Cisco | Networking Academy®
Mind Wide Open™

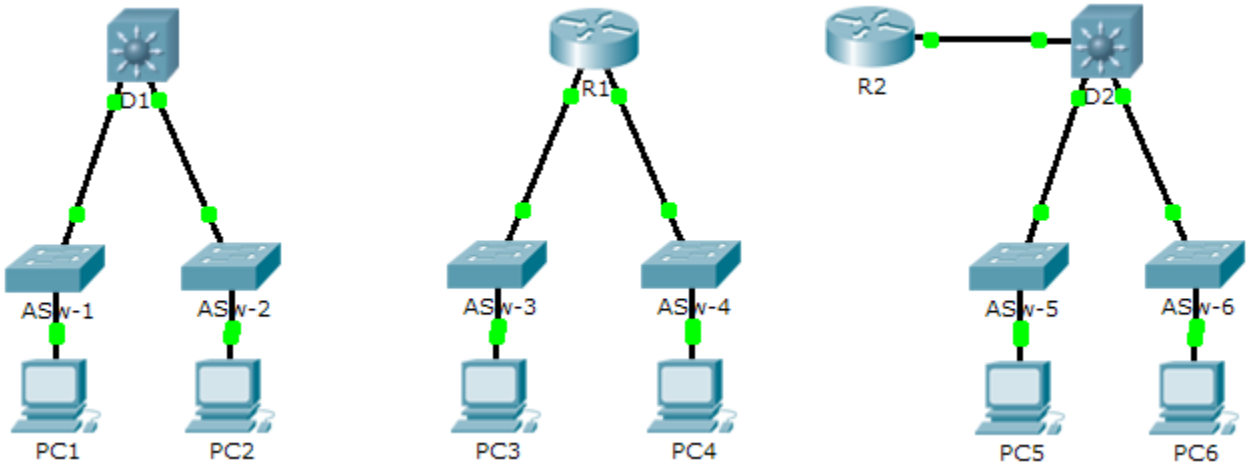
Switching y routing CCNA: Escalamiento de redes

Manual de Packet Tracer para el instructor

Packet Tracer: Comparación entre los switches 2960 y 3560 (versión para el instructor)

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

Topología



Objetivo

Parte 1: Comparar los switches de capa 2 y capa 3

Parte 2: Comparar un router y un switch de capa 3

Información básica

En esta actividad, utilizará distintos comandos para examinar tres topologías de switching diferentes y comparar las similitudes y las diferencias entre los switches 2960 y 3560. También comparará la tabla de routing de un router 1941 con un switch 3560.

Parte 1: Comparar los switches de capa 2 y capa 3

a. Examine los aspectos físicos de **D1** y **ASw-1**.

- ¿Cuántas interfaces físicas tiene cada switch en total? 26
- ¿Cuántas interfaces Fast Ethernet y Gigabit Ethernet tiene cada switch? 24 interfaces Fast Ethernet y 2 interfaces Gigabit Ethernet.
- Indique la velocidad de transmisión de las interfaces Fast Ethernet y Gigabit Ethernet en cada switch. Las interfaces Fast Ethernet admiten velocidades de entre 10 y 100 mbps, y las interfaces Gigabit Ethernet admiten velocidades de hasta 1000 mbps.
- ¿Alguno de los dos switches es de diseño modular? No

b. La interfaz de un switch 3560 se puede configurar como interfaz de capa 3 introduciendo el comando **no switchport** en el modo de configuración de interfaz. Esto permite que los técnicos asignen una dirección IP y una máscara de subred a la interfaz de la misma forma que se configura en la interfaz de un router.

- ¿Cuál es la diferencia entre un switch de capa 2 y un switch de capa 3? Un switch de capa 2 toma decisiones de reenvío sobre la base de las direcciones L2 (MAC). Las interfaces de los switches de capa 3 se pueden configurar con direcciones IP. Los switches también se pueden configurar con protocolos de routing, al igual que un router.
- ¿Cuál es la diferencia entre la interfaz física y la interfaz VLAN de un switch? Una interfaz física de switch se utiliza para conectar físicamente las terminales a la red. Una interfaz virtual conmutada (SVI o VLAN) se utiliza para configurar el switch con una dirección IP para que se lo pueda administrar de forma remota.
- ¿En qué capa funciona un switch 2960 y un switch 3560? El switch 2960 opera en la capa 2, y el 3560 opera en las capas 2 y 3.
- ¿Qué comando permite que el técnico asigne una dirección IP y una máscara de subred a la interfaz Fast Ethernet en un switch 2960? Las interfaces Fast Ethernet en los switches 2960 no se pueden configurar con una dirección IP y una máscara de subred.
- Emita el comando **show run** para examinar la configuración de los switches **D1** y **ASw-1**. ¿Observa diferencias entre ellos? Sí, las interfaces G0/2 y la interfaz G0/1 del D1 están configuradas con el comando **no switchport** y muestran una dirección IP y una máscara configuradas en ambas interfaces Gigabit Ethernet. El D1 tiene routing IP habilitado.
- Muestre la tabla de routing en ambos switches mediante el comando **show ip route**. ¿Por qué cree que el comando no funciona en **ASW-1**, pero sí lo hace en **D1**? Funciona en el D1 porque este opera en las capas 2 y 3, lo que permite que funcione como switch de capa 2; al mismo tiempo, puede enrutar paquetes y tomar decisiones de reenvío según la información de capa 3 (direcciones IP), algo que los switches convencionales no pueden hacer.

Parte 2: Comparar un router y un switch de capa 3

a. Hasta hace poco, los routers y switches eran dispositivos separados y diferentes. El término “switch” se dejó solo para referirse a dispositivos basados en hardware que funcionan en la capa 2. Por el contrario, los routers son dispositivos que toman decisiones de reenvío según la información de capa 3, y utilizan protocolos de routing para compartir información de routing y para comunicarse con otros routers. Los switches de capa 3, como el 3560, se pueden configurar para reenviar paquetes de capa 3. Si se introduce el comando **ip routing** en el modo de configuración global, los switches de capa 3 se pueden configurar con los protocolos de routing y, de ese modo, pueden poseer algunas de las capacidades de un router. Sin embargo, aunque son similares en algunos aspectos, son diferentes en muchos otros.

- Abra la ficha Physical (Capa física) en el D1 y el R1. ¿Observa similitudes y diferencias entre los dos? Ambos tienen un puerto de consola y dos interfaces Gigabit Ethernet. El R1 es modular y se le pueden agregar diversas interfaces, mientras que el D1 solo posee interfaces fijas. El R1 tiene interfaces seriales y asíncronas, mientras que el D1 solo tiene interfaces Ethernet. Desde el punto de vista retrospectivo, el D1 solo puede utilizar cables de cobre, mientras que el R1 puede utilizar varios tipos de conexiones.
- Emita el comando **show run** y examine la configuración del R1 y el D1. ¿Qué diferencias ve entre los dos? El R1 y el D1 tienen configuradas las mismas direcciones IP, pero en diferentes interfaces. Para que se pueda asignar una dirección IP al puerto de switch, los técnicos deben emitir el comando **no switchport**.
- ¿Qué comando permite que el D1 configure una dirección IP en una de sus interfaces físicas? El comando **no switchport**.

