegiado con protección con contraseña para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento. Establecerá las contraseñas más adelante en esta práctica de laboratorio.

El conjunto de comandos del modo EXEC privilegiado incluye los comandos del modo EXEC del usuario y el comando **configure**, a través del cual se obtiene acceso a los modos de comando restantes. Use el comando **enable** para ingresar al modo EXEC privilegiado.

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>. Use el comando **enable** para ingresar al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Verifique que el archivo de configuración esté limpio con el comando **show running-config** del modo EXEC privilegiado. Si se guardó un archivo de configuración anteriormente, se debe eliminar. 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, borre y recargue el switch.

Nota: en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

b. Examine el archivo de configuración activa actual.

```
Switch# show running-config
```

¿Cuántas interfaces FastEthernet tiene un switch 2960?

¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960?

¿Cuál es el rango de valores que se muestra para las líneas vty?

c. Examine el archivo de configuración de inicio en la NVRAM.

```
Switch# show startup-config
startup-config is not present
```

¿Por qué aparece este mensaje?

d. Examine las características de la SVI para la VLAN 1.

```
Switch# show interface vlan1
```

¿Hay alguna dirección IP asignada a la VLAN 1?

¿Cuál es la dirección MAC de esta SVI? Las respuestas varían.

¿Está activa esta interfaz?

e. Examine las propiedades IP de la VLAN 1 SVI.

```
Switch# show ip interface vlan1
```

¿Qué resultado ve?

f. Conecte el cable Ethernet de la PC-A al puerto 6 en el switch y examine las propiedades IP de la VLAN 1 SVI. Aguarde un momento para que el switch y la computadora negocien los parámetros de dúplex y velocidad.

Nota: si utiliza Netlab, habilite la interfaz F0/6 en el S1.

```
Switch# show ip interface vlan1
```

¿Qué resultado ve?

g. Examine la información de la versión del IOS de Cisco del switch.

```
Switch# show version
```

¿Cuál es la versión del IOS de Cisco que está ejecutando el switch?

¿Cuál es el nombre del archivo de imagen del sistema?

¿Cuál es la dirección MAC base de este switch? Las respuestas varían.

h. Examine las propiedades predeterminadas de la interfaz FastEthernet que usa la PC-A.

```
Switch# show interface f0/6
```

¿La interfaz está activa o desactivada?

¿Qué haría que una interfaz se active?

¿Cuál es la dirección MAC de la interfaz?

¿Cuál es la configuración de velocidad y de dúplex de la interfaz?

i. Examine la configuración VLAN predeterminada del switch.

```
Switch# show vlan
```

¿Cuál es el nombre predeterminado de la VLAN 1?

¿Qué puertos hay en esta VLAN?

¿La VLAN 1 está activa?

¿Qué tipo de VLAN es la VLAN predeterminada?

j. Examine la memoria flash.

Ejecute uno de los siguientes comandos para examinar el contenido del directorio flash.

```
Switch# show flash
Switch# dir flash:
```

Los archivos poseen una extensión, tal como .bin, al final del nombre del archivo. Los directorios no tienen una extensión de archivo.

¿Cuál es el nombre de archivo de la imagen de IOS de Cisco?

Parte 2. configurar los parámetros básicos de los dispositivos de red

En la parte 2, configurará los parámetros básicos para el switch y la computadora.

Paso 1. configurar los parámetros básicos del switch, incluidos el nombre de host, las contraseñas locales, el mensaje MOTD, la dirección de administración y el acceso por Telnet.

En este paso, configurará la computadora y los parámetros básicos del switch, como el nombre de host y la dirección IP para la SVI de administración del switch. La asignación de una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administra el switch. Telnet y SSH son los dos métodos de administración que más se usan. No obstante, Telnet no es un protocolo seguro. 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 NVRAM, verifique que usted esté en el modo EXEC privilegiado. Introduzca el comando **enable** si la petición de entrada volvió a cambiar a Switch>.

```
Switch> enable
Switch#
```

b. Ingrese al modo de configuración global.

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

La petición de entrada volvió a cambiar para reflejar el modo de configuración global.

c. Asigne el nombre de host del switch.

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

d. Configurar la encriptación de contraseñas.

```
S1(config)# service password-encryption
S1(config)#
```

e. Asigne **class** como contraseña secreta para el acceso al modo EXEC privilegiado.

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

f. Evite las búsquedas de DNS no deseadas.

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

g. Configure un mensaje MOTD.

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

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

```
S1(config)# exit
S1#
```

```
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available



Press RETURN to get started.


Unauthorized access is strictly prohibited.
S1>
```

¿Qué teclas de método abreviado se usan para ir directamente del modo de configuración global al modo EXEC privilegiado?

i. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario. Introduzca la contraseña **class** cuando se le solicite hacerlo.

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

Nota: cuando se introduce la contraseña, esta no se muestra.

j. Ingrese al modo de configuración global para establecer la dirección IP de la SVI del switch. Esto permite la administración remota del switch.

Antes de poder administrar el S1 en forma remota desde la PC-A, debe asignar una dirección IP al switch. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica recomendada para la configuración básica del switch es cambiar la VLAN de administración a otra VLAN distinta de la VLAN 1.

Con fines de administración, utilice la VLAN 99. La selección de la VLAN 99 es arbitraria y de ninguna manera implica que siempre deba usar la VLAN 99.

Primero, cree la nueva VLAN 99 en el switch. Luego, establezca la dirección IP del switch en 192.168.1.2 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando **no shutdown**. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del switch a la VLAN 99.

k. Asigne todos los puertos de usuario a VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
```

```
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Para establecer la conectividad entre el host y el switch, los puertos que usa el host deben estar en la misma VLAN que el switch. Observe que, en el resultado de arriba, la interfaz VLAN 1 queda en estado down porque no se asignó ninguno de los puertos a la VLAN 1. Después de unos segundos, la VLAN 99 pasa al estado up porque ahora se le asigna al menos un puerto activo (F0/6 con la PC-A conectada).

l. Emita el comando **show vlan brief** para verificar que todos los puertos de usuario estén en la VLAN 99.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
99   VLAN0099                          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
                                                 Gi0/1, Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

m. Configure el gateway IP predeterminado para el S1. Si no se estableció ningún gateway predeterminado, no se puede administrar el switch desde una red remota que esté a más de un router de distancia. Sí responde a los pings de una red remota. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente conectará la LAN a un router para tener acceso externo. Suponiendo que la interfaz LAN en el router es 192.168.1.1, establezca el gateway predeterminado para el switch.

```
S1(config)# ip default-gateway 192.168.1.1
S1(config)#
```

n. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción **logging synchronous**.

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

o. Configure las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no puede acceder al switch mediante telnet.

```
S1(config)# line vty 0 15
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
```

¿Por qué se requiere el comando **login**?

Paso 2. configurar una dirección IP en la PC-A.

Asigne a la computadora la dirección IP y la máscara de subred que se muestran en la tabla de direccionamiento. Aquí se describe una versión abreviada del procedimiento. Para esta topología, no se requiere ningún gateway predeterminado; sin embargo, puede introducir **192.168.1.1** para simular un router conectado al S1.

1) Haga clic en el ícono **Inicio** de Windows > **Panel de control**.
2) Haga clic en **Ver por:** y elija **Íconos pequeños**.
3) Selecciones **Centro de redes y recursos compartidos** > **Cambiar configuración del adaptador**.
4) Seleccione **Conexión de área local**, haga clic con el botón secundario y elija **Propiedades**.
5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** > **Propiedades**.
6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca la dirección IP y la máscara de subred.

Parte 3. verificar y probar la conectividad de red

En la parte 3, 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 switch.

Desde la conexión de consola en la PC-A, muestre y verifique la configuración del switch. El comando **show run** muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

a. Aquí se muestra un ejemplo de configuración. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

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

Current configuration : 2206 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
!
<output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 104D000A0618
 logging synchronous
 login
line vty 0 4
 password 7 14141B180F0B
 login
line vty 5 15
 password 7 14141B180F0B
 login
!
end

S1#
```

b. Verifique la configuración de la VLAN 99 de administración.

```
S1# show interface vlan 99
Vlan99 is up, line protocol is up
```

```
Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
Internet address is 192.168.1.2/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 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 00:00:06, output 00:08:45, 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
   175 packets input, 22989 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
   1 packets output, 64 bytes, 0 underruns
   0 output errors, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

¿Cuál es el ancho de banda en esta interfaz?

¿Cuál es el estado de la VLAN 99?

¿Cuál es el estado del protocolo de línea?

Paso 2. probar la conectividad de extremo a extremo con ping.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de la propia PC-A primero.

```
C:\Users\User1> ping 192.168.1.10
```

b. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración de SVI del S1.

```
C:\Users\User1> ping 192.168.1.2
```

Debido a que la PC-A debe resolver la dirección MAC del S1 mediante ARP, es posible que se agote el tiempo de espera del primer paquete. Si los resultados del ping siguen siendo incorrectos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Revise el cableado físico y el direccionamiento lógico, si es necesario.

Paso 3. probar y verificar la administración remota del S1.

Ahora utilizará Telnet para acceder al switch en forma remota. 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 computadora de administración podría estar ubicada en la planta baja. En este paso, utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. Telnet no es un protocolo seguro; sin embargo, lo usará para probar el acceso remoto. Con Telnet, toda la información, incluidos los comandos y las contraseñas, se envía durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, usará SSH para acceder a los dispositivos de red en forma remota.

Nota: si utiliza Windows 7, es posible que el administrador deba habilitar el protocolo Telnet. Para instalar el cliente de Telnet, abra una ventana cmd y escriba **pkgmgr /iu:"TelnetClient"**. A continuación, se muestra un ejemplo.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

a. Con la ventana cmd 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\User1> telnet 192.168.1.2
```

b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC privilegiado.

c. Escriba **exit** para finalizar la sesión de Telnet.

Paso 4. guardar el archivo de configuración en ejecución del switch.

Guarde la configuración.

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

Parte 4. Administrar la tabla de direcciones MAC

En la parte 4, determinará la dirección MAC que detectó el switch, configurará una dirección MAC estática en una interfaz del switch y, a continuación, eliminará la dirección MAC estática de esa interfaz.

Paso 1. registrar la dirección MAC del host.

En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** para determinar y registrar las direcciones (físicas) de capa 2 de la NIC de la computadora.

Paso 2. Determine las direcciones MAC que el switch ha aprendido.

Muestre las direcciones MAC con el comando **show mac address-table**.

```
S1# show mac address-table
```

¿Cuántas direcciones dinámicas hay?

¿Cuántas direcciones MAC hay en total?

¿La dirección MAC dinámica coincide con la dirección MAC de la PC-A?

Paso 3. enumerar las opciones del comando show mac address-table.

a. Muestre las opciones de la tabla de direcciones MAC.

```
S1# show mac address-table ?
```

¿Cuántas opciones se encuentran disponibles para el comando **show mac address-table**?

b. Emita el comando **show mac address-table dynamic** para mostrar solo las direcciones MAC que se detectaron dinámicamente.

```
S1# show mac address-table dynamic
```

¿Cuántas direcciones dinámicas hay?

c. Vea la entrada de la dirección MAC para la PC-A. El formato de dirección MAC para el comando es xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Paso 4. Configure una dirección MAC estática.

a. limpie la tabla de direcciones MAC.

Para eliminar las direcciones MAC existentes, use el comando **clear mac address-table** del modo EXEC privilegiado.

```
S1# clear mac address-table dynamic
```

b. Verifique que la tabla de direcciones MAC se haya eliminado.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC estáticas hay?

¿Cuántas direcciones dinámicas hay?

c. Examine nuevamente la tabla de direcciones MAC

Es muy probable que una aplicación en ejecución en la computadora ya haya enviado una trama por la NIC hacia el S1. Observe nuevamente la tabla de direcciones MAC en el modo EXEC privilegiado para ver si el S1 volvió a detectar la dirección MAC para la PC-A.

```
S1# show mac address-table
```

¿Cuántas direcciones dinámicas hay?

¿Por qué cambió esto desde la última visualización?

Si el S1 aún no volvió a detectar la dirección MAC de la PC-A, haga ping a la dirección IP de la VLAN 99 del switch desde la PC-A y, a continuación, repita el comando **show mac address-table**.

d. Configure una dirección MAC estática.

Para especificar a qué puertos se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto.

Configure una dirección MAC estática en F0/6 con la dirección que se registró para la PC-A en la parte 4, paso 1. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe usar la dirección MAC de su PC-A, que es distinta de la del ejemplo.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

e. Verifique las entradas de la tabla de direcciones MAC.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC hay en total?

¿Cuántas direcciones estáticas hay?

f. Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

Nota: la dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

g. Verifique que la dirección MAC estática se haya borrado.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC estáticas hay en total?

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch?

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado?

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?

Apéndice A: inicialización y recarga de un router y un switch

Paso 1. inicializar y volver a cargar el router.

a. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

```
Router> enable
Router#
```

b. Introduzca el comando **erase startup-config** para eliminar la configuración de inicio de la NVRAM.

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

c. Emita el comando **reload** para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje Proceed with reload?, presione Enter. (Si presiona cualquier otra tecla, se cancela 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 una petición de entrada para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Enter.

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

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

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

e. Aparece otra petición de entrada para finalizar la instalación automática. Responda escribiendo **yes** (sí) y presione Enter.

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

Paso 2. inicializar y volver a cargar el switch.

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

```
Switch> enable
Switch#
```

b. 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#
```

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

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

d. Se le solicitará que verifique el nombre de archivo. Si introdujo el nombre correctamente, presione Enter; de lo contrario, puede cambiar el nombre de archivo.

e. Se le solicita que confirme la eliminación de este archivo. Presione Intro para confirmar.

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

f. Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicita que elimine el archivo de configuración. Presione Intro para confirmar.

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

g. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Luego, recibirá una petición de entrada para confirmar la recarga del switch. Presione Enter para continuar.

```
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. Responda escribiendo **no** y presione Enter.

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

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

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

2. Configuración de seguridad de puertos de

Topología

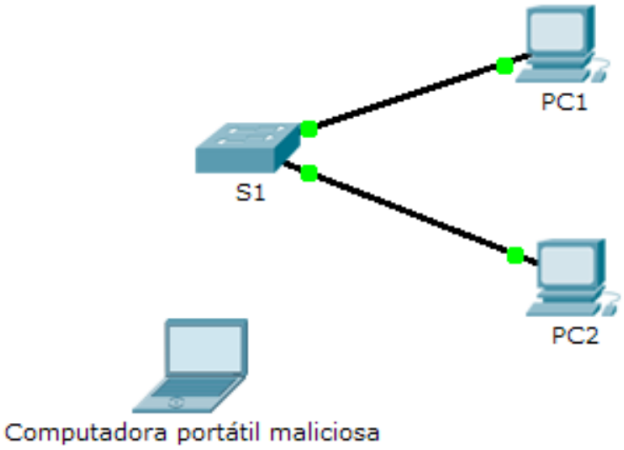


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Computadora portátil maliciosa	NIC	10.10.10.12	255.255.255.0

Objetivo

Parte 1: configurar la seguridad de puertos

Parte 2: verificar la seguridad de puertos

Información básica

En esta actividad, configurará y verificará la seguridad de puertos de un switch. La seguridad de puertos permite restringir el tráfico de entrada de un puerto mediante la limitación de las direcciones MAC que tienen permitido enviar tráfico al puerto.

Parte 1: Configurar la seguridad del puerto

a. Acceda a la línea de comandos del **S1** y habilite la seguridad de puertos en Fast Ethernet 0/1 y 0/2.

b. Establezca la seguridad máxima, de modo que solo un dispositivo pueda acceder a los puertos Fast Ethernet 0/1 y 0/2.

c. Proteja los puertos de modo que la dirección MAC de un dispositivo se detecte de forma dinámica y se agregue a la configuración en ejecución.

d. Establezca la infracción de manera que no se deshabiliten los puertos Fast Ethernet 0/1 y 0/2 cuando se produzca una infracción, sino que se descarten los paquetes de origen desconocido.

e. Deshabilite todos los demás puertos sin utilizar. Sugerencia: utilice la palabra clave **range** para aplicar esta configuración a todos los puertos de forma simultánea.

Parte 2: Verificar la seguridad de puerto

a. En la **PC1**, haga ping a la **PC2**.

b. Verifique que la seguridad de puertos esté habilitada y que las direcciones MAC de la **PC1** y la **PC2** se hayan agregado a la configuración en ejecución.

c. Conecte la **Computadora portátil maliciosa** a cualquier puerto de switch no utilizado y observe que las luces de enlace estén rojas.

d. Habilite el puerto y verifique que la **Computadora portátil maliciosa** pueda hacer ping a la **PC1** y la **PC2**. Después de la verificación, desactive el puerto conectado a la **Computadora portátil maliciosa.**

e. Desconecte la **PC2** y conecte la **Computadora portátil maliciosa** al puerto de la **PC2**. Verifique que la **Computadora portátil maliciosa** no pueda hacer ping a la **PC1**.

f. Muestre las infracciones de seguridad de puertos correspondientes al puerto al que está conectada la **Computadora portátil maliciosa**.

g. Desconecte la **Computadora portátil maliciosa** y vuelva a conectar la **PC2**. Verifique que la **PC2** pueda hacer ping a la **PC1**.

h. ¿Por qué la **PC2** puede hacer ping a la **PC1**, pero la **Computadora portátil maliciosa** no puede?

3. Configuración de redes VLAN y enlaces troncales

Topología

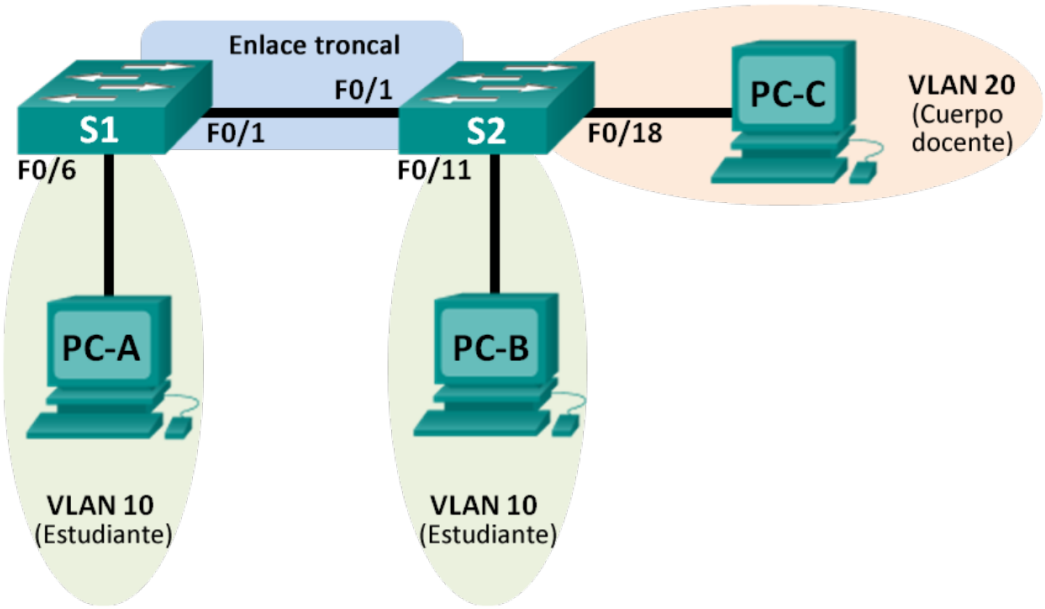


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: crear redes VLAN y asignar puertos de switch

Parte 3: mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

Parte 4: configurar un enlace troncal 802.1Q entre los switches

Parte 5: eliminar la base de datos de VLAN

Información básica/situación

Los switches modernos usan redes de área local virtuales (VLAN) para mejorar el rendimiento de la red mediante la división de grandes dominios de difusión de capa 2 en otros más pequeños. Las VLAN también se pueden usar como medida de seguridad al controlar qué hosts se pueden comunicar. Por lo general, las redes VLAN facilitan el diseño de una red para respaldar los objetivos de una organización.

Los enlaces troncales de VLAN se usan para abarcar redes VLAN a través de varios dispositivos. Los enlaces troncales permiten transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN.

En esta práctica de laboratorio, creará redes VLAN en los dos switches de la topología, asignará las VLAN a los puertos de acceso de los switches, verificará que las VLAN funcionen como se espera y, a continuación, creará un enlace troncal de VLAN entre los dos switches para permitir que los hosts en la misma VLAN se comuniquen a través del enlace troncal, independientemente del switch al que está conectado el host.

Nota: los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros 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.

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

Recursos necesarios

- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (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. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

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

Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2. inicializar y volver a cargar los switches según sea necesario.

Paso 3. configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Asigne **class** como la contraseña del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

e. Configure **logging synchronous** para la línea de consola.

f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

g. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

h. Desactive administrativamente todos los puertos que no se usen en el switch.

i. Copie la configuración en ejecución en la configuración de inicio

Paso 4. configurar los equipos host.

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

Paso 5. Probar la conectividad.

Verifique que los equipos host puedan hacer ping entre sí.

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

¿Se puede hacer ping de la PC-A a la PC-B?

¿Se puede hacer ping de la PC-A a la PC-C?

¿Se puede hacer ping de la PC-A al S1?

¿Se puede hacer ping de la PC-B a la PC-C?

¿Se puede hacer ping de la PC-B al S2?

¿Se puede hacer ping de la PC-C al S2?

¿Se puede hacer ping del S1 al S2?

Si la respuesta a cualquiera de las preguntas anteriores es no, ¿por qué fallaron los pings?

Parte 2. crear redes VLAN y asignar puertos de switch

En la parte 2, creará redes VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

Paso 1. crear las VLAN en los switches.

a. Cree las VLAN en S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

b. Cree las mismas VLAN en el S2.

c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.

```
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
                                                 Gi0/1, Gi0/2
10   Student                           active
20   Faculty                           active
99   Management                        active
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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
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
------- --------- ----------------- ------------------------------------------
```

¿Cuál es la VLAN predeterminada?

¿Qué puertos se asignan a la VLAN predeterminada?

Paso 2. asignar las VLAN a las interfaces del switch correctas.

a. Asigne las VLAN a las interfaces en el S1.

1) Asigne la PC-A a la VLAN Estudiantes.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

2) Transfiera la dirección IP del switch a la VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

b. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, 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, Gi0/1
                                                 Gi0/2
10   Student                           active    Fa0/6
20   Faculty                           active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

c. Emita el comando **show ip interface brief**.

¿Cuál es el estado de la VLAN 99? ¿Por qué?

d. Use la topología para asignar las VLAN a los puertos correspondientes en el S2.

e. Elimine la dirección IP para la VLAN 1 en el S2.

f. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.

g. Use el comando **show vlan brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.

```
S2# show vlan brief

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, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Student                           active    Fa0/11
```

```
20   Faculty                          active    Fa0/18
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

¿Es posible hacer ping de la PC-A a la PC-B? ¿Por qué?

¿Es posible hacer ping del S1 al S2? ¿Por qué?

Parte 3. mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

En la parte 3, cambiará las asignaciones de VLAN a los puertos y eliminará las VLAN de la base de datos de VLAN.

Paso 1. asignar una VLAN a varias interfaces.

a. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.

c. Reasigne F0/11 y F0/21 a la VLAN 20.

d. Verifique que las asignaciones de VLAN sean las correctas.

Paso 2. eliminar una asignación de VLAN de una interfaz.

a. Use el comando **no switchport access vlan** para eliminar la asignación de la VLAN 10 a F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Verifique que se haya realizado el cambio de VLAN.

¿A qué VLAN está asociada ahora F0/24?

Paso 3. eliminar una ID de VLAN de la base de datos de VLAN.

a. Agregue la VLAN 30 a la interfaz F0/24 sin emitir el comando VLAN.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Nota: la tecnología de switches actual ya no requiere la emisión del comando **vlan** para agregar una VLAN a la base de datos. Al asignar una VLAN desconocida a un puerto, la VLAN se agrega a la base de datos de VLAN.

b. Verifique que la nueva VLAN se muestre en la tabla de VLAN.

```
S1# show vlan brief

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, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
30   VLAN0030                          active    Fa0/24
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

¿Cuál es el nombre predeterminado de la VLAN 30?

c. Use el comando **no vlan 30** para eliminar la VLAN 30 de la base de datos de VLAN.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Emita el comando **show vlan brief**. F0/24 se asignó a la VLAN 30.

Una vez que se elimina la VLAN 30, ¿a qué VLAN se asigna el puerto F0/24? ¿Qué sucede con el tráfico destinado al host conectado a F0/24?

```
S1# show vlan brief

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, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

e. Emita el comando **no switchport access vlan** en la interfaz F0/24.

f. Emita el comando **show vlan brief** para determinar la asignación de VLAN para F0/24. ¿A qué VLAN se asignó F0/24?

Nota: antes de eliminar una VLAN de la base de datos, se recomienda reasignar todos los puertos asignados a esa VLAN.

¿Por qué debe reasignar un puerto a otra VLAN antes de eliminar la VLAN de la base de datos de VLAN?

Parte 4. configurar un enlace troncal 802.1Q entre los switches

En la parte 4, configurará la interfaz F0/1 para que use el protocolo de enlace troncal dinámico (DTP) y permitir que negocie el modo de enlace troncal. Después de lograr y verificar esto, desactivará DTP en la interfaz F0/1 y la configurará manualmente como enlace troncal.

Paso 1. usar DTP para iniciar el enlace troncal en F0/1.

El modo de DTP predeterminado de un puerto en un switch 2960 es dinámico automático. Esto permite que la interfaz convierta el enlace en un enlace troncal si la interfaz vecina se establece en modo de enlace troncal o dinámico deseado.

a. Establezca F0/1 en el S1 en modo de enlace troncal.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar  1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar  1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

También debe recibir mensajes del estado del enlace en el S2.

```
S2#
*Mar  1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar  1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
*Mar  1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

b. Emita el comando **show vlan brief** en el S1 y el S2. La interfaz F0/1 ya no está asignada a la VLAN 1. Las interfaces de enlace troncal no se incluyen en la tabla de VLAN.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/24, Gi0/1, Gi0/2
10   Student                           active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

c. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99

S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Nota: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

d. Verifique que el tráfico de VLAN se transfiera a través de la interfaz de enlace troncal F0/1.

¿Se puede hacer ping del S1 al S2?

¿Se puede hacer ping de la PC-A a la PC-B?

¿Se puede hacer ping de la PC-A a la PC-C?

¿Se puede hacer ping de la PC-B a la PC-C?

¿Se puede hacer ping de la PC-A al S1?

¿Se puede hacer ping de la PC-B al S2?

¿Se puede hacer ping de la PC-C al S2?

Si la respuesta a cualquiera de las preguntas anteriores es no, justifíquela a continuación.

Paso 2. configurar manualmente la interfaz de enlace troncal F0/1.

El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

a. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switches.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Emita el comando **show interfaces trunk** para ver el modo de enlace troncal. Observe que el modo cambió de **desirable** a **on**.

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

¿Por qué desearía configurar una interfaz en modo de enlace troncal de forma manual en lugar de usar DTP?

Parte 5. Eliminar la base de datos de VLAN

En la parte 5, eliminará la base de datos de VLAN del switch. Es necesario hacer esto al inicializar un switch para que vuelva a la configuración predeterminada.

Paso 1. determinar si existe la base de datos de VLAN.

Emita el comando **show flash** para determinar si existe el archivo **vlan.dat** en la memoria flash.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

Nota: si hay un archivo **vlan.dat** en la memoria flash, la base de datos de VLAN no contiene la configuración predeterminada.

Paso 2. eliminar la base de datos de VLAN.

a. Emita el comando **delete vlan.dat** para eliminar el archivo vlan.dat de la memoria flash y restablecer la base de datos de VLAN a la configuración predeterminada. Se le solicitará dos veces que confirme que desea eliminar el archivo vlan.dat. Presione Enter ambas veces.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

b. Emita el comando **show flash** para verificar que se haya eliminado el archivo vlan.dat.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)
```

Para inicializar un switch para que vuelva a la configuración predeterminada, ¿cuáles son los otros comandos que se necesitan?

Reflexión

1. ¿Qué se necesita para permitir que los hosts en la VLAN 10 se comuniquen con los hosts en la VLAN 20?

2. ¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?