- Utilice el comando **show ip route** en ambos dispositivos. ¿Observa similitudes o diferencias entre las dos tablas? Los códigos son los mismos, excepto que el router tiene un código L para “local”. Este es un enlace configurado en la interfaz física del R1, que el switch no tiene. En las tablas de routing de ambos dispositivos se muestran las mismas redes.
- Ahora, analice la tabla de routing del R2 y el D2. ¿Qué es evidente ahora que no lo era en la configuración del R1 y el D1? Ambos tienen EIGRPconfigurado y ambos descubren redes del otro.

b. Realice las siguientes pruebas para verificar que cada topología tenga plena conectividad:

- Haga ping de la **PC1** a la **PC2.**
- Haga ping de la **PC3** a la **PC4.**
- Haga ping de la **PC5** a la **PC6.**

En los tres ejemplos, cada computadora está en una red diferente. ¿Qué dispositivo se utiliza para proporcionar la comunicación entre las redes? El router o el switch multicapa.

¿Por qué pudimos hacer ping a través de las redes sin que haya un router? Un switch multicapa puede enrutar entre redes siempre y cuando esté configurado con una dirección IP y tenga habilitado el routing IP. También debe estar habilitado si planea ejecutar protocolos de routing, como EIGRP, en el switch. No se olvide de que el comando **no switchport** debe estar habilitado en la interfaz para poder asignarle una dirección IP y una máscara de subred a la interfaz física del switch.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Comparar los switches de capa 2 y capa 3	a	20	
	b	40	
Total de la parte 1		**60**	
Parte 2: Comparar un router y un switch de capa 3	a	30	
	b	10	
Total de la parte 2		**40**	
Puntuación total		**100**	

Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

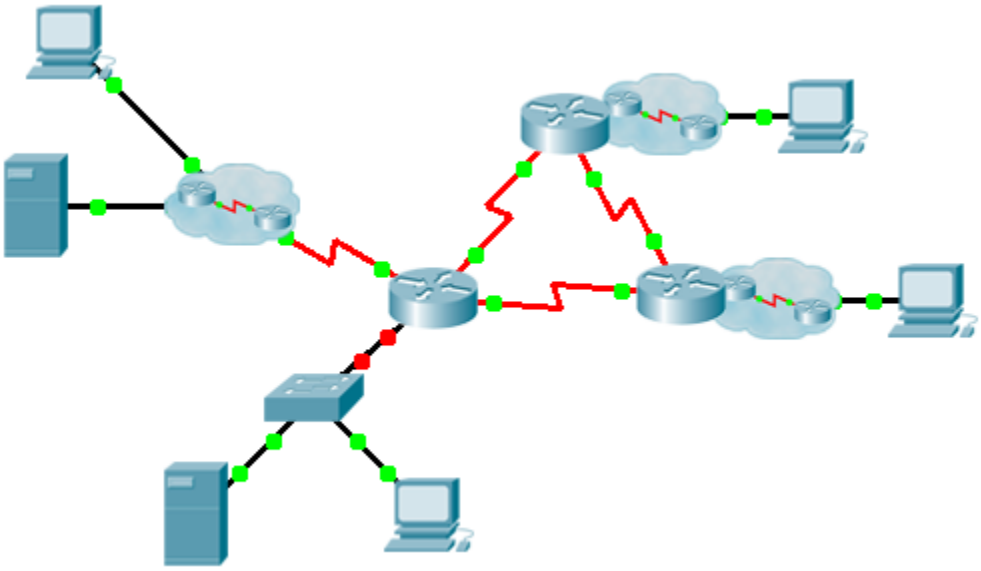


Tabla de asignación de direcciones

Nota para el instructor: en la versión para los estudiantes, hay espacios en blanco en lugar de todas las variables que se muestran entre corchetes dobles.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0.15	[[R1G0sub15Add]]	[[R1G0sub15SM]]	N/A
	G0/0.30	[[R1G0sub30Add]]	[[R1G0sub30SM]]	N/A
	G0/0.45	[[R1G0sub45Add]]	[[R1G0sub45SM]]	N/A
	G0/0.60	[[R1G0sub60Add]]	[[R1G0sub60SM]]	N/A
	S0/0/0	[[R1S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R1S001Add]]	255.255.255.252	N/A
	S0/1/0	[[R1S010Add]]	255.255.255.252	N/A
[[R2Name]]	G0/0	[[R2G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R2S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R2S001Add]]	255.255.255.252	N/A
[[R3Name]]	G0/0	[[R3G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R3S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R3S001Add]]	255.255.255.252	N/A
[[S1Name]]	VLAN 60	[[S1VLAN60Add]]	[[R1G0sub60SM]]	[[R1G0sub60Add]]
[[PC1Name]]	NIC	DHCP asignado	DHCP asignado	DHCP asignado

Tabla de asignaciones de VLAN y de puertos

Número de VLAN - Nombre	Asignación de puertos	Red
15 - Servers (Servidores)	F0/11 - F0/20	[[R1-VLANsrvNet]]
30 - PCs	F0/1 - F0/10	[[R1-VLANpcNet]]
45 - Native	G1/1	[[R1-VLANntvNet]]
60 - Management	VLAN 60	[[R1-VLANmanNet]]

Situación

Esta actividad incluye muchas de las habilidades que adquirió durante sus estudios en CCNA. Primero deberá completar la documentación de la red. De modo que debe asegurarse de tener una versión impresa de las instrucciones. Durante la implementación, configurará las VLAN, los enlaces troncales, la seguridad de puertos y el acceso remoto SSH en un switch. Luego deberá implementar el routing entre redes VLAN y NAT en un router. Por último, deberá utilizar su documentación para verificar la implementación al probar la conectividad de extremo a extremo.

Documentación

Deberá documentar completamente la red. Necesitará una copia impresa de este conjunto de instrucciones, que incluirá un diagrama de topología sin etiquetas:

- Rotule todos los nombres de los dispositivos, las direcciones de red y demás información importante generada por Packet Tracer.
- Complete la **tabla de direccionamiento** y la **tabla de asignación de VLAN y de puertos**.
- Complete los espacios en blanco en los pasos **implementación** y **verificación**. La información se proporcionará cuando inicie la actividad de Packet Tracer.

Implementación

Nota: todos los dispositivos en la topología, excepto **[[R1Name]]**, **[[S1Name]]** y **[[PC1Name]]**, están totalmente configurados. No tiene acceso a los otros routers. Puede acceder a todos los servidores y equipos para fines de prueba.

Implemente los siguientes requisitos mediante su documentación:

[[S1Name]]

- Configure el acceso de administración remota, que incluye asignación de direcciones IP y SSH:
  - El dominio es cisco.com.
  - Al usuario **[[UserText]]** le corresponde la contraseña **[[UserPass]]**.
  - La longitud de la clave criptográfica es 1024.
  - SSH versión 2, limitado a dos intentos de autenticación y a un tiempo de espera de 60 segundos.
  - Las contraseñas de texto no cifrado deben cifrarse.
- Configure, nombre y asigne las VLAN. Los puertos deben configurarse manualmente como puertos de acceso.
- Configurar enlaces troncales.
- Implementar seguridad de puerto:
  - En Fa0/1, permita que se agreguen dos direcciones MAC de forma automática al archivo de configuración cuando se detecten. El puerto no debe ser inhabilitado, pero se debe capturar un mensaje de syslog si ocurre una violación.
  - Deshabilite todos los otros puertos sin utilizar.