4. Implementación de seguridad de VLAN

Topología

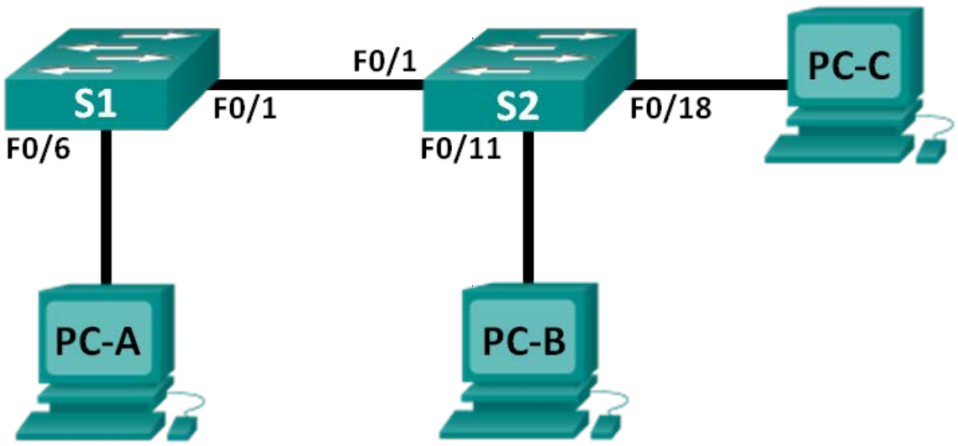


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: implementar seguridad de VLAN en los switches

Información básica/situación

La práctica recomendada indica que se deben configurar algunos parámetros básicos de seguridad para los puertos de enlace troncal y de acceso en los switches. Esto sirve como protección contra los ataques de VLAN y la posible detección del tráfico de la red dentro de esta.

En esta práctica de laboratorio, configurará los dispositivos de red en la topología con algunos parámetros básicos, verificará la conectividad y, a continuación, aplicará medidas de seguridad más estrictas en los switches. Utilizará varios comandos **show** para analizar la forma en que se comportan los switches Cisco. Luego, aplicará medidas de seguridad.

Nota: los switches que se utilizan en esta práctica de laboratorio son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros 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.

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

Recursos necesarios

- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (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. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, configurará los parámetros básicos en los switches y las computadoras. Consulte la tabla de direccionamiento para obtener información sobre nombres de dispositivos y direcciones.

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

Paso 2. inicializar y volver a cargar los switches.

Paso 3. configurar las direcciones IP en la PC-A, la PC-B y la PC-C.

Consulte la tabla de direccionamiento para obtener la información de direcciones de las computadoras.

Paso 4. configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

c. Asigne **class** como la contraseña del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de VTY y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

e. Configure el inicio de sesión sincrónico para las líneas de vty y de consola.

Paso 5. configurar las VLAN en cada switch.

a. Cree las VLAN y asígneles nombres según la tabla de asignaciones de VLAN.

b. Configure la dirección IP que se indica para la VLAN 99 en la tabla de direccionamiento en ambos switches.

c. Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.

d. Configure F0/11 en el S2 como puerto de acceso y asígnelo a la VLAN 10.

e. Configure F0/18 en el S2 como puerto de acceso y asígnelo a la VLAN 99.

f. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN y de puertos.

¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2?

Paso 6. configurar la seguridad básica del switch.

a. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

b. Encripte todas las contraseñas.

c. Desactive todos los puertos físicos sin utilizar.

d. Deshabilite el servicio web básico en ejecución.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Copie la configuración en ejecución en la configuración de inicio.

Paso 7. verificar la conectividad entre la información de VLAN y los dispositivos.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

b. Desde el S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?

d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2. ¿Tuvo éxito? ¿Por qué?

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

Parte 2. implementar seguridad de VLAN en los switches

Paso 1. configurar puertos de enlace troncal en el S1 y el S2.

a. Configure el puerto F0/1 en el S1 como puerto de enlace troncal.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Configure el puerto F0/1 en el S2 como puerto de enlace troncal.

```
S2(config)# interface f0/1
```

```
S2(config-if)# switchport mode trunk
```

c. Verifique los enlaces troncales en el S1 y el S2. Emita el comando **show interface trunk** en los dos switches.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Paso 2. cambiar la VLAN nativa para los puertos de enlace troncal en el S1 y el S2.

Es aconsejable para la seguridad cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.

a. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?

b. Configure la VLAN nativa de la interfaz de enlace troncal F0/1 del S1 en la VLAN 99 Management&Native.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Espere unos segundos. Debería comenzar a recibir mensajes de error en la sesión de consola del S1. ¿Qué significa el mensaje %CDP-4-NATIVE_VLAN_MISMATCH:?

d. Configure la VLAN 99 como VLAN nativa de la interfaz de enlace troncal F0/1 del S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Verifique que ahora la VLAN nativa sea la 99 en ambos switches. A continuación, se muestra el resultado del S1.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Paso 3. verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

b. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?

d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A. ¿Tuvo éxito? ¿Por qué?

Paso 4. impedir el uso de DTP en el S1 y el S2.

Cisco utiliza un protocolo exclusivo conocido como "protocolo de enlace troncal dinámico" (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del siguiente comando:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

a. Desactive la negociación en el S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Desactive la negociación en el S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Verifique que la negociación esté desactivada mediante la emisión del comando **show interface f0/1 switchport** en el S1 y el S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
```

```
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Paso 5. implementar medidas de seguridad en los puertos de acceso del S1 y el S2.

Aunque desactivó los puertos sin utilizar en los switches, si se conecta un dispositivo a uno de esos puertos y la interfaz está habilitada, se podría producir un enlace troncal. Además, todos los puertos están en la VLAN 1 de manera predeterminada. Se recomienda colocar todos los puertos sin utilizar en una VLAN de "agujero negro". En este paso, deshabilitará los enlaces troncales en todos los puertos sin utilizar. También asignará los puertos sin utilizar a la VLAN 999. A los fines de esta práctica de laboratorio, solo se configurarán los puertos 2 a 5 en ambos switches.

a. Emita el comando **show interface f0/2 switchport** en el S1. Observe el modo administrativo y el estado para la negociación de enlaces troncales.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Deshabilite los enlaces troncales en los puertos de acceso del S1.

```
S1(config)# interface range f0/2 - 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Deshabilite los enlaces troncales en los puertos de acceso del S2.

d. Verifique que el puerto F0/2 esté establecido en modo de acceso en el S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

e. Verifique que las asignaciones de puertos de VLAN en ambos switches sean las correctas. A continuación, se muestra el S1 como ejemplo.

```
S1# show vlan brief
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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, Gi0/1, Gi0/2
10   Data                              active
99   Management&Native                 active    Fa0/6
999  BlackHole                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
Restrict VLANs allowed on trunk ports.
```

De manera predeterminada, se permite transportar todas las VLAN en los puertos de enlace troncal. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.

f. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10 y 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10 y 99.

h. Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo EXEC privilegiado en el S1 y el S2

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

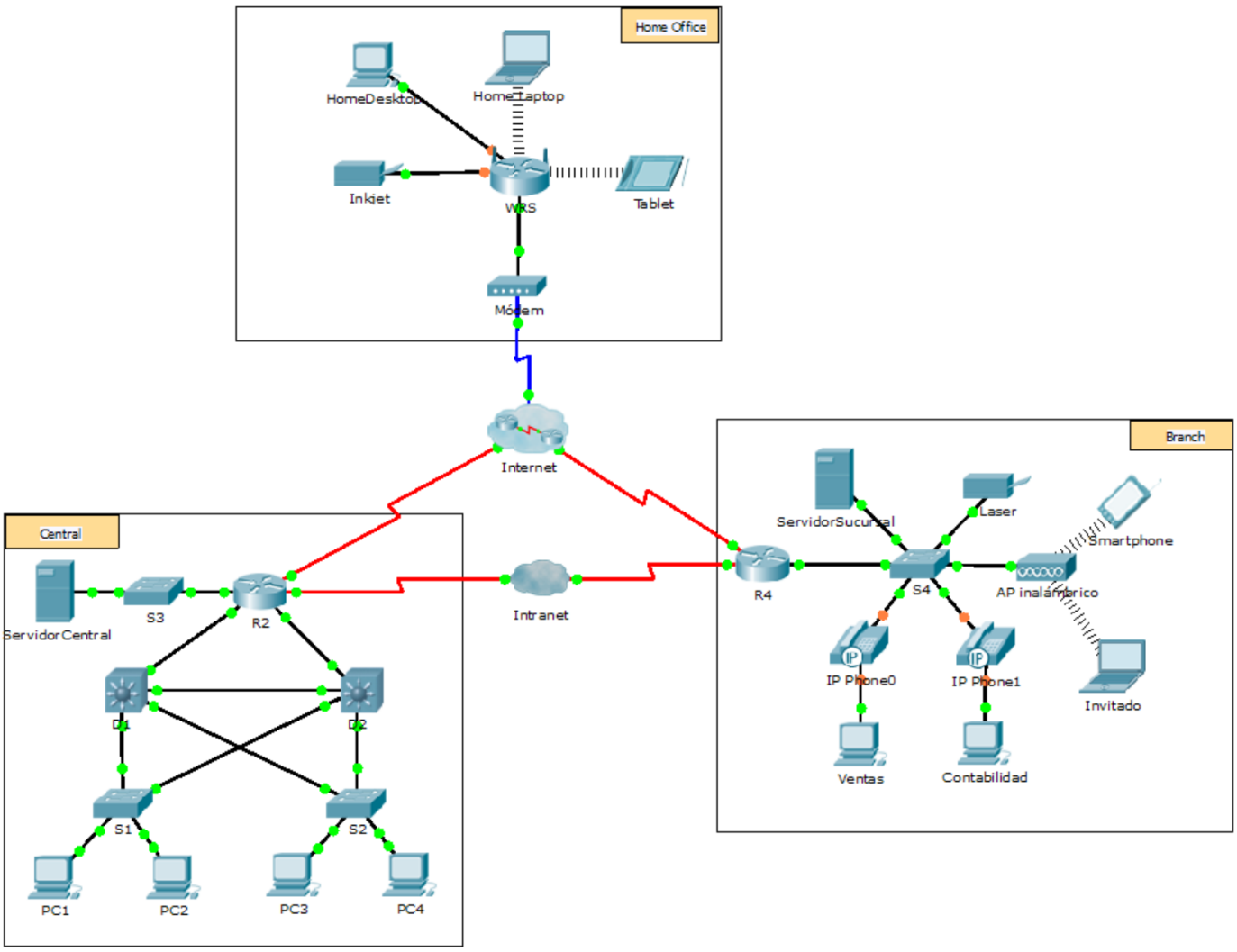
¿Cuál es el resultado?

Reflexión

¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco?

5. Utilización de traceroute para detectar la red

Topología



Situación

La empresa para la que trabaja adquirió una nueva sucursal. Usted solicitó un mapa de la topología de la nueva ubicación, pero parece que no existe. Sin embargo, tiene información de nombres de usuario y contraseñas de los dispositivos de red de la nueva sucursal y conoce la dirección web del servidor de esta. Por lo tanto, verificará la conectividad y usará el comando **tracert** para determinar la ruta a la ubicación. Se conectará al router perimetral de la nueva ubicación para determinar los dispositivos y las redes que están conectados. Como parte de este proceso, utilizará distintos comandos show para recopilar la información necesaria para terminar de registrar el esquema de direccionamiento IP y crear un diagrama de la topología.

Nota: la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

Rastreo y registro de una ubicación remota

Nota: a medida que complete los siguientes pasos, copie el resultado del comando en un archivo de texto para facilitar la consulta y registre la información que falta en la tabla de **registro del esquema de direccionamiento**.

Consulte la página de **Sugerencias** para repasar los comandos utilizados. En Packet Tracer, haga clic en la flecha derecha (>) que se encuentra en el sector inferior derecho de la ventana de instrucciones. Si tiene una versión impresa de las instrucciones, la página de **Sugerencias** es la última.

a. Haga clic en **Sales** (Ventas) y en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema). Use el comando **ipconfig** para revisar la configuración de la dirección IP de **Sales**.

b. La dirección del nuevo servidor web es **b2server.pt.pka.** Introduzca el siguiente comando **nslookup** para descubrir la dirección IP de **b2server**:

```
PC> nslookup b2server.pt.pka
```

¿Qué dirección devolvió el comando para **b2server**?

c. Introduzca el comando **tracert** para determinar la ruta desde **Sales** hasta **b2server.pt.pka**.

```
PC> tracert b2server.pt.pka
```

d. Acceda a la primera dirección IP del resultado de **tracert** mediante Telnet e inicie sesión.

```
PC> telnet 172.16.0.1
```

e. Ya está conectado al router **R4**. Emita el comando **traceroute** en el router con la dirección de b2server determinada en el punto b. ¿Qué diferencia hay entre el comando **traceroute** en el router y el comando **tracert** en la computadora?

¿Cuál es la importancia del **R4** para **Sales**?

f. Use el comando **show ip interface brief** para mostrar el estado de las interfaces en el **R4**. Según el resultado del comando, ¿qué interfaz se utiliza para llegar al siguiente dispositivo en la lista de resultados del comando **tracert**?

Sugerencia: utilice el comando **show running-config** para ver los valores de máscara de subred de las interfaces.

g. Acceda a la segunda dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. Puede utilizar el número en la columna del extremo izquierdo del resultado del comando **tracert** para seguir su recorrido por la lista. ¿Cuál es el nombre del dispositivo al que está conectado?

h. Emita el comando **show ip route** y analice el resultado. Según la lista de códigos que se muestra al comienzo del resultado, ¿cuáles son los diferentes tipos de rutas que se muestran en la tabla de routing?

i. Según el resultado del comando **show ip route**, ¿cuál es la interfaz de salida de la siguiente dirección IP que se indica en el resultado original del comando **tracert**?

j. Acceda a la tercera dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. ¿Cuál es el nombre de host del dispositivo actual?

Emita el comando **show ip route connected**. ¿Cuáles son las redes conectadas directamente a este router?

Consulte la tabla de **registro del esquema de direccionamiento**. ¿Qué interfaces conectan los dispositivos entre trace route 2 y trace route 3?

k. Acceda a la cuarta dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. ¿Cuál es el nombre del dispositivo?

l. Emita un comando para determinar a qué interfaz está conectado **b2server.pt.pka**.

m. Si utilizó la tabla de **registro del esquema de direccionamiento** a medida que completó los pasos anteriores, la tabla debería estar completa. De lo contrario, termine la tabla.

n. Con un registro completo del esquema de direccionamiento y con el conocimiento de la ruta desde **Sales** hasta **branch2.pt.pka**, debería estar en condiciones de delinear la ubicación de la nueva sucursal en el espacio correspondiente al **registro de la topología** que aparece más abajo.

Registro del esquema de direccionamiento

ID de trace route	Dispositivo	Interfaz	Dirección	Máscara de subred
-	Ventas	NIC	172.16.0.x (DHCP)	255.255.255.0
1				
		S0/0/1.1	64.100.200.1	255.255.255.252
2				
		G0/1	64.104.223.1	255.255.255.252
		S0/0/0	64.100.100.2	
3				
		G0/2		255.255.255.0
		F0/1	128.107.46.1	
4		G0/0		
5	b2server.pt.pka	NIC	128.107.64.254	255.255.255.0

Registro de la topología

Utilice el espacio a continuación para delinear la topología de la ubicación de la nueva sucursal.

Tabla de calificación sugerida

Sección de la actividad	Puntos posibles	Puntos obtenidos
Preguntas (2 puntos cada una)	20	
Registro del esquema de direccionamiento	60	
Registro de la topología	20	
Puntos totales	**100**	

Sugerencias: referencia resumida de comandos

Comandos de DOS

ipconfig: el resultado del comando predeterminado contiene la dirección IP, la máscara de red y el gateway para todos los adaptadores de red virtuales y físicos.

ipconfig /all: con esta opción, se muestra la misma información de direccionamiento IP para cada adaptador como opción predeterminada. Además, se muestran las configuraciones de DNS y WINS para cada adaptador.

Nslookup: se muestra la información que puede utilizar para diagnosticar la infraestructura del sistema de nombres de dominios (DNS).

Sintaxis:

nslookup dns.name

Tracert: determina la ruta elegida hacia un destino mediante el envío de mensajes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al destino con valores cada vez mayores en el campo de tiempo de vida (TTL). La ruta que se muestra consiste en la lista de interfaces de router cercanas de los routers que están en la ruta entre un host de origen y un destino. La interfaz cercana es la interfaz del router que está más cerca del host emisor en la ruta. Si se utiliza sin parámetros, tracert muestra la ayuda.

Sintaxis:

tracert [NombreDestino/Dirección IP]

Comandos del IOS

show ip interface: el resultado de este comando muestra el estado y la configuración de la interfaz IP.

show IP interface brief: el resultado de este comando muestra un breve resumen del estado y la configuración de IP.

show ip route: el resultado de este comando muestra la tabla de routing IP completa.

show ip route connected: el resultado de este comando muestra una lista de redes activas conectadas directamente.

show running-config: el resultado de este comando muestra la configuración operativa actual.

traceroute: rastrea la ruta al destino.

6. Configuración de routing entre VLAN con router on-a-stick

Topología

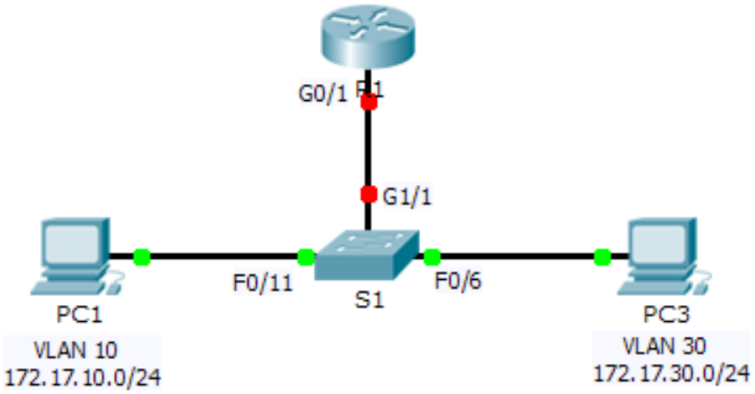


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Objetivos

Parte 1: probar la conectividad sin routing entre VLAN

Parte 2: agregar VLAN a un switch

Parte 3: configurar subinterfaces

Parte 4: probar la conectividad con routing entre VLAN

Situación

En esta actividad, verificará la conectividad antes de implementar el routing entre VLAN. Luego, configurará las VLAN y el routing entre VLAN. Por último, habilitará el enlace troncal y verificará la conectividad entre las VLAN.

Parte 1: Probar conectividad sin routing entre VLAN

Paso 1: hacer ping entre la PC1 y la PC3.

Espere a que converjan los switches o haga clic en **Fast Forward Time** (Adelantar el tiempo) varias veces. Cuando las luces de enlace para la **PC1** y la **PC3** estén de color verde, haga ping entre la **PC1** y la **PC3**. Como las dos computadoras están en redes separadas y el **R1** no está configurado, el ping falla.

Paso 2: pasar al modo de simulación para controlar los pings.

a. Para pasar al modo Simulation (Simulación), haga clic en la ficha **Simulation** o presione **Mayús+S**.

b. Haga clic en **Capture/Forward** (Capturar/Adelantar) para ver los pasos que sigue el ping entre la **PC1** y la **PC3**. Observe que el ping nunca deja la **PC1**. ¿Qué proceso falló y por qué?

Parte 2: agregar VLAN a un switch

Paso 1: crear VLAN en el S1.

Vuelva al modo **Realtime** (Tiempo real) y cree la VLAN 10 y la VLAN 30 en el **S1**.

Paso 2: Asignar VLAN a puertos.

a. Configure las interfaces F0/6 y F0/11 como puertos de acceso y asigne las VLAN.

- Asigne la **PC1** a la VLAN 10.
- Asigne la **PC3** a la VLAN 30.

b. Emita el comando **show vlan brief** para verificar la configuración de VLAN.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, 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
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Paso 3: probar la conectividad entre la PC1 y la PC3.

En la **PC1**, haga ping a la **PC3**. Los pings deberían seguir fallando. ¿Por qué fallaron los pings?

Parte 3: configurar subinterfaces

Paso 1: configurar las subinterfaces en el R1 con la encapsulación 802.1Q.

a. Cree la subinterfaz G0/0.10.

- Establezca el tipo de encapsulación en 802.1Q y asigne la VLAN 10 a la subinterfaz.
- Consulte la **tabla de direccionamiento** y asigne la dirección IP correcta a la subinterfaz.

b. Repita el proceso para la subinterfaz G0/0.30.

Paso 2: verificar la configuración.

a. Utilice el comando **show ip interface brief** para verificar la configuración de las subinterfaces. Ambas subinterfaces están inactivas. Las subinterfaces son interfaces virtuales que se asocian a una interfaz física. Por lo tanto, para habilitar las subinterfaces, debe habilitar la interfaz física a la que se asocian.

b. Habilite la interfaz G0/0. Verifique que las subinterfaces ahora estén activas.

Parte 4: probar la conectividad con routing entre VLAN

Paso 1: hacer ping entre la PC1 y la PC3.

En la **PC1**, haga ping a la **PC3**. Los pings deberían seguir fallando.

Paso 2: habilitar el enlace troncal.

a. En el **S1**, emita el comando **show vlan**. ¿A qué VLAN se asignó la interfaz G1/1?

b. Como el router se configuró con varias subinterfaces asignadas a diferentes VLAN, el puerto de switch que se conecta al router se debe configurar como enlace troncal. Habilite el enlace troncal en la interfaz G1/1.

a. ¿Cómo puede determinar que la interfaz es un puerto de enlace troncal mediante el comando **show vlan**?

b. Emita el comando **show interface trunk** para verificar que la interfaz se haya configurado como enlace troncal.

Paso 3: pasar al modo de simulación para controlar los pings.

a. Para pasar al modo **Simulation** (Simulación), haga clic en la ficha **Simulation** o presione **Mayús+S**.

b. Haga clic en **Capture/Forward** (Capturar/Adelantar) para ver los pasos que sigue el ping entre la **PC1** y la **PC3**.

c. Debería ver solicitudes y respuestas de ARP entre el **S1** y el **R1**. Luego, solicitudes y respuestas de ARP entre el **R1** y el **S3**. De esta manera, la **PC1** puede encapsular una solicitud de eco ICMP con la información de capa de enlace de datos correspondiente, y el R1 enruta la solicitud a la **PC3**.

Nota: una vez finalizado el proceso ARP, es posible que deba hacer clic en Reset Simulation (Restablecer simulación) para ver el proceso ICMP completo.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 60 puntos. Las cuatro preguntas valen 10 puntos cada una.

7. Configuración de rutas estáticas y predeterminadas IPv4

Topología

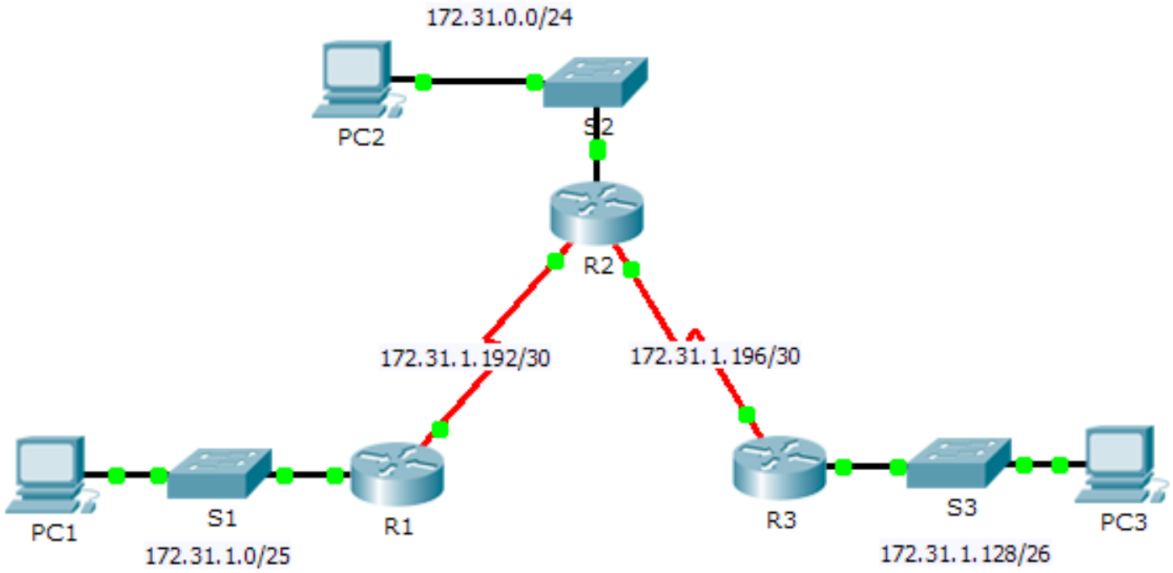


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.1.1	255.255.255.128	N/A
	S0/0/0	172.31.1.194	255.255.255.252	N/A
R2	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	172.31.1.193	255.255.255.252	N/A
	S0/0/1	172.31.1.197	255.255.255.252	N/A
R3	G0/0	172.31.1.129	255.255.255.192	N/A
	S0/0/1	172.31.1.198	255.255.255.252	N/A
PC1	NIC	172.31.1.126	255.255.255.128	172.31.1.1
PC2	NIC	172.31.0.254	255.255.255.0	172.31.0.1
PC3	NIC	172.31.1.190	255.255.255.192	172.31.1.129

Objetivos

Parte 1: examinar la red y evaluar la necesidad de routing estático

Parte 2: configurar rutas estáticas y predeterminadas

Parte 3: verificar la conectividad

Información básica

En esta actividad, configurará rutas estáticas y predeterminadas. Una ruta estática es una ruta que el administrador de red introduce manualmente para crear una ruta confiable y segura. En esta actividad, se utilizan cuatro rutas estáticas diferentes: una ruta estática recursiva, una ruta estática conectada directamente, una ruta estática completamente especificada y una ruta predeterminada.

Parte 1: examinar la red y evaluar la necesidad de routing estático

a. Observe el diagrama de la topología. ¿Cuántas redes hay en total?

b. ¿Cuántas redes están conectadas directamente al R1, al R2 y al R3?

c. ¿Cuántas rutas estáticas requiere cada router para llegar a las redes que no están conectadas directamente?

d. Pruebe la conectividad a las LAN del R2 y el R3 haciendo ping de la PC1 a la PC2 y la PC3.

¿Por qué no logró hacerlo?

Parte 2: configurar rutas estáticas y predeterminadas

Paso 1: configurar rutas estáticas recursivas en el R1.