[[R1Name]]

- Configurar el routing entre VLAN.
- Configure los servicios de DHCP para VLAN 30. Utilice **LAN** como el nombre con distinción de mayúsculas para el conjunto.
- Implemente el routing:
  - Utilice la ID del proceso OSPF 1 y la ID del router 1.1.1.1.
  - Configure una instrucción network para todo el espacio de direcciones de **[[DisplayNet]]**.
  - Deshabilite las interfaces que no deben enviar mensajes OSPF.
  - Configure una ruta predeterminada a Internet.
- Implemente NAT:
  - Configure una ACL n.º 1 estándar con una instrucción. Se permiten todas las direcciones IP que pertenecen al espacio de direcciones de **[[DisplayNet]]**.

- Consulte su registro y configure la NAT estática para el servidor de archivos.
- Configure la NAT dinámica con PAT mediante un nombre de conjunto de su elección, una máscara /30 y estas dos direcciones públicas:

  [[NATPoolText]]

[[PC1Name]]

Verifique que **[[PC1Name]]** haya recibido información de direccionamiento completa del **[[R1Name]]**.

Verificación

Todos los dispositivos deben poder hacer ping a todos los otros dispositivos. Si no es así, revise sus configuraciones para aislar y resolver problemas. Entre las pruebas se incluyen:

- Verificar el acceso remoto a **[[S1Name]]** mediante SSH desde una computadora.
- Verificar que las VLAN están asignadas a los puertos correspondientes y que la seguridad de puerto esté activada.
- Verificar los vecinos OSPF y que la tabla de routing esté completa.
- Verificar las traducciones y estáticas de NAT.
  - El **host externo** debe poder acceder al **servidor de archivos** en la dirección pública.
  - Las computadoras internas deben poder acceder al **servidor web**.
- Documente cualquier problema que haya encontrado y las soluciones en la tabla **Documentación de resolución de problemas** a continuación.

Documentación de resolución de problemas

Problema	Solución

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 70 puntos. La documentación vale 30 puntos.

ID:[[indexAdds]][[indexNATs]][[indexNames]]

```
**************************************************
ISOMORPH ID KEY:
ID = XYZ where;
 X = indexAdds for /24 private address space
 Y = indexNATs for NAT and SSH specific configs
 Z = indexNAMES for device names
Note: Each seed contains variables that are independent
of the other seeds. You do not need to test all the
various combinations.
==================================================
ISOMORPH ID = 000
==================================================
!HQ!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 172.16.15.32 255.255.255.224
 default-router 172.16.15.33
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 172.16.15.17 255.255.255.240
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.15.33 255.255.255.224
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 172.16.15.1 255.255.255.248
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.15.9 255.255.255.248
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 172.16.15.0 0.0.0.255 area 0
```



```
!
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 172.16.15.18 209.165.200.227
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 172.16.15.0 0.0.0.255
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!HQ-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
en
conf t
int vlan 60
ip add 172.16.15.10 255.255.255.248
no shut
ip default-gateway 172.16.15.9
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
```



```
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user HQadmin pass ciscoclass
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh

=========================================================
ISOMORPH ID = 111
=========================================================
!Admin!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 10.10.10.192 255.255.255.192
 default-router 10.10.10.193
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 10.10.10.161 255.255.255.224
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.10.10.193 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 10.10.10.129 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.10.10.145 255.255.255.240
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 10.10.10.0 0.0.0.255 area 0
interface s0/0/0
```



```
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
!
ip nat pool TEST 198.133.219.128 198.133.219.129 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 10.10.10.162 198.133.219.130
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 10.10.10.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!Admin-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 10.10.10.146 255.255.255.240
no shut
ip default-gateway 10.10.10.145
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
```



```
ip domain-name cisco.com
crypto key gen rsa
1024

user Admin pass letmein
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh

================================================================
ISOMORPH ID: 222
================================================================
!Central!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 192.168.45.128 255.255.255.192
 default-router 192.168.45.129
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 192.168.45.65 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.45.129 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 192.168.45.17 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.45.33 255.255.255.240
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 192.168.45.0 0.0.0.255 area 0
interface s0/0/0
 ip nat inside
interface s0/0/1
```



```
 ip nat inside
interface s0/1/0
 ip nat outside
!
ip nat pool TEST 64.100.32.56 64.100.32.57 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 192.168.45.66 64.100.32.58
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 192.168.45.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!Cnt-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 192.168.45.34 255.255.255.240
no shut
ip default-gateway 192.168.45.33
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
```



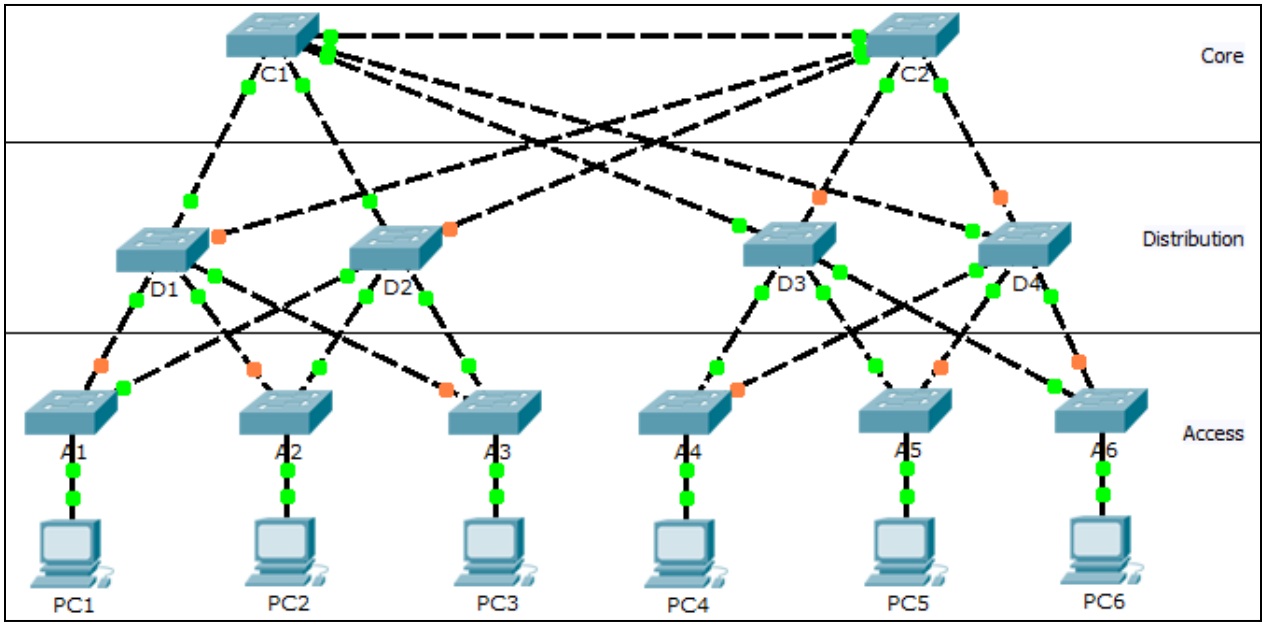
```
1024

user CAdmin pass itsasecret
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh
```


Packet Tracer: Análisis de un diseño redundante (versión para el instructor)

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

Topología



Objetivos

Parte 1: Revisar la convergencia de STP

Parte 2: Examinar el proceso ARP

Parte 3: Probar la redundancia en una red conmutada

Información básica

En esta actividad, observará cómo funciona STP, de manera predeterminada, y cómo reacciona ante fallas. Se agregaron switches que no requieren configuración a la red. Los switches de Cisco se pueden conectar a la red sin ninguna acción adicional requerida por parte del administrador de red. Se modificó la prioridad del puente a los fines de esta actividad.

Parte 1: Revisar la convergencia del STP

Cuando el STP se converge por completo, ocurren las siguientes condiciones:

- Todas las PC tienen luces de enlace verdes en los puertos conmutados.
- Los switches de capa de acceso tienen un uplink de reenvío (enlace verde) a un switch de capa de distribución y un uplink de bloqueo (enlace ámbar) a un segundo switch de capa de distribución.
- Los switches de capa de distribución tienen un uplink de reenvío (enlace verde) a un switch de capa de núcleo y un uplink de bloqueo (enlace ámbar) a otro switch de capa de núcleo.

Parte 2: Examinar el proceso ARP

Paso 1: Cambie a modo de simulación.

Paso 2: Haga ping de PC1 a PC6.

a. Utilice la herramienta **Add Simple PDU** (Agregar PDU simple) para crear una PDU de la **PC1** a la **PC6**. Asegúrese de que ARP e ICMP estén seleccionados en **Event List Filters** (Filtros de lista de eventos). Haga clic en **Capture/Forward** (Capturar/Adelantar) para examinar el proceso ARP mientras la red conmutada descubre las direcciones MAC de la **PC1** y la **PC6**. Observe que los puertos de bloqueo detienen todos los bucles posibles. Por ejemplo, la solicitud de ARP de la **PC1** viaja del **A1** al **D2**, después al **C1** y, por último, al **D1,** y vuelve al **A1**. Sin embargo, como STP bloquea el enlace entre el **A1** y el **D1**, no se produce ningún bucle.

b. Observe que la respuesta de ARP de la **PC6** se transporta de regreso por una ruta. ¿Por qué? Porque es la única ruta válida cuando STP bloquea los enlaces redundantes.

c. Registre la ruta sin bucles entre la **PC1** y la **PC6**. **PC1** > **A1** > **D2** > **C1** > **D3** > **A6** > **PC6**

Paso 3: Volver a examinar el proceso ARP.

a. Debajo de la lista desplegable **Scenario 0** (Situación 0), haga clic en **New** (Nuevo) para crear el **Scenario 1**. Examine el proceso del ARP nuevamente haciendo ping entre dos PC diferentes.

b. ¿Qué parte de la ruta cambió desde el último conjunto de pings? Las respuestas pueden variar según la computadora desde la que los estudiantes hagan ping.

Parte 3: Probar la redundancia en una red conmutada

Paso 1: Elimine el enlace entre el A1 y el D2.

Cambie al modo **Realtime** (Tiempo real). Elimine el enlace entre el **A1** y el **D2**. Lleva algo de tiempo que el STP converja y establezca una nueva ruta sin bucles. Dado que solo el **A1** se ve afectado, observe cómo la luz ámbar del enlace entre el **A1** y el **D1** cambia a verde. Puede hacer clic en **Fast Forward Time** (Adelantar el tiempo) para acelerar el proceso de convergencia de STP.

Paso 2: Haga ping entre la PC1 y la PC6.

a. Después de que el enlace entre el **A1** y el **D1** se active (indicado por una luz verde), cambie al modo **Simulation** (Simulación) y cree el **Scenario 2**. Haga ping entre la **PC1** y la **PC6** de nuevo.

b. Registre la nueva ruta sin bucles. **PC1** > **A1** > **D1** > **C1** > **D3** > **A6** > **PC6**

Paso 3: Eliminar el enlace entre el C1 y el D3.

a. Cambie al modo **Realtime (Tiempo real)**. Observe que los enlaces entre el **D3** y el **D4** al **C2** son de color ámbar. Elimine el enlace entre el **C1** y el **D3**. Lleva algo de tiempo que el STP converja y establezca una nueva ruta sin bucles. Observe los enlaces de color ámbar en el **D3** y el **D4**. Puede hacer clic en **Fast Forward Time** (Adelantar el tiempo) para acelerar el proceso de convergencia de STP.

b. ¿Cuál es el enlace activo a **C2** ahora? El enlace entre el F0/1 del **D3** y el F0/2 del **C2**.

Paso 4: Haga ping entre la PC1 y la PC6.

a. Cambie al modo **Simulation** y cree **Scenario 3**. Haga ping entre la **PC1** y la **PC6**.

b. Registre la nueva ruta sin bucles. **PC1** > **A1** > **D1** > **C1** > **D4** > **A6** > **PC6**

Paso 5: Elimine el D4.

Cambie al modo **Realtime (Tiempo real)**. Observe que el **A4**, el **A5** y el **A6** reenvían el tráfico al **D4**. Elimine el **D4**. Lleva algo de tiempo que el STP converja y establezca una nueva ruta sin bucles. Observe que los enlaces entre el **A4**, el **A5** y el **A6** al **D3** cambien a reenvío (verde). Ahora, los tres switches deben reenviar el tráfico al **D3**.

Paso 6: Haga ping entre la PC1 y la PC6.

a. Cambie al modo **Simulation** y cree **Scenario 4**. Haga ping entre la **PC1** y la **PC6**.

b. Registre la nueva ruta sin bucles. **PC1** > **A1** > **D1** > **C1** > **C2** > **D3** > **A6** > **PC6**

c. ¿Qué tiene de especial la nueva ruta que usted no haya visto antes? El **D3** ahora es el switch designado para el reenvío de paquetes si la **PC1** quisiera hacer ping a la **PC6**. No hay rutas redundantes debajo del **C2**.

Paso 7: Elimine el C1.

Cambie al modo **Realtime (Tiempo real)**. Observe que el **D1** y el **D2** reenvían el tráfico al **C1**. Elimine el **C1**. Lleva algo de tiempo que el STP converja y establezca una nueva ruta sin bucles. Observe que los enlaces entre el **D1** y el **D2** al **C2** cambien a reenvío (verde). Una vez que hayan convergido, los switches deben reenviar el tráfico al **C2**.