a. ¿Qué es una ruta estática recursiva?

b. ¿Por qué una ruta estática recursiva requiere dos búsquedas en la tabla de routing?

c. Configure una ruta estática recursiva a cada red que no esté conectada directamente al R1, incluidos los enlaces WAN entre el R2 y el R3.

d. Pruebe la conectividad a la LAN del R2 y haga ping a las direcciones IP de la PC2 y la PC3.

¿Por qué no logró hacerlo?

Paso 2: configurar rutas estáticas conectadas directamente en el R2.

a. ¿En qué se diferencia una ruta estática conectada directamente de una ruta estática recursiva?

b. Configure una ruta estática conectada directamente del R2 a cada red que no esté conectada directamente.

c. ¿Con qué comando se muestran solo las redes conectadas directamente?

d. ¿Con qué comando se muestran solo las rutas estáticas que se indican en la tabla de routing?

e. Al ver la tabla de routing completa, ¿cómo se puede distinguir entre una ruta estática conectada directamente y una red conectada directamente?

Paso 3: configurar una ruta predeterminada en el R3.

a. ¿En qué se diferencia una ruta predeterminada de una ruta estática común?

b. Configure una ruta predeterminada en el R3 de modo que se pueda llegar a cada red que no esté conectada directamente.

c. ¿Cómo se muestra una ruta estática en la tabla de routing?

Paso 4: Registre los comandos para las rutas completamente especificadas.

Nota: actualmente, Packet Tracer no admite la configuración de las rutas estáticas completamente especificadas. Por lo tanto, en este paso, registre la configuración para las rutas completamente especificadas.

a. Explique qué es una ruta completamente especificada.

b. ¿Qué comando proporciona una ruta estática completamente especificada del R3 a la LAN del R2?

c. Escriba una ruta completamente especificada del R3 a la red entre el R2 y el R1. No configure la ruta, solo calcúlela.

d. Escriba una ruta estática completamente especificada del R3 a la LAN del R1. No configure la ruta, solo calcúlela.

Paso 5: verificar la configuración de las rutas estáticas.

Utilice los comandos **show** correspondientes para verificar que la configuración sea la correcta.

¿Qué comandos **show** puede utilizar para verificar que las rutas estáticas se hayan configurado correctamente?

Parte 3: Verificar la conectividad

Ahora todos los dispositivos deberían poder hacer ping a todos los demás dispositivos. Si no fuera así, revise la configuración de las rutas estáticas y predeterminadas.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: examinar la red y evaluar la necesidad de routing estático	Desde a hasta d	10	
	Total de la parte 1	**10**	
Parte 2: configurar rutas estáticas y predeterminadas	Paso 1	7	
	Paso 2	7	
	Paso 3	3	
	Paso 4	10	
	Paso 5	3	
	Total de la parte 2	**30**	
	Puntuación de Packet Tracer	**60**	
	Puntuación total	**100**	

8. Configuración de rutas estáticas y predeterminadas IPv6

Topología

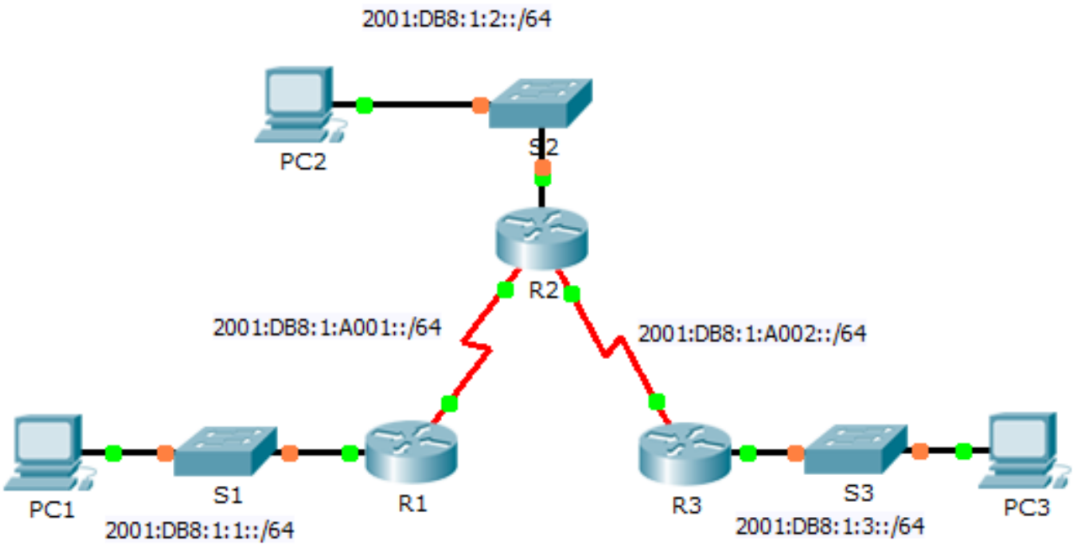


Tabla de direccionamiento IPv6

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:1:1::1/64	N/A
	S0/0/0	2001:DB8:1:A001::1/64	N/A
R2	G0/0	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	S0/0/1	2001:DB8:1:A002::1/64	N/A
R3	G0/0	2001:DB8:1:3::1/64	N/A
	S0/0/1	2001:DB8:1:A002::2/64	N/A
PC1	NIC	2001:DB8:1:1::F/64	FE80::1
PC2	NIC	2001:DB8:1:2::F/64	FE80::2
PC3	NIC	2001:DB8:1:3::F/64	FE80::3

Objetivos

Parte 1: examinar la red y evaluar la necesidad de routing estático

Parte 2: configurar rutas estáticas y predeterminadas IPv6

Parte 3: verificar la conectividad

Información básica

En esta actividad, configurará rutas estáticas y predeterminadas IPv6. Una ruta estática es una ruta que el administrador de red introduce manualmente para crear una ruta que sea confiable y segura. En esta actividad, se utilizan cuatro rutas estáticas diferentes: una ruta estática recursiva, una ruta estática conectada directamente, una ruta estática completamente especificada y una ruta predeterminada.

Parte 1: examinar la red y evaluar la necesidad de routing estático

a. Observe el diagrama de la topología. ¿Cuántas redes hay en total?

b. ¿Cuántas redes están conectadas directamente al R1, al R2 y al R3?

c. ¿Cuántas rutas estáticas requiere cada router para llegar a las redes que no están conectadas directamente?

d. ¿Qué comando se utiliza para configurar las rutas estáticas IPv6?

Parte 2: configurar rutas estáticas y predeterminadas IPv6

Paso 1: habilitar el routing IPv6 en todos los routers.

Antes de configurar rutas estáticas, se debe configurar el router para que reenvíe paquetes IPv6.

¿Qué comando permite lograr este resultado?

Introduzca este comando en cada router.

Paso 2: configurar rutas estáticas recursivas en el R1.

Configure una ruta estática IPv6 recursiva en cada red que no esté conectada directamente al R1.

Paso 3: configurar una ruta estática conectada directamente y completamente especificada en el R2.

a. Configure una ruta estática conectada directamente desde el R2 hasta la LAN del R1.

b. Configure una ruta completamente especificada desde el R2 hasta la LAN del R3.

Paso 4: configurar una ruta predeterminada en el R3.

Configure una ruta predeterminada recursiva en el R3 que llegue a todas las redes que no estén conectadas directamente.

Paso 5: verificar la configuración de las rutas estáticas.

a. ¿Qué comando se utiliza para verificar la configuración de IPv6 en una computadora desde el símbolo del sistema?

b. ¿Con qué comando se muestran las direcciones IPv6 configuradas en la interfaz de un router?

c. ¿Con qué comando se muestra el contenido de la tabla de routing IPv6?

Parte 3: Verificar la conectividad de la red

Ahora todos los dispositivos deberían poder hacer ping a todos los demás dispositivos. Si no fuera así, revise la configuración de las rutas estáticas y predeterminadas.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: examinar la red y evaluar la necesidad de routing estático	Desde a hasta d	20	
	Total de la parte 1	**20**	
Parte 2: configurar rutas estáticas y predeterminadas IPv6	Paso 1	5	
	Paso 5	15	
	Total de la parte 2	**20**	
	Puntuación de Packet Tracer	**60**	
	Puntuación total	**100**	

9. Diseño e implementación de un esquema de direccionamiento VLSM

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
	G0/0			No aplicable
	G0/1			No aplicable
	S0/0/0			No aplicable
	G0/0			No aplicable
	G0/1			No aplicable
	S0/0/0			No aplicable
	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	NIC			
	NIC			
	NIC			
	NIC			

Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direccionamiento VLSM

Parte 3: asignar direcciones IP a los dispositivos y verificar la conectividad

Información básica

En esta actividad, se le proporciona una dirección de red /24 que debe utilizar para diseñar un esquema de direccionamiento VLSM. A partir de un conjunto de requisitos, asignará las subredes y el direccionamiento, configurará los dispositivos y verificará la conectividad.

Parte 1: examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias.

Dividirá la dirección de red en subredes. La red tiene los siguientes requisitos:

- La LAN de requerirá direcciones IP host.
- La LAN de requerirá direcciones IP host.
- La LAN de requerirá direcciones IP host.
- La LAN de requerirá direcciones IP host.

¿Cuántas subredes se necesitan en la topología de la red?

Paso 2: determinar la información de la máscara de subred para cada subred.

a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requerida para ?
   ¿Cuántas direcciones host utilizables admitirá esta subred?
b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para ?
   ¿Cuántas direcciones host utilizables admitirá esta subred?
c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para ?
   ¿Cuántas direcciones host utilizables admitirá esta subred?
d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para ?
   ¿Cuántas direcciones host utilizables admitirá esta subred?
e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requerida para la conexión entre y ?

Parte 2: diseñar el esquema de direccionamiento VLSM

Paso 1: dividir la red según la cantidad de hosts por subred.

a. Utilice la primera subred para admitir la LAN más grande.
b. Utilice la segunda subred para admitir la segunda LAN más grande.
c. Utilice la tercera subred para admitir la tercera LAN más grande.
d. Utilice la cuarta subred para admitir la cuarta LAN más grande.
e. Utilice la quinta subred para admitir la conexión entre y .

Paso 2: registrar las subredes VLSM.

Complete la **tabla de subredes** con las descripciones de las subredes (p. ej., LAN de), la cantidad de hosts necesarios, la dirección de red para la subred, la primera dirección host utilizable y la dirección de difusión. Repita hasta que aparezcan todas las direcciones.

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección host utilizable	Dirección de difusión

Paso 3: Documente el esquema de direccionamiento.

a. Asigne las primeras direcciones IP utilizables a | para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables a | para los dos enlaces LAN. Asigne la última dirección IP utilizable al enlace WAN.

c. Asigne las segundas direcciones IP utilizables a los switches.

d. Asigne las últimas direcciones IP utilizables a los hosts.

Parte 3: asignar direcciones IP a los dispositivos y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para completar la configuración del direccionamiento.

Paso 1: configurar el direccionamiento IP en las interfaces LAN de .

Paso 2: configurar el direccionamiento IP en , incluido el gateway predeterminado.

Paso 3: configurar el direccionamiento IP en , incluido el gateway predeterminado.

Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde , , y . Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: examinar los requisitos de la red	Paso 1	1	
	Paso 2	4	
Total de la parte 1		**5**	
Parte 2: diseñar el esquema de direccionamiento VLSM			
Completar la tabla de subredes		25	
Registrar el direccionamiento		40	
Total de la parte 2		**65**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

ID:

10. Cálculo y configuración del resumen de ruta IPv4

Topología

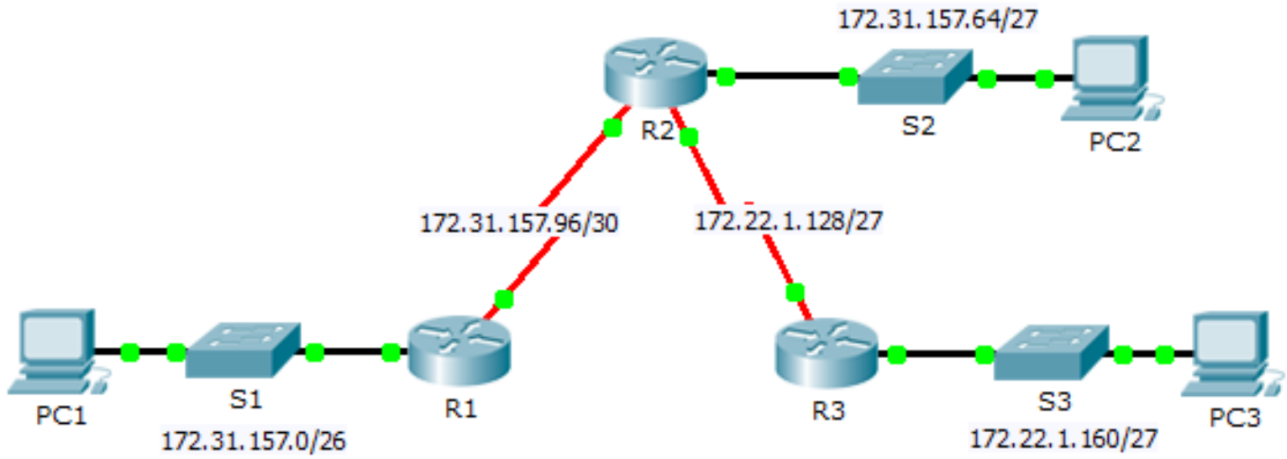


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.157.1	255.255.255.192	N/A
	S0/0/0	172.31.157.97	255.255.255.252	N/A
R2	G0/0	172.31.157.65	255.255.255.224	N/A
	S0/0/0	172.31.157.98	255.255.255.252	N/A
	S0/0/1	172.22.1.129	255.255.255.224	N/A
R3	G0/0	172.22.1.161	255.255.255.224	N/A
	S0/0/1	172.22.1.158	255.255.255.224	N/A
PC1	NIC	172.31.157.62	255.255.255.192	172.31.157.1
PC2	NIC	172.31.157.94	255.255.255.224	172.31.157.65
PC3	NIC	172.22.1.190	255.255.255.224	172.22.1.161

Objetivos

Parte 1: calcular rutas resumidas

Parte 2: configurar rutas resumidas

Parte 3: verificar la conectividad

Información básica

En esta actividad, calculará y configurará rutas resumidas. La sumarización de ruta, también conocida como "agregación de rutas", es el proceso de anunciar un conjunto de direcciones contiguas como una única dirección.

Parte 1: calcular rutas resumidas

Paso 1: calcular una ruta resumida en el R1 para llegar a las LAN en el R3.

a. Enumere las redes 172.22.1.128/27 y 172.22.1.160/27 en formato binario.