Paso 8: Haga ping entre la PC1 y la PC6.

a. Cambie al modo **Simulation** y cree **Scenario 5**. Haga ping entre la **PC1** y la **PC6**.

b. Registre la nueva ruta sin bucles. **PC1** > **A1** > **D1** > **C2** > **D3** > **A6** > **PC6**

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Examinar el proceso ARP	Paso 2b	5	
	Paso 2c	15	
	Paso 3	5	
	Total de la parte 2	**25**	
Parte 3: Probar la redundancia en una red conmutada	Paso 2	15	
	Paso 3	5	
	Paso 4	15	
	Paso 6b	15	
	Paso 6c	10	
	Paso 8	15	
	Total de la parte 3	**75**	
	Puntuación total	**100**	

Packet Tracer: Configuración de PVST+ (versión para el instructor)

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

Topología

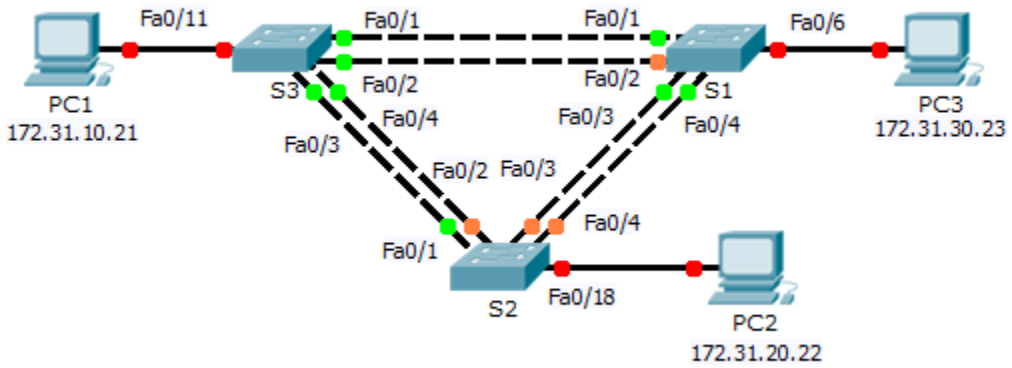


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.31.99.1	255.255.255.0	N/A
S2	VLAN 99	172.31.99.2	255.255.255.0	N/A
S3	VLAN 99	172.31.99.3	255.255.255.0	N/A
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.254
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.254
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.254

Especificaciones de la asignación de puertos de switch

Puertos	Asignaciones	Red
S1 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S3 F0/11	VLAN 10	172.17.10.0/24

Objetivos

Parte 1: configurar VLANs

Parte 2: Configurar el protocolo de árbol de expansión PVST+ y el balanceo de carga

Parte 3: Configurar PortFast y la protección BPDU

Información básica

En esta actividad, configurará redes VLAN y enlaces troncales, y examinará y configurará los puentes raíz principales y secundarios del protocolo de árbol de expansión. También optimizará la topología conmutada mediante PVST+, PortFast y la protección BPDU.

Parte 1: Configurar las VLAN

Paso 1: Habilitar los puertos de usuario en el S1, el S2 y el S3 en modo de acceso.

Consulte el diagrama de topología para determinar qué puertos de switch (**S1, S2** y **S3**) están activados para el acceso a dispositivos para usuarios finales. Estos tres puertos se configuran para el modo de acceso y se habilitan con el comando **no shutdown**.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# no shutdown

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# no shutdown

S3(config)# interface f0/11
S3(config-if)# switchport mode access
S3(config-if)# no shutdown
```

Paso 2: Crear las VLAN.

Mediante el uso del comando apropiado, cree las VLAN 10, 20, 30, 40, 50, 60, 70, 80 y 99 en todos los switches.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99

S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99
```



```
S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

Paso 3: Asigne las VLAN a los puertos de switch.

Las asignaciones de puertos se enumeran en la tabla al comienzo de la actividad. Guarde la configuración después de asignar puertos de switch a las VLAN.

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 30

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20

S3(config)# interface f0/11
S3(config-if)# switchport access vlan 10
```

Paso 4: Verifique las VLAN.

Utilice el comando **show vlan brief** en todos los switches para verificar que todas las VLAN estén registradas en la tabla de VLAN.

Paso 5: Asigne los enlaces troncales a la VLAN 99 nativa.

Utilice el comando apropiado para configurar los puertos F0/1 a F0/4 en cada switch como puertos de enlace troncal y asigne estos puertos de enlace troncal a la VLAN 99 nativa.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

Paso 6: Configure la interfaz de administración en los tres switches con una dirección.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.31.99.1 255.255.255.0
```



```
S2(config)# interface vlan99
S2(config-if)# ip address 172.31.99.2 255.255.255.0

S3(config)# interface vlan99
S3(config-if)# ip address 172.31.99.3 255.255.255.0
```

Verifique que los switches estén configurados correctamente haciendo ping entre ellos.

Parte 2: Configurar el protocolo de árbol de expansión PVST+ y el balanceo de carga

Dado que hay una instancia separada del spanning-tree para cada VLAN activa, se efectúa una elección de raíz separada para cada instancia. Si las prioridades del switch establecidas de manera predeterminada se utilizan para seleccionar la raíz, se elige la misma raíz para cada instancia del árbol de expansión, como ya hemos visto. Esto podría ocasionar un diseño inferior. Algunas razones para controlar la selección del switch raíz incluyen:

- El switch raíz es el responsable de generar las BPDU para el STP 802.1D y es el centro del tráfico de control del árbol de expansión. El switch raíz debe ser capaz de manejar esta carga adicional.
- La ubicación de la raíz define las rutas conmutadas activas en la red. Es posible que la ubicación aleatoria produzca rutas por debajo de lo óptimo. Lo ideal es que la raíz se encuentre en la capa de distribución.
- Considere la topología que se utiliza en esta actividad. De los seis enlaces troncales configurados, sólo tres transportan tráfico. Si bien esto evita los bucles, es un desperdicio de recursos. Dado que la raíz puede definirse en función de la VLAN, es posible que algunos puertos estén bloqueando elementos para una VLAN y reenviando elementos a otra. Esto se demuestra a continuación.

Paso 1: Configurar el modo STP.

Utilice el comando **spanning-tree mode** para establecer que los switches utilicen PVST como el modo STP.

```
S1(config)# spanning-tree mode pvst

S2(config)# spanning-tree mode pvst

S3(config)# spanning-tree mode pvst
```

Paso 2: Configurar el balanceo de carga del protocolo de árbol de expansión PVST+.

a. Configure el **S1** para que sea la raíz principal para las VLAN 1, 10, 30, 50 y 70. Configure el **S3** para que sea la raíz principal para las VLAN 20, 40, 60, 80 y 99. Configure el **S2** para que sea la raíz secundaria para todas las VLAN.

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary

S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary

S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

b. Verifique la configuración mediante el comando **show spanning-tree**.

Parte 3: Configurar PortFast y la protección BPDU

Paso 1: Configurar PortFast en los switches.

PortFast hace que un puerto ingrese al estado de reenvío casi de inmediato al disminuir drásticamente el tiempo de estados de escucha y aprendizaje. PortFast minimiza el tiempo que tarda en conectarse el servidor o la estación de trabajo. Configure PortFast en las interfaces del switch que están conectadas a las computadoras.

```
S1(config)# interface f0/6
S1(config-if-range)# spanning-tree portfast

S2(config)# interface f0/18
S2(config-if-range)# spanning-tree portfast

S3(config)# interface f0/11
S3(config-if-range)# spanning-tree portfast
```

Paso 2: Configurar la protección BPDU en los switches.

La mejora en la Protección STP PortFast BPDU permite que los diseñadores de red apliquen las fronteras de dominio de STP y mantengan predecible la topología activa. Los dispositivos detrás de los puertos que tienen PortFast SPT habilitado no pueden influir en la topología STP. Al recibir las BPDU, la función de protección BPDU deshabilita el puerto que tiene PortFast configurado. La protección BPDU lleva a cabo la transición del puerto al estado err-disabled, y aparece un mensaje en la consola. Configure la protección BPDU en las interfaces del switch que están conectadas a las computadoras.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable

S3(config)# interface f0/11
S3(config-if)# spanning-tree bpduguard enable
```

Paso 3: Verificar la configuración.

Utilice el comando **show running-configuration** para verificar la configuración.

Packet Tracer: Configuración de PVST+ rápido (versión para el instructor)

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

Topología

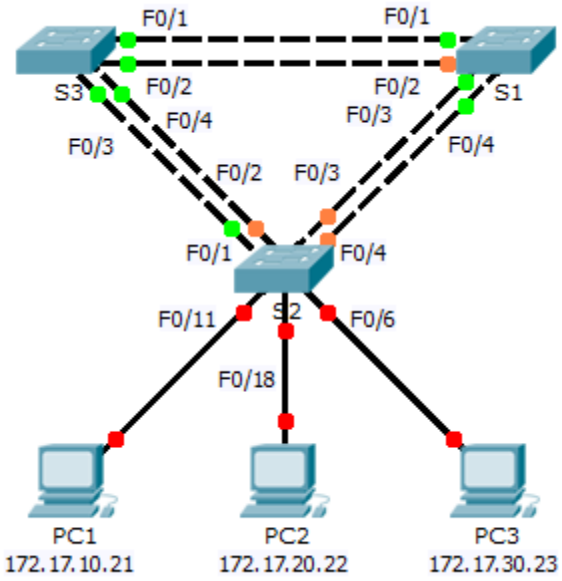


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.254
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.254

Especificaciones de la asignación de puertos de switch

Puertos	Asignaciones	Red
S2 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S2 F0/11	VLAN 10	172.17.10.0/24

Objetivos

Parte 1: configurar VLANs

Parte 2: Configurar el protocolo de árbol de expansión PVST+ rápido y el balanceo de carga

Parte 3: Configurar PortFast y la protección BPDU

Información básica

En esta actividad, configurará redes VLAN y enlaces troncales, el protocolo de árbol de expansión PVST+ rápido, los puentes raíz principales y secundarios, y examinará los resultados de la configuración. También optimizará la red al configurar PortFast y la protección BPDU en los puertos perimetrales.

Parte 1: Configurar las VLAN

Paso 1: Habilitar los puertos de usuario en el S2 en modo de acceso.

Consulte el diagrama de topología para determinar qué puertos de switch en el **S2** están activados para el acceso a dispositivos para usuarios finales. Estos tres puertos se configuran para el modo de acceso y se habilitan con el comando **no shutdown**.

```
S2(config)# interface range f0/6,f0/11,f0/18
S2(config-if-range)# switchport mode access
S2(config-fi-range)# no shutdown
```

Paso 2: Crear las VLAN.

Mediante el uso del comando apropiado, cree las VLAN 10, 20, 30, 40, 50, 60, 70, 80 y 99 en todos los switches.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99

S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99

S3(config)# vlan 10
```



```
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

Paso 3: Asigne las VLAN a los puertos de switch.

Las asignaciones de puertos se enumeran en la tabla al comienzo de la actividad. Guarde la configuración después de asignar puertos de switch a las VLAN.

```
S2(config)# interface f0/6
S2(config-if)# switchport access vlan 30
S2(config-if)# interface f0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface f0/18
S2(config-if)# switchport access vlan 20
```

Paso 4: Verifique las VLAN.

Utilice el comando **show vlan brief** en todos los switches para verificar que todas las VLAN estén registradas en la tabla de VLAN.

Paso 5: Asigne los enlaces troncales a la VLAN 99 nativa.

Utilice el comando apropiado para configurar los puertos F0/1 a F0/4 en cada switch como puertos de enlace troncal y asigne estos puertos de enlace troncal a la VLAN 99 nativa.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

Paso 6: Configure la interfaz de administración en los tres switches con una dirección.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.17.99.11 255.255.255.0

S2(config)# interface vlan99
S2(config-if)# ip address 172.17.99.12 255.255.255.0
```



```
S3(config)# interface vlan99
S3(config-if)# ip address 172.17.99.13 255.255.255.0
```

Verifique que los switches estén configurados correctamente haciendo ping entre ellos.

Parte 2: Configurar el balanceo de carga del protocolo de árbol de expansión PVST+ rápido

El protocolo de árbol de expansión rápido (RSTP; IEEE 802.1w) se puede ver como una evolución del estándar 802.1D más que como una revolución. La terminología de 802.1D sigue siendo fundamentalmente la misma. La mayoría de los parámetros no se modificaron, de modo que los usuarios familiarizados con 802.1D pueden configurar el nuevo protocolo rápidamente y sin dificultades. En la mayoría de los casos, RSTP funciona mejor que las extensiones exclusivas de Cisco sin ninguna configuración adicional. También se puede volver de 802.1w a 802.1D para interoperar con puentes antiguos por puerto.

Paso 1: Configurar el modo STP.

Utilice el comando **spanning-tree mode** para establecer que los switches utilicen PVST rápido como el modo STP.

```
S1(config)# spanning-tree mode rapid-pvst

S2(config)# spanning-tree mode rapid-pvst

S3(config)# spanning-tree mode rapid-pvst
```

Paso 2: Configurar el balanceo de carga del protocolo de árbol de expansión PVST+ rápido.

Configure el **S1** para que sea la raíz principal para las VLAN 1, 10, 30, 50 y 70. Configure el **S3** para que sea la raíz principal para las VLAN 20, 40, 60, 80 y 99. Configure el **S2** para que sea la raíz secundaria para todas las VLAN.

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary

S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary

S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

Verifique la configuración mediante el comando **show spanning-tree**.

Parte 3: Configurar PortFast y la protección BPDU

Paso 1: Configurar PortFast en el S2.

PortFast hace que un puerto ingrese al estado de reenvío casi de inmediato al disminuir drásticamente el tiempo de estados de escucha y aprendizaje. PortFast minimiza el tiempo que tarda en conectarse el servidor o la estación de trabajo. Configure PortFast en las interfaces del **S2** que están conectadas a las computadoras.

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree portfast
```


Paso 2: Configurar la protección BPDU en el S2.

La mejora en la Protección STP PortFast BPDU permite que los diseñadores de red apliquen las fronteras de dominio de STP y mantengan predecible la topología activa. Los dispositivos detrás de los puertos que tienen PortFast SPT habilitado no pueden influir en la topología STP. Al recibir las BPDU, la función de protección BPDU deshabilita el puerto que tiene PortFast configurado. La protección BPDU lleva a cabo la transición del puerto al estado err-disabled, y aparece un mensaje en la consola. Configure la protección BPDU en las interfaces del **S2** que están conectadas a las computadoras.