```
172.22.1.128: 10101100.00010110.00000001.10000000
172.22.1.160: 10101100.00010110.00000001.10100000
```

b. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de la ruta resumida. Tienen en común los 26 bits del extremo izquierdo.

```
172.22.1.128: 10101100.00010110.00000001.10000000
172.22.1.160: 10101100.00010110.00000001.10100000
```

c. Copie los bits coincidentes y rellene los restantes con ceros para determinar la dirección de red resumida.

```
10101100.00010110.00000001.10000000
```

d. ¿Cuál es la dirección de red resumida y la máscara de subred?

Paso 2: calcular una ruta resumida en el R3 para llegar a las LAN en el R1 y el R2.

a. Calcule la ruta resumida para las redes 172.31.157.0/26, 172.31.157.64/27 y 172.31.157.96/30. Enumerar las redes en formato binario. Luego cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de la ruta resumida.

b. ¿Cuál es la dirección de red resumida y la máscara de subred?

Parte 2: configurar rutas resumidas

Paso 1: configurar una ruta resumida para el R1.

Configure la ruta resumida recursiva que calculó en el paso 1 de la parte 1.

Paso 2: configurar una ruta resumida para el R3.

Configure la ruta resumida conectada directamente que calculó en el paso 2 de la parte 1.

Parte 3: Verificar la conectividad

Verifique que todos los equipos host y los routers puedan hacer ping a los equipos host y a los routers de la topología. De lo contrario, resuelva y corrija los problemas.

11. Cálculo y configuración del resumen de ruta IPv6

Topología

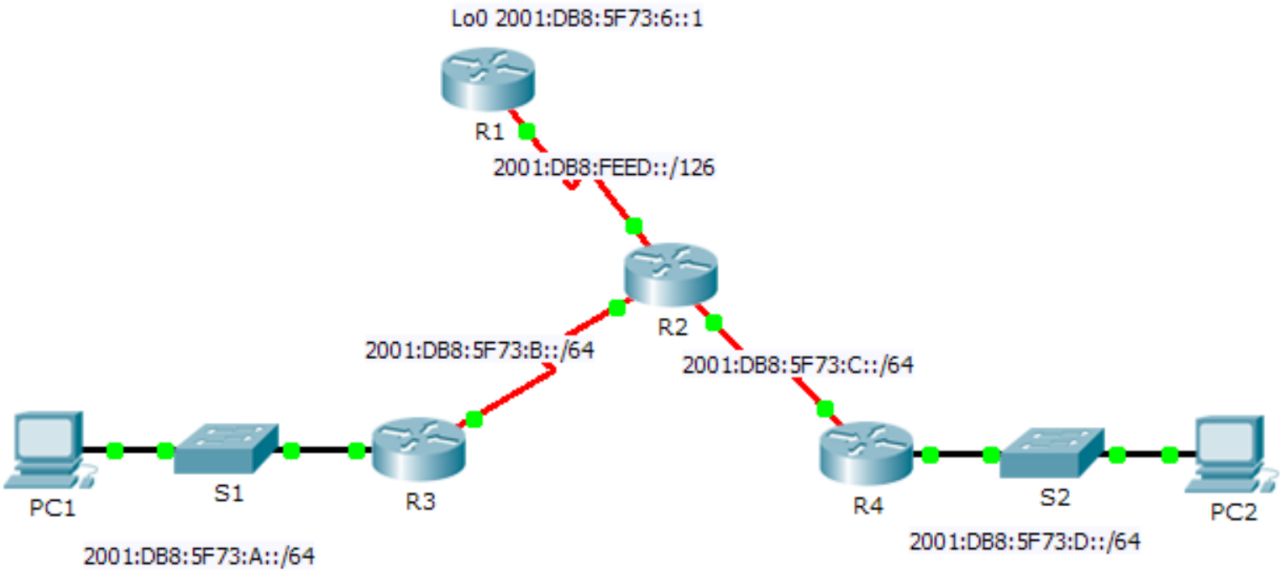


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6
R1	S0/0/0	2001:DB8:FEED::1/126
	Lo0	2001:DB8:5F73:6::1/64
R2	S0/0/0	2001:DB8:FEED::2/126
	S0/0/1	2001:DB8:5F73:B::1/64
	S0/1/0	2001:DB8:5F73:C::1/64
R3	G0/1	2001:DB8:5F73:A::1/64
	S0/0/0	2001:DB8:5F73:B::2/64
R4	G0/1	2001:DB8:5F73:D::1/64
	S0/0/1	2001:DB8:5F73:C::2/64

Objetivos

Parte 1: calcular una ruta resumida para el R1

Parte 2: configurar la ruta resumida y verificar la conectividad

Información básica

En esta actividad, deberá calcular, configurar y verificar una ruta resumida para todas las redes a las que el R1 tiene acceso a través del R2. El R1 está configurado con una interfaz loopback. En lugar de agregar una LAN u otra red al R1, se utilice una interfaz loopback para simplificar la prueba al verificar el routing.

Parte 1: configurar una ruta resumida para el R1

Al resumir una dirección IPv6, observe el prefijo para determinar dónde finaliza la dirección. En este caso, una dirección /64 termina en el cuarto segmento.

a. Enumere los primeros cuatro segmentos de cada una de las redes. Como los primeros tres segmentos tienen los mismos dígitos hexadecimales, no hay necesidad de escribirlos en binario. El cuarto segmento es diferente (:A, :B, :C y :D); por lo tanto, escriba los 16 bits de cada uno en binario. Cuente el número de bits coincidentes en el extremo izquierdo para determinar el prefijo de la ruta resumida.

2001:DB8:5F73:0000000000001010

2001:DB8:5F73:0000000000001011

2001:DB8:5F73:0000000000001100

2001:DB8:5F73:0000000000001101

b. En el cuarto segmento, las direcciones de red tienen los primeros 13 bits en común. Por lo tanto, el prefijo resumido se compone de los 48 bits de los primeros tres segmentos más los 13 bits del cuarto segmento (o /61).

c. Copie los bits coincidentes y rellene los restantes con ceros para determinar que la dirección de red resumida es 2001:0DB8:5F73:8::/61.

Parte 2: configurar la ruta resumida y verificar la conectividad

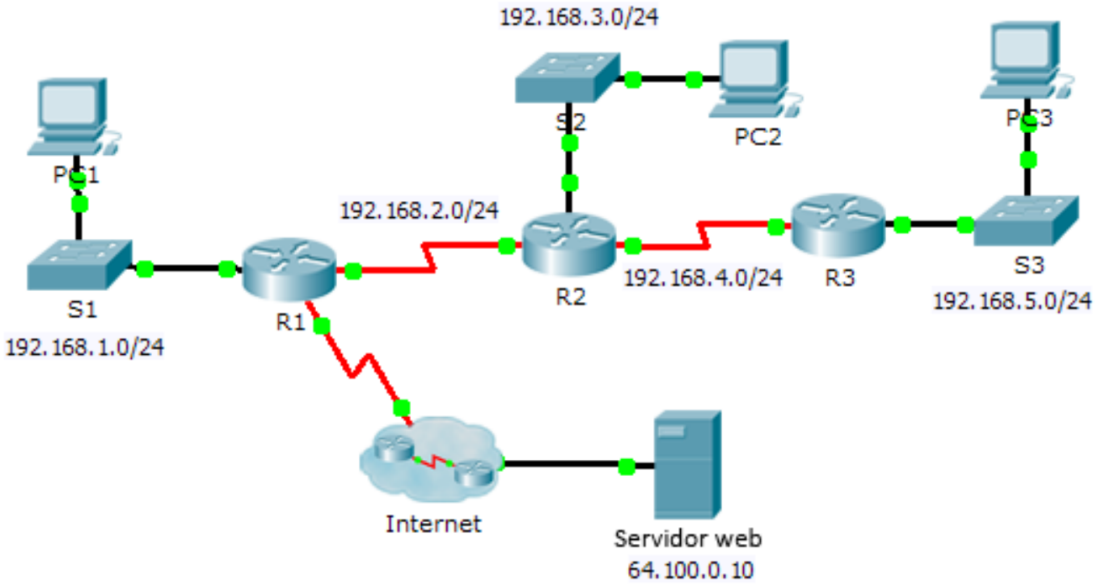
a. Configure una ruta resumida conectada directamente en el R1.

b. La PC1 debe poder hacer ping a la PC2.

c. La PC1 y la PC2 deben poder hacer ping a la interfaz loopback 0 en el R1.

12. Configuración de RIPv2

Topología



Objetivos

Parte 1: configurar RIPv2

Parte 2: verificar las configuraciones

Información básica

Si bien el protocolo RIP se utiliza con muy poca frecuencia en las redes modernas, es útil como base para comprender el routing de red básico. En esta actividad, configurará una ruta predeterminada y RIP versión 2 con instrucciones network e interfaces pasivas adecuadas, y verificará que haya plena conectividad.

Parte 1: Configurar RIPv2

Paso 1: configurar RIPv2 en el R1.

a. Utilice el comando adecuado para crear una ruta predeterminada en el **R1** para que todo el tráfico de Internet salga de la red a través de S0/0/1.

b. Ingrese al modo de configuración del protocolo RIP.

c. Utilice la versión 2 del protocolo RIP y deshabilite la sumarización de redes.

d. Configure RIP para las redes que se conectan al **R1**.

e. Configure el puerto LAN que no contiene ningún router de modo que no envíe información de routing.

f. Anuncie la ruta predeterminada configurada en el paso 1a a otros routers RIP.

g. Guarde la configuración.

Paso 2: configurar RIPv2 en el R2.

a. Ingrese al modo de configuración del protocolo RIP.

b. Utilice la versión 2 del protocolo RIP y deshabilite la sumarización de redes.

c. Configure RIP para las redes conectadas directamente al **R2**.

d. Configure la interfaz que no contiene ningún router de modo que no envíe información de routing.

e. Guarde la configuración.

Paso 3: configurar RIPv2 en el R3.

Repita el paso 2 en el **R3**.

Parte 2: verificar las configuraciones

Paso 1: ver las tablas de routing de R1, R2 y R3.

a. Utilice el comando adecuado para mostrar la tabla de routing del **R1**. RIP (R) ahora aparece con rutas conectadas (C) y rutas locales (L) en la tabla de routing. Todas las redes tienen una entrada. También se incluye una ruta predeterminada.

b. Vea las tablas de routing del **R2** y el **R3**. Observe que cada router tiene una lista completa de todas las redes 192.168.x.0 y una ruta predeterminada.

Paso 2: verificar la plena conectividad a todos los destinos.

Todos los dispositivos deberían poder hacer ping a los demás dispositivos dentro de la red. Además, todos los dispositivos deberían poder hacer ping al **servidor web**.

13. Configuración de RIPng

Topología

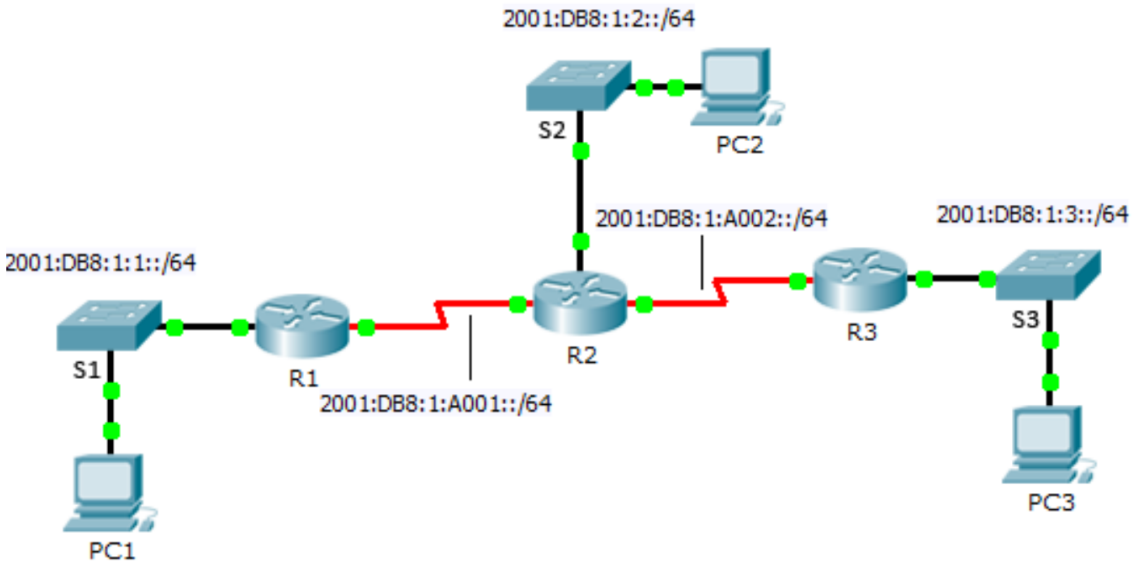


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6
R1	G0/0	2001:DB8:1:1::1/64
	S0/0/0	2001:DB8:1:A001::1/64
R2	G0/0	2001:DB8:1:2::1/64
	S0/0/0	2001:DB8:1:A001::2/64
	S0/0/1	2001:DB8:1:A002::1/64
R3	G0/0	2001:DB8:1:3::1/64
	S0/0/1	2001:DB8:1:A002::2/64

Objetivos

Parte 1: configurar RIPng

Parte 2: verificar las configuraciones y la conectividad

Información básica

RIP de última generación (RIPng) es un protocolo de routing vector distancia para enrutar direcciones IPv6. RIPng se basa en RIPv2 y tiene la misma distancia administrativa y limitación de 15 saltos. Esta actividad lo ayudará a familiarizarse con RIPng.

Parte 1: configurar RIPng

Paso 1: configurar RIPng en el R1.

a. Habilite el routing IPv6 en el **R1**.

```
R1(config)# ipv6 unicast-routing
```

b. Ingrese al modo de configuración del protocolo RIPng.

```
R1(config)# ipv6 router rip CISCO
```

c. Habilite RIPng para las redes que se conectan al **R1**.

```
R1(config-rtr)# int g0/0
R1(config-if)# ipv6 rip CISCO enable
R1(config-if)# int s0/0/0
R1(config-if)# ipv6 rip CISCO enable
```

d. Guarde la configuración.

Paso 2: configurar RIPng en el R2 y el R3.

Repita los pasos 1a hasta 1d en el **R2** y el **R3**.

Parte 2: verificar las configuraciones y la conectividad

Paso 1: ver las tablas de routing de R1, R2 y R3.

a. Utilice el comando adecuado para ver la tabla de routing del **R1**. RIPng (R) ahora aparece con rutas conectadas (C) y rutas locales (L) en la tabla de routing. Todas las redes tienen una entrada.

b. Verifique que las interfaces adecuadas utilicen RIPng.