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree bpduguard enable
```

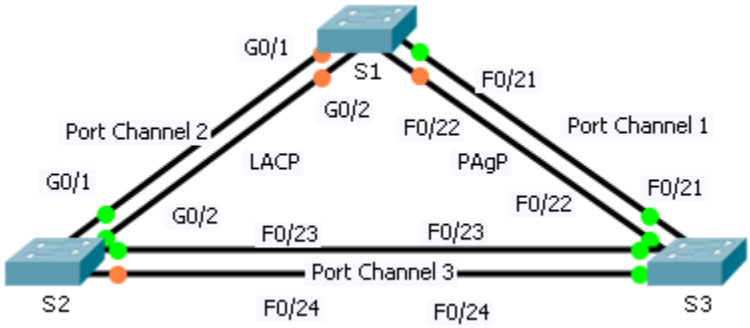
Paso 3: Verificar la configuración.

Use el comando **show run** para verificar la configuración.

Packet Tracer: Configuración de EtherChannel (versión para el instructor)

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

Topología



Objetivos

Parte 1: Configurar los parámetros básicos del switch

Parte 2: Configurar un EtherChannel con PAgP de Cisco

Parte 3: Configurar un EtherChannel LACP 802.3ad

Parte 4: Configurar un enlace EtherChannel redundante

Información básica

Se acaban de instalar tres switches. Entre los switches, hay uplinks redundantes. Por lo general, se puede utilizar solo uno de estos enlaces; de lo contrario, se podría originar un bucle de puente. Sin embargo, si se usa un solo enlace, se utiliza solo la mitad del ancho de banda disponible. EtherChannel permite agrupar hasta ocho enlaces redundantes en un único enlace lógico. En esta práctica de laboratorio, configurará el protocolo de agregación de puertos (PAgP), que es un protocolo de EtherChannel de Cisco, y el protocolo de control de agregación de enlaces (LACP), una versión de estándar abierto IEEE 802.3ad de EtherChannel.

Parte 1: Configurar los parámetros básicos del switch

Paso 1: Configurar los parámetros básicos del switch.

a. Asigne un nombre de host a cada switch según el diagrama de topología.

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

```
Switch(config)# hostname S2
```

```
Switch(config)# hostname S3
```

b. Configure todos los puertos requeridos como enlaces troncales, según las conexiones entre los dispositivos.

Nota: si los puertos están configurados con el modo dinámico automático y no establece el modo de los puertos en enlace troncal, no se forman enlaces troncales, y los enlaces continúan como puertos de acceso. El modo predeterminado en un switch 2960 es dinámico automático.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# interface range f0/21 - 22
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# end

S2(config)# interface range g0/1 - 2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# interface range f0/23 - 24
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# end

S3(config)# interface range f0/21 - 24
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# end
```

Parte 2: Configurar un EtherChannel con PAgP de Cisco

Nota: al configurar EtherChannels, se recomienda desactivar los puertos físicos que se van a agrupar en ambos dispositivos antes de configurarlos en grupos de canales. De lo contrario, la protección de configuración incorrecta de EtherChannel puede colocar estos puertos en el estado err-disabled. Se pueden volver a habilitar los puertos y los canales de puertos después de configurar EtherChannel.

Paso 1: Configurar el canal de puertos 1.

a. El primer EtherChannel creado para esta actividad agrega los puertos F0/22 y F0/21 entre el **S1** y el **S3**. Utilice el comando **show interfaces trunk** para asegurarse de que tiene un enlace troncal activo para esos dos enlaces.

```
S1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
F0/21       on           802.1q         trunking      1
F0/22       on           802.1q         trunking      1
G0/1        on           802.1q         trunking      1
G0/2        on           802.1q         trunking      1

<resultado omitido>
```

b. En ambos switches, agregue los puertos F0/21 y F0/22 al canal de puertos 1 con el comando **channel-group 1 mode desirable**. La opción **mode desirable** permite que el switch negocie activamente para formar un enlace de PAgP.

```
S1(config)# interface range f0/21 – 22
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
```



```
S3(config)# interface range f0/21 - 22
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 1 mode desirable
S3(config-if-range)# no shutdown
```

c. Configure la interfaz lógica para que se convierta en un enlace troncal ingresando primero el comando **interface port-channel** *número* y, a continuación, el comando **switchport mode trunk**. Agregue esta configuración a ambos switches.

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
```

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
```

Paso 2: Verificar el estado del canal de puertos 1.

a. Emita el comando **show etherchannel summary** para verificar que EtherChannel funcione en ambos switches. Este comando muestra el tipo de EtherChannel, los puertos utilizados y el estado de estos.

```
S1# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)          PAgP      F0/21(P)    F0/22(P)

S3# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```



```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         PAgP      F0/21(P)    F0/22(P)
```

b. Si no aparece el EtherChannel, desactive las interfaces físicas en ambos extremos del EtherChannel y vuelva a activarlas. Esto implica utilizar el comando **shutdown** en esas interfaces, seguido de un comando **no shutdown** algunos segundos más tarde.

Los comandos **show interfaces trunk** y **show spanning-tree** también muestran el canal de puertos como un único enlace lógico.

```
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1
Po1         on           802.1q         trunking      1

<resultado omitido>

S1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.436E.8494
              Cost        9
              Port        27(Port-channel 1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F313.2395
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
Po1              Root FWD 9         128.27   Shr
```


Parte 3: Configurar un EtherChannel LACP 802.3ad

Paso 1: Configurar el canal de puertos 2.

a. En el año 2000, el IEEE lanzó 802.3ad, que es una versión de estándar abierto de EtherChannel. Con los comandos anteriores, configure el enlace entre el **S1** y el **S2** como EtherChannel LACP en los puertos G0/1 y G0/2. En el **S1** debe utilizar un número de canal de puertos diferente a 1, porque ya lo utilizó en el paso anterior. Para configurar un canal de puertos como LACP, utilice el comando de configuración de interfaz **channel-group** *número* **mode active**. El modo activo indica que el switch intenta negociar activamente ese enlace como LACP, en comparación con PAgP.

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 2 mode active
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 2
S1(config-if)# switchport mode trunk

S2(config)# interface range g0/1 - 2
S2(config-if-range)# shutdwon
S2(config-if-range)# channel-group 2 mode active
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 2
S2(config-if)# switchport mode trunk
```

Paso 2: Verificar el estado del canal de puertos 2.

a. Utilice los comandos **show** del paso 2 de la parte 1 para verificar el estado del canal de puertos 2. Busque el protocolo que utiliza cada puerto.

```
S1# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
```



```
1       Po1(SU)           PAgP    Fa0/21(P)  Fa0/22(P)
2       Po2(SU)           LACP    Gig0/1(P)  Gig0/2(P)
```

Parte 4: Configurar un enlace EtherChannel redundante

Paso 1: Configurar el canal de puertos 3.

Existen varias maneras de introducir el comando **channel-group** *número* **mode**:

```
S2(config)# interface range f0/23 - 24
S2(config-if-range)# channel-group 3 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
```

a. En el switch **S2**, agregue los puertos F0/23 y F0/24 al canal de puertos 3 con el comando **channel-group 3 mode passive**. La opción **passive** indica que desea que el switch utilice LACP solamente si se detecta otro dispositivo LACP. Configure el canal de puertos 3 como interfaz de enlace troncal de forma estática.