```
R1# show ipv6 protocols
```

c. Vea la configuración en ejecución en el **R1**. Incluye entradas de RIPng.

d. Repita los pasos 1a hasta 1c en el **R2** y el **R3** para verificar que se hayan configurado de forma correcta.

Paso 2: verificar la plena conectividad.

Ahora todos los dispositivos deberían poder hacer ping a todos los demás dispositivos. De lo contrario, revise las configuraciones para detectar errores e implemente las soluciones adecuadas.

14. Configuración de OSPFv2 en un área única

Topología

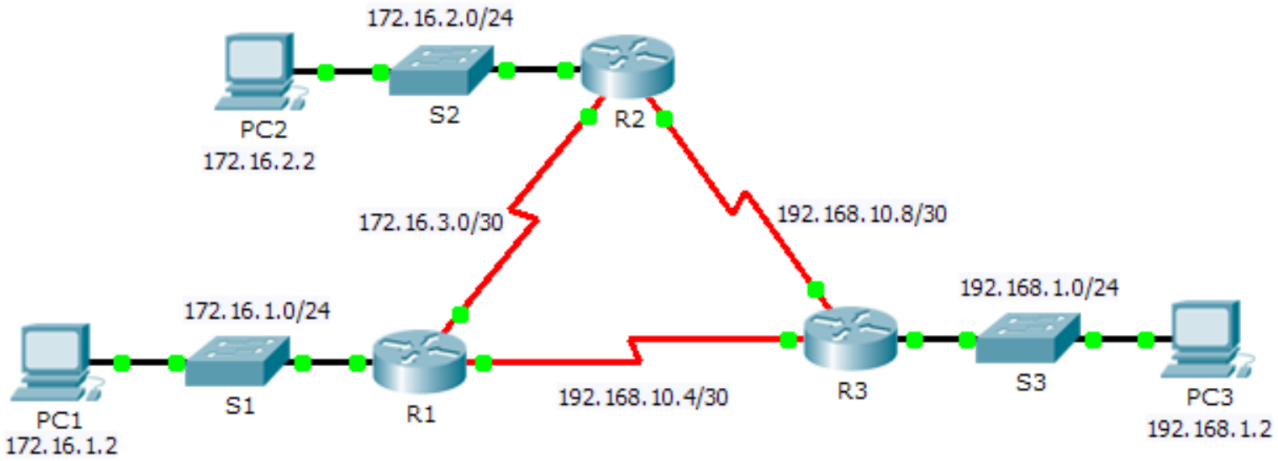


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.2	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.2	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Objetivos

Parte 1: configurar el routing OSPFv2

Parte 2: verificar las configuraciones

Información básica

En esta actividad, el direccionamiento IP ya está configurado. Usted es responsable de configurar la topología de tres routers con OSPFv2 básico de área única y, a continuación, de verificar la conectividad entre las terminales.

Parte 1: configurar el routing OSPFv2

Paso 1: configurar OSPF en R1, R2 y R3.

Utilice los siguientes requisitos para configurar el routing OSPF en los tres routers:

- ID de proceso 10
- ID del router para cada router: R1 = 1.1.1.1; R2 = 2.2.2.2; R3 = 3.3.3.3
- Dirección de red de cada interfaz
- Interfaz LAN configurada como pasiva (no utilice la palabra clave **default**)

Paso 2: verificar que el routing OSPF funcione.

En cada router, la tabla de routing ahora debe tener una ruta a cada red de la topología.

Parte 2: Verificación de las configuraciones

Cada computadora debe poder hacer ping a las otras dos computadoras. De lo contrario, revise las configuraciones.

15. Configuración de OSPFv3 básico en un área única

Topología

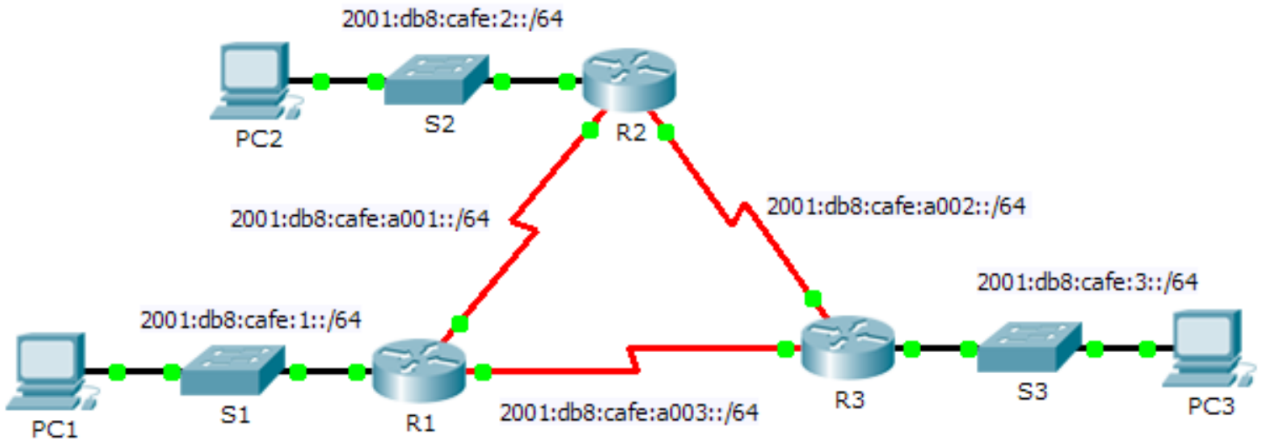


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
R1	F0/0	2001:db8:cafe:1::1/64	N/A
	S0/0/0	2001:db8:cafe:a001::1/64	N/A
	S0/0/1	2001:db8:cafe:a003::1/64	N/A
R2	F0/0	2001:db8:cafe:2::1/64	N/A
	S0/0/0	2001:db8:cafe:a001::2/64	N/A
	S0/0/1	2001:db8:cafe:a002::1/64	N/A
R3	F0/0	2001:db8:cafe:3::1/64	N/A
	S0/0/0	2001:db8:cafe:a003::264	N/A
	S0/0/1	2001:db8:cafe:a002::2/64	N/A
PC1	NIC	2001:db8:cafe:1::10/64	fe80::1
PC2	NIC	2001:db8:cafe:2::10/64	fe80::2
PC3	NIC	2001:db8:cafe:3::10/64	fe80::3

Objetivos

Parte 1: configurar el routing OSPFv3

Parte 2: verificar la conectividad

Información básica

En esta actividad, el direccionamiento IPv6 ya está configurado. Usted es responsable de configurar la topología de tres routers con OSPFv3 básico de área única y, a continuación, de verificar la conectividad entre las terminales.

Parte 1: configurar el routing OSPFv3

Paso 1: configurar OSPFv3 en R1, R2 y R3.

Utilice los siguientes requisitos para configurar el routing OSPF en los tres routers:

- Habilitación del routing IPv6
- ID de proceso 10
- ID del router para cada router: R1 = 1.1.1.1; R2 = 2.2.2.2; R3 = 3.3.3.3
- Habilitación de OSPFv3 en cada interfaz

Nota: la versión 6.0.1 de Packet Tracer no admite el comando **auto-cost reference-bandwidth**, por lo que no se ajustan los costos de ancho de banda en esta actividad.

Paso 2: verificar que el routing OSPF funcione.

Verifique que todos los routers hayan establecido adyacencia con los otros dos routers. Verifique que en la tabla de routing haya una ruta a cada red de la topología.

Parte 2: Verificar la conectividad

Cada computadora debe poder hacer ping a las otras dos computadoras. De lo contrario, revise las configuraciones.

Nota: esta actividad se califica únicamente con pruebas de conectividad. En la ventana de instrucciones no se mostrará su puntuación. Para ver su puntuación, haga clic en **Check Results (Verificar resultados)** > **Assessment Items (Elementos de evaluación)**. Para ver los resultados de una prueba de conectividad específica, haga clic en **Check Results** > **Connectivity Tests (Pruebas de conectividad)**.

16. Configuración de ACL estándar

Topología

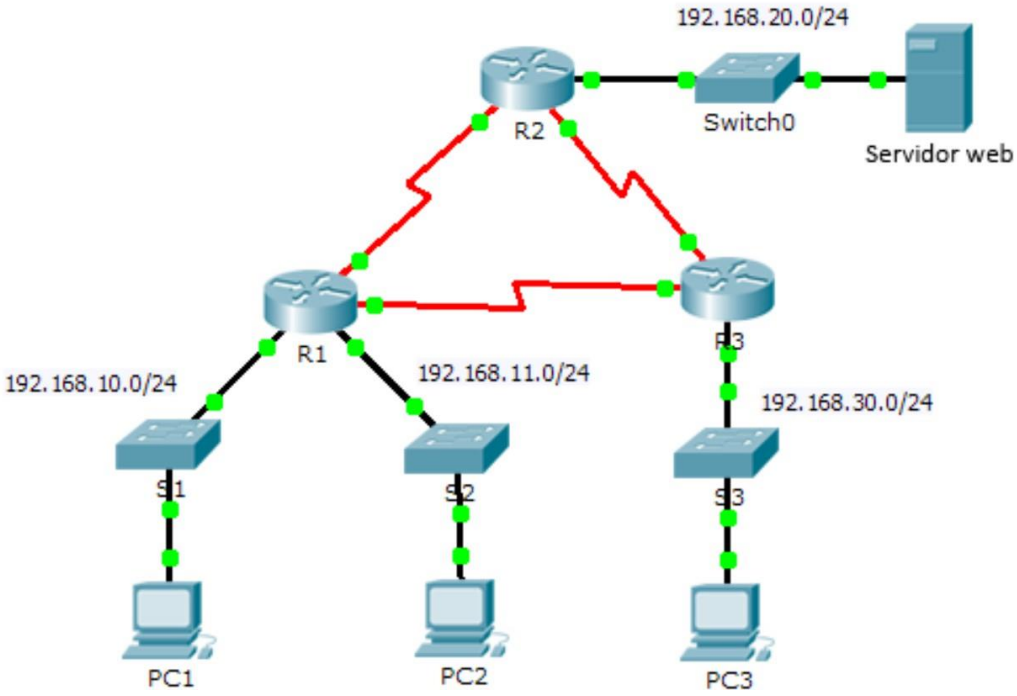


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Información básica/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad. Debería poder hacer ping correctamente a todos los dispositivos.

Paso 2: evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el **R2** están implementadas las siguientes políticas de red:

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. En el **R3** están implementadas las siguientes políticas de red:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**. Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

Parte 2: configurar, aplicar y verificar una ACL estándar

Paso 1: configurar y aplicar una ACL estándar numerada en el R2.

a. Cree una ACL con el número 1 en el **R2** con una instrucción que deniegue el acceso a la red 192.168.20.0/24 desde la red 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, configure la siguiente instrucción:

```
R2(config)# access-list 1 permit any
```

c. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del router. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Paso 2: configurar y aplicar una ACL estándar numerada en el R3.

a. Cree una ACL con el número 1 en el **R3** con una instrucción que deniegue el acceso a la red 192.168.30.0/24 desde la red de la **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. De manera predeterminada, las ACL deniegan todo el tráfico que no coincide con una regla. Para permitir el resto del tráfico, cree una segunda regla para la ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Para aplicar la ACL, colóquela en la interfaz Gigabit Ethernet 0/0 para el tráfico saliente.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Paso 3: verificar la configuración y la funcionalidad de la ACL.

a. En el **R2** y el **R3**, introduzca el comando **show access-list** para verificar las configuraciones de la ACL. Introduzca el comando **show run** o **show ip interface gigabitethernet 0/0** para verificar la colocación de las ACL.

b. Una vez colocadas las dos ACL, el tráfico de la red se restringe según las políticas detalladas en la parte 1. Utilice las siguientes pruebas para verificar las implementaciones de ACL:

- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
- Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
- Un ping de 192.168.11.10 a 192.168.20.254 falla.
- Un ping de 192.168.10.10 a 192.168.30.10 falla.
- Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
- Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.

17. Configuración de ACL estándar nombradas

Topología

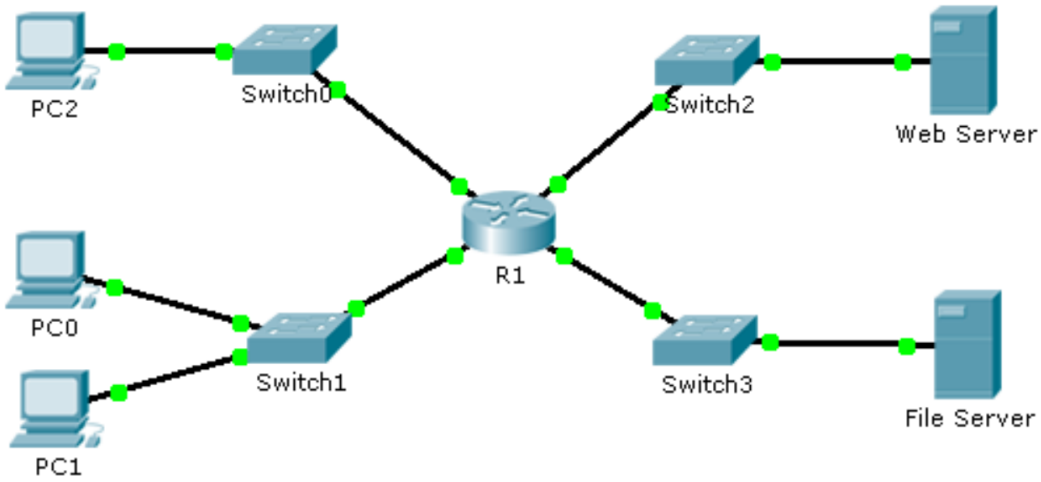


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
Servidor de archivos	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Servidor web	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objetivos

Parte 1: configurar y aplicar una ACL estándar con nombre

Parte 2: verificar la implementación de la ACL

Información básica/situación

El administrador de red sénior le solicitó que cree una ACL estándar con nombre para impedir el acceso a un servidor de archivos. Se debe denegar el acceso de todos los clientes de una red y de una estación de trabajo específica de una red diferente.

Parte 1: configurar y aplicar una ACL estándar con nombre

Paso 1: verificar la conectividad antes de configurar y aplicar la ACL.

Las tres estaciones de trabajo deben poder hacer ping tanto al **Servidor web** como al **Servidor de archivos**.

Paso 2: configurar una ACL estándar con nombre.

Configure la siguiente ACL con nombre en el **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

Nota: a los fines de la puntuación, el nombre de la ACL distingue mayúsculas de minúsculas.

Paso 3: aplicar la ACL con nombre.

a. Aplique la ACL de salida a la interfaz Fast Ethernet 0/1.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. Guarde la configuración.

Parte 2: verificar la implementación de la ACL

Paso 1: verificar la configuración de la ACL y su aplicación a la interfaz.

Utilice el comando **show access-lists** para verificar la configuración de la ACL. Utilice el comando **show run** o **show ip interface fastethernet 0/1** para verificar que la ACL se haya aplicado de forma correcta a la interfaz.

Paso 2: verificar que la ACL funcione correctamente.

Aunque las tres estaciones de trabajo deberían poder hacer ping al **servidor web**, pero sólo **PC1** debería poder hacer ping al **servidor web**.

18. Configuración de ACL extendidas

Topología

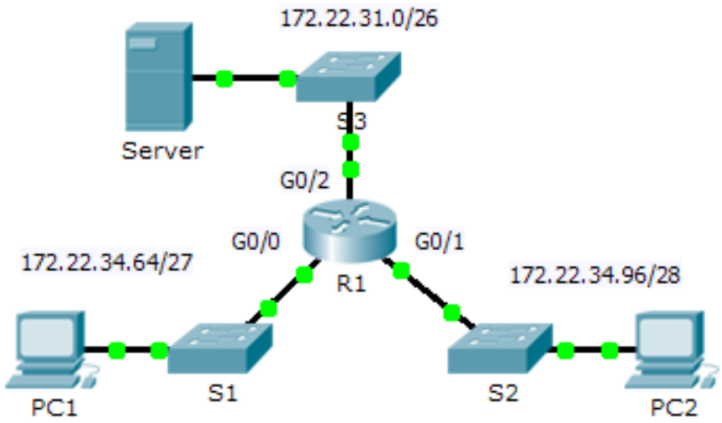


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objetivos

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Información básica/situación

Dos empleados necesitan acceder a los servicios que proporciona el servidor. La **PC1** solo necesita acceso FTP, mientras que la **PC2** solo necesita acceso web. Ambas computadoras pueden hacer ping al servidor, pero no entre sí.

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Paso 1: configurar una ACL para que permita tráfico FTP e ICMP.

a. Desde el modo de configuración global en el **R1**, introduzca el siguiente comando para determinar el primer número válido para una lista de acceso extendida.

```
R1(config)# access-list ?
```

```
  <1-99>      IP standard access list
  <100-199>   IP extended access list
```

b. Agregue **100** al comando, seguido de un signo de interrogación.

```
R1(config)# access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

c. Para permitir el tráfico FTP, introduzca **permit**, seguido de un signo de interrogación.

```
R1(config)# access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

d. Esta ACL permite tráfico FTP e ICMP. ICMP se indica más arriba, pero FTP no, porque FTP utiliza TCP. Entonces, se introduce TCP. Introduzca **tcp** para refinar aún más la ayuda de la ACL.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

e. Observe que se podría filtrar por **PC1** por medio de la palabra clave **host** o bien se podría permitir cualquier **(any)** host. En este caso, se permite cualquier dispositivo que tenga una dirección que pertenezca a la red 172.22.34.64/27. Introduzca la dirección de red, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D  Source wildcard bits
```

f. Para calcular la máscara wildcard, determine el número binario opuesto a una máscara de subred.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

g. Introduzca la máscara wildcard, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

h. Configure la dirección de destino. En esta situación, se filtra el tráfico hacia un único destino: el servidor. Introduzca la palabra clave **host** seguida de la dirección IP del servidor.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  range        Match only packets in the range of port numbers
  <cr>
```

i. Observe que una de las opciones es **<cr>** (retorno de carro). Es decir, puede presionar la tecla **Enter**, y la instrucción permitiría todo el tráfico TCP. Sin embargo, solo se permite el tráfico FTP. Por lo tanto, introduzca la palabra clave **eq**, seguida de un signo de interrogación para mostrar las opciones disponibles. Luego, introduzca **ftp** y presione la tecla **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la **PC1** al **Servidor**. Observe que el número de la lista de acceso es el mismo y que no es necesario detallar un tipo específico de tráfico ICMP.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. El resto del tráfico se deniega de manera predeterminada.

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del **R1**, el tráfico al cual se aplica la ACL 100 ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/0. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Paso 3: verificar la implementación de la ACL.

a. Haga ping de la **PC1** al **Servidor**. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

b. Desde la **PC1,** acceda mediante FTP al **Servidor**. Tanto el nombre de usuario como la contraseña son **cisco**.

```
PC> ftp 172.22.34.62
```

c. Salga del servicio FTP del **Servidor**.

```
ftp> quit
```

d. Haga ping de la **PC1** a la **PC2**. El host de destino debe ser inalcanzable, debido a que el tráfico no está permitido de manera explícita.

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Paso 1: configurar una ACL para que permita acceso HTTP y tráfico ICMP.

a. Las ACL con nombre comienzan con la palabra clave **ip**. Desde el modo de configuración global del **R1**, introduzca el siguiente comando, seguido por un signo de interrogación.

```
R1(config)# ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
```

b. Puede configurar ACL estándar y extendidas con nombre. Esta lista de acceso filtra tanto las direcciones IP de origen como de destino, por lo tanto, debe ser extendida. Introduzca **HTTP_ONLY** como nombre. (A los fines de la puntuación de Packet Tracer, el nombre distingue mayúsculas de minúsculas).

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. El indicador de comandos cambia. Ahora está en el modo de configuración de ACL extendida con nombre. Todos los dispositivos en la LAN de la **PC2** necesitan acceso TCP. Introduzca la dirección de red, seguida de un signo de interrogación.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
```

d. Otra manera de calcular el valor de una wildcard es restar la máscara de subred a 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
=   0.  0.  0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?
```

e. Para finalizar la instrucción, especifique la dirección del servidor como hizo en la parte 1 y filtre el tráfico **www**.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

f. Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la **PC2** al **Servidor**. Nota: la petición de entrada se mantiene igual, y no es necesario detallar un tipo específico de tráfico ICMP.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

g. El resto del tráfico se deniega de manera predeterminada. Salga del modo de configuración de ACL extendida con nombre.

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del **R1**, el tráfico al cual se aplica la lista de acceso **HTTP_ONLY** ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/1. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Paso 3: verificar la implementación de la ACL.

a. Haga ping de la **PC2** al **Servidor**. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

b. Desde la **PC2,** acceda mediante FTP al **Servidor**. La conexión debería fallar.

c. Abra el navegador web en la **PC2** e introduzca la dirección IP del **Servidor** como URL. La conexión debería establecerse correctamente.

19. Configuración de DHCP

Topología

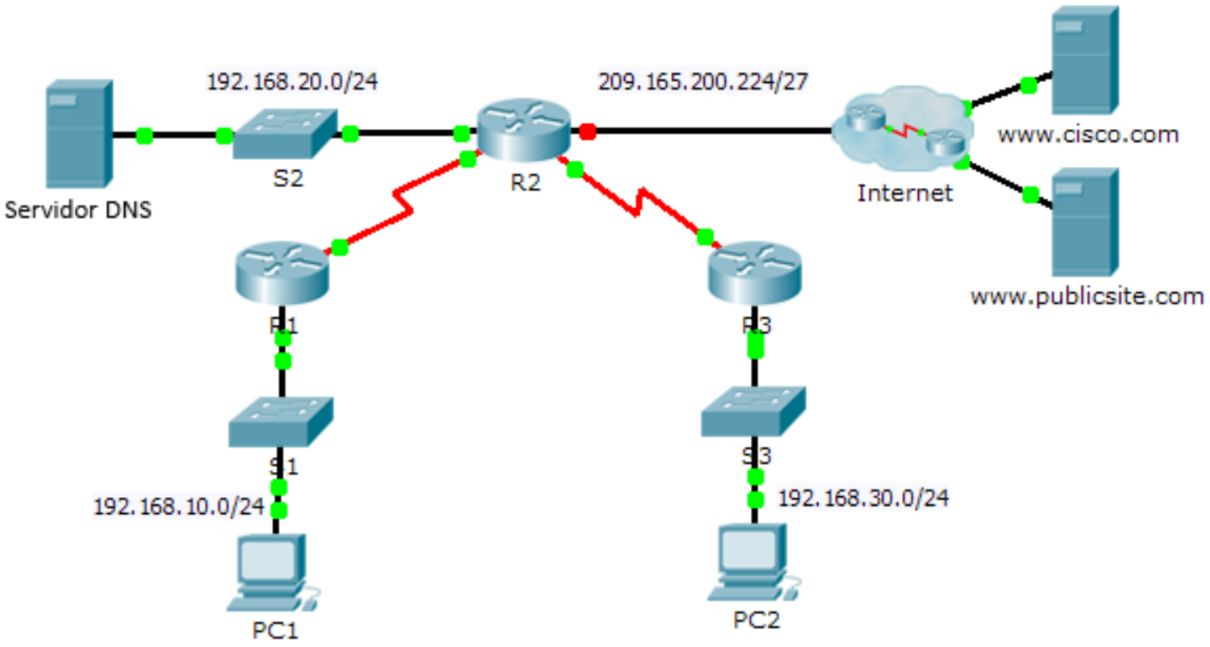


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
R2	G0/0	192.168.20.1	255.255.255.0	No aplicable
	G0/1	DHCP asignado	DHCP asignado	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
R3	G0/0	192.168.30.1	255.255.255.0	No aplicable
	S0/0/1	10.2.2.1	255.255.255.0	No aplicable
PC1	NIC	DHCP asignado	DHCP asignado	DHCP asignado
PC2	NIC	DHCP asignado	DHCP asignado	DHCP asignado
Servidor DNS	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: configurar un router como servidor de DHCP

Parte 2: configurar la retransmisión de DHCP

Parte 3: configurar un router como cliente DHCP

Parte 4: verificar DHCP y la conectividad

Situación

Un servidor de DHCP dedicado es escalable y relativamente fácil de administrar, pero puede ser costoso tener uno en cada ubicación en una red. Sin embargo, se puede configurar un router Cisco para proporcionar servicios DHCP sin necesidad de un servidor dedicado. Los routers Cisco utilizan el conjunto de características del IOS de Cisco, es decir, Easy IP como servidor de DHCP optativo con todas las características. Easy IP alquila las configuraciones por 24 horas de manera predeterminada. Como técnico de red de la empresa, tiene la tarea de configurar un router Cisco como servidor de DHCP para proporcionar la asignación dinámica de direcciones a los clientes de la red. También se le pide que configure el router perimetral como cliente DHCP para que reciba una dirección IP de la red ISP.

Parte 1: configurar un router como servidor de DHCP

Paso 1: configurar las direcciones IPv4 excluidas.

Configure el **R2** para excluir las primeras 10 direcciones de las LAN del R1 y del R3. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP.

Paso 2: crear un pool de DHCP en el R2 para la LAN del R1.

a. Cree un pool de DHCP llamado **`R1-LAN`** (con distinción entre mayúsculas y minúsculas).

b. Configure el pool de DHCP para que incluya la dirección de red, el gateway predeterminado y la dirección IP del servidor DNS.

Paso 3: crear un pool de DHCP en el R2 para la LAN del R3.

a. Cree un pool de DHCP llamado **`R3-LAN`** (con distinción entre mayúsculas y minúsculas).

b. Configure el pool de DHCP para que incluya la dirección de red, el gateway predeterminado y la dirección IP del servidor DNS.

Parte 2: configurar la retransmisión de DHCP

Paso 1: configurar el R1 y el R3 como agentes de retransmisión DHCP.

Paso 2: establecer la PC1 y la PC2 para que reciban información de direccionamiento IP de DHCP.

Parte 3: configurar el R2 como cliente DHCP

a. Configure la interfaz Gigabit Ethernet 0/1 en el R2 para que reciba el direccionamiento IP de DHCP y active la interfaz.

Nota: utilice la función **Fast Forward Time (Adelantar el tiempo)** de Packet Tracer para acelerar el proceso o espere hasta que el R2 forme una adyacencia de EIGRP con el router del ISP.

b. Utilice el comando **show ip interface brief** para verificar que el R2 haya recibido una dirección IP de DHCP.

Parte 4: verificar la conectividad y DHCP

Paso 1: verificar las asignaciones de DHCP.

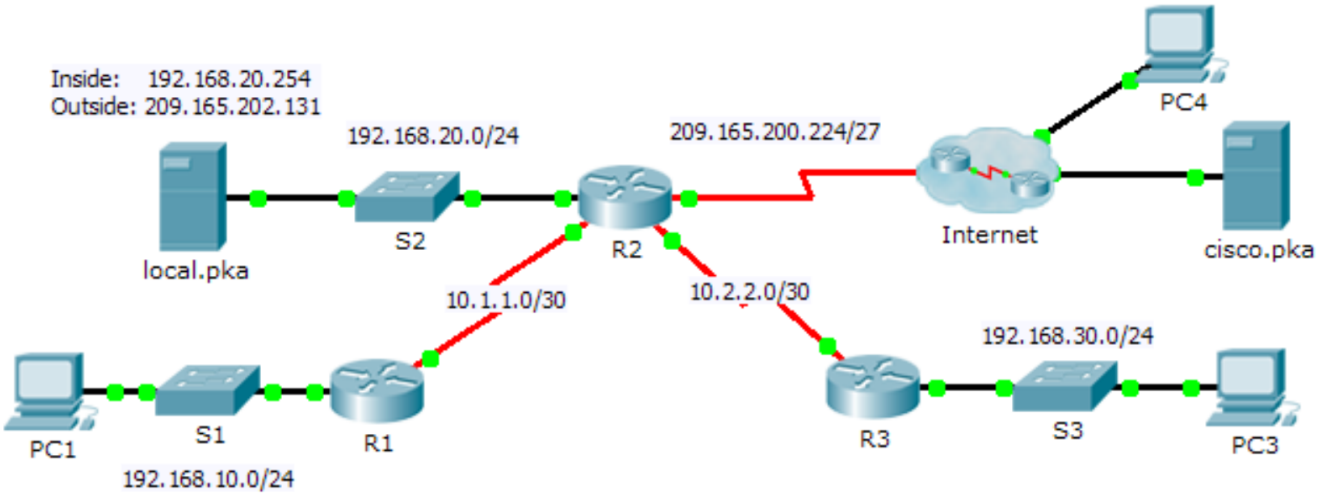
```
R2# show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.11    0002.4AA5.1470           --                     Automatic
192.168.30.11    0004.9A97.2535           --                     Automatic
```

Paso 2: verificar las configuraciones.

Verifique que la **PC1** y la **PC2** puedan hacer ping entre sí y a todos los demás dispositivos.

20. Implementación de NAT estática y dinámica

Topología



Objetivos

Parte 1: configurar la NAT dinámica con PAT

Parte 2: configurar la NAT estática

Parte 3: verificar la implementación de NAT

Parte 1: configurar la NAT dinámica con PAT

Paso 1: configurar el tráfico que se permitirá para traducciones NAT.

En el **R2**, configure una ACL estándar con nombre **R2NAT** que utilice tres instrucciones para permitir, en orden, los siguientes espacios de direcciones privadas:192.168.10.0/24, 192.168.20.0/24 y 192.168.30.0/24.

Paso 2: configurar un conjunto de direcciones para NAT.

a. Configure el **R2** con un conjunto de NAT que utilice las primeras dos direcciones en el espacio de direcciones 209.165.202.128/30. La cuarta dirección se utiliza para la NAT estática más adelante, en la parte 2.

Paso 3: asociar la ACL con nombre con el conjunto de NAT y habilitar PAT.

Paso 4: configurar las interfaces NAT.

Configure las interfaces del **R2** con los comandos de NAT inside y outside apropiados.

Parte 2: Configurar NAT estática

Consulte la topología. Cree una traducción de NAT estática para asignar la dirección interna de **local.pka** a su dirección externa.

Parte 3: verificar la implementación de NAT

Paso 1: acceder a los servicios a través de Internet.

a. Mediante el navegador web de la **PC1** o la **PC3**, acceda a la página web de **cisco.pka**.

b. Mediante el navegador web de la **PC4**, acceda a la página web de **local.pka.**

Paso 2: ver las traducciones NAT.

Vea las traducciones NAT en el **R2**.

```
R2# show ip nat translations
```