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S2(config)# interface range f0/23 - 24
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 3 mode passive
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 3
S2(config-if)# switchport mode trunk
```

b. En el switch **S3**, agregue los puertos F0/23 y F0/24 al canal de puertos 3 con el comando **channel-group 3 mode active**. La opción **active** indica que desea que el switch utilice LACP incondicionalmente. Configure el canal de puertos 3 como interfaz de enlace troncal de forma estática.

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S3(config)# interface range f0/23 - 24
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 3 mode active
S3(config-if-range)# no shutdown
S3(config-if-range)# interface port-channel 3
S3(config-if)# switchport mode trunk
```


Paso 2: Verificar el estado del canal de puertos 3.

a. Utilice los comandos **show** del paso 2 de la parte 1 para verificar el estado del canal de puertos 3. Busque el protocolo que utiliza cada puerto.

```
S2# show etherchannel summary
<resultado omitido>
Number of channel-groups in use: 2
Number of aggregators:           2
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)           LACP   Gig0/1(P) Gig0/2(P)
3      Po3(SU)           LACP   Fa0/23(P) Fa0/24(P)
```

b. El canal de puertos 2 no funciona porque el protocolo de árbol de expansión colocó algunos puertos en el modo de bloqueo. Desafortunadamente, esos puertos eran puertos Gigabit. Para restaurar estos puertos, configure el **S1** para que sea la raíz **principal** para la VLAN 1 o establezca la prioridad en **24576**.

```
S1(config)# spanning-tree vlan 1 root primary
```

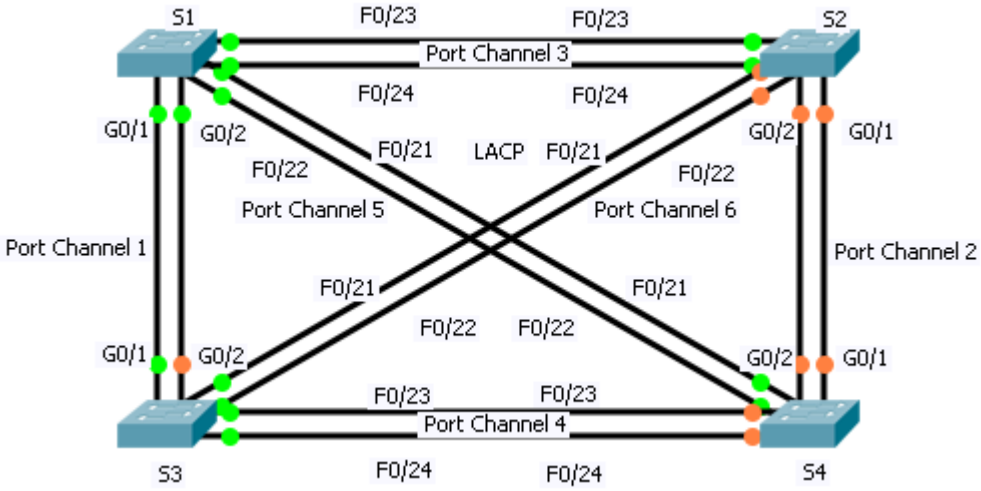
o

```
S1(config)# spanning-tree vlan 1 priority 24576
```


Packet Tracer: Resolución de problemas de EtherChannel (versión para el instructor)

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

Topología



Objetivos

Parte 1: Examinar la capa física y corregir los problemas del modo de puerto de switch

Parte 2: Identificar y corregir los problemas de asignación del canal de puertos

Parte 3: Identificar y corregir los problemas del protocolo de canal de puertos

Información básica

Recientemente, un técnico principiante configuró cuatro switches. Los usuarios se quejan de que la red funciona con lentitud y desean que usted investigue el problema.

Parte 1: Examinar la capa física y corregir los problemas del modo de puerto de switch

Parte 1: Buscar los puertos de acceso.

Examine los switches. Cuando se asignan puertos físicos a un puerto EtherChannel, actúan como si fueran uno solo. Cada par está en funcionamiento o inactivo. No se mezclan con un puerto verde y otro puerto naranja.

Parte 2: Establecer los puertos en modo de enlace troncal.

a. Verifique que todos los puertos físicos en la topología estén establecidos como enlaces troncales. Corrija cualquiera que esté en el modo de acceso.

```
S2(config)# interface range f0/21 - 24
S2(config-if-range)# switchport mode trunk
```



```
S2(config-if-range)# interface range g0/1-2
S2(config-if-range)# switchport mode trunk
```

b. Corrija cualquier puerto EtherChannel que no esté configurado en modo de enlace troncal.

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** en las interfaces de canal de puertos.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk

S2(config)# interface port-channel 2
S2(config-if)# switchport mode trunk
S2(config-if)# interface port-channel 3
S2(config-if)# switchport mode trunk
S2(config-if)# interface Port-channel 6
S2(config-if)# switchport mode trunk
```

Parte 2: Identificar y corregir los problemas de asignación del canal de puertos

Parte 1: Examinar las asignaciones del canal de puertos.

La topología ilustra los puertos físicos y las asignaciones de EtherChannel. Verifique que los switches estén configurados según lo indicado.

```
S1# show etherchannel summary
<resultado omitido>
1      Po1(SD)           LACP   Gig0/1(I) Gig0/2(I)
3      Po3(SU)           LACP   Fa0/23(P) Fa0/24(P)
5      Po5(SU)           LACP   Fa0/21(P) Fa0/22(P)

S2# show etherchannel summary
<resultado omitido>
2      Po2(SU)           LACP   Gig0/1(P) Gig0/2(P)
3      Po3(SU)           LACP   Fa0/23(P) Fa0/24(P)
6      Po6(SD)           LACP   Fa0/21(I) Fa0/22(I)

S3# show etherchannel summary
<resultado omitido>
1      Po1(SD)           PAgP   Gig0/1(I) Gig0/2(I)
4      Po4(SD)           PAgP   Fa0/23(I) Fa0/24(I)
6      Po6(SD)           PAgP   Fa0/21(I) Fa0/22(I)

S4# show etherchannel summary
<resultado omitido>
2      Po2(SU)           LACP   Gig0/1(P) Gig0/2(P)
4      Po4(SU)           LACP   Fa0/21(P) Fa0/22(P) Fa0/23(I) Fa0/24(I)
5      Po5(SD)           -
```


Parte 2: Corregir las asignaciones del canal de puertos.

Corrija cualquier puerto de switch que no esté asignado al puerto EtherChannel correcto.

```
S4(config)# interface range f0/21 - 22
S4(config-if-range)# channel-group 5 mode active
```

Parte 3: Identificar y corregir los problemas del protocolo del canal de puertos

Parte 1: Identificar los problemas del protocolo.

En el año 2000, el IEEE lanzó 802.3ad (LACP), que es una versión de estándar abierto de EtherChannel. Por razones de compatibilidad, el equipo de diseño de red decidió utilizar LACP a través de la red. Todos los puertos que participan en EtherChannel deben negociar activamente el enlace como LACP, en comparación con PAgP. Verifique que los puertos físicos estén configurados según lo indicado.

```
S3# show etherchannel summary
<resultado omitido>
1      Po1(SD)           PAgP   Gig0/1(I) Gig0/2(I)
4      Po4(SD)           PAgP   Fa0/23(I) Fa0/24(I)
6      Po6(SD)           PAgP   Fa0/21(I) Fa0/22(I)
```

Parte 2: Corregir los problemas del protocolo.

Corrija cualquier puerto de switch que no negocie mediante LACP.

```
S3(config)# interface range g0/1 - 2
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 1 mode active
S3(config-if-range)# interface range f0/21 - 22
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 6 mode active
S3(config-if-range)# interface range f0/23 - 24
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 4 mode active
```


Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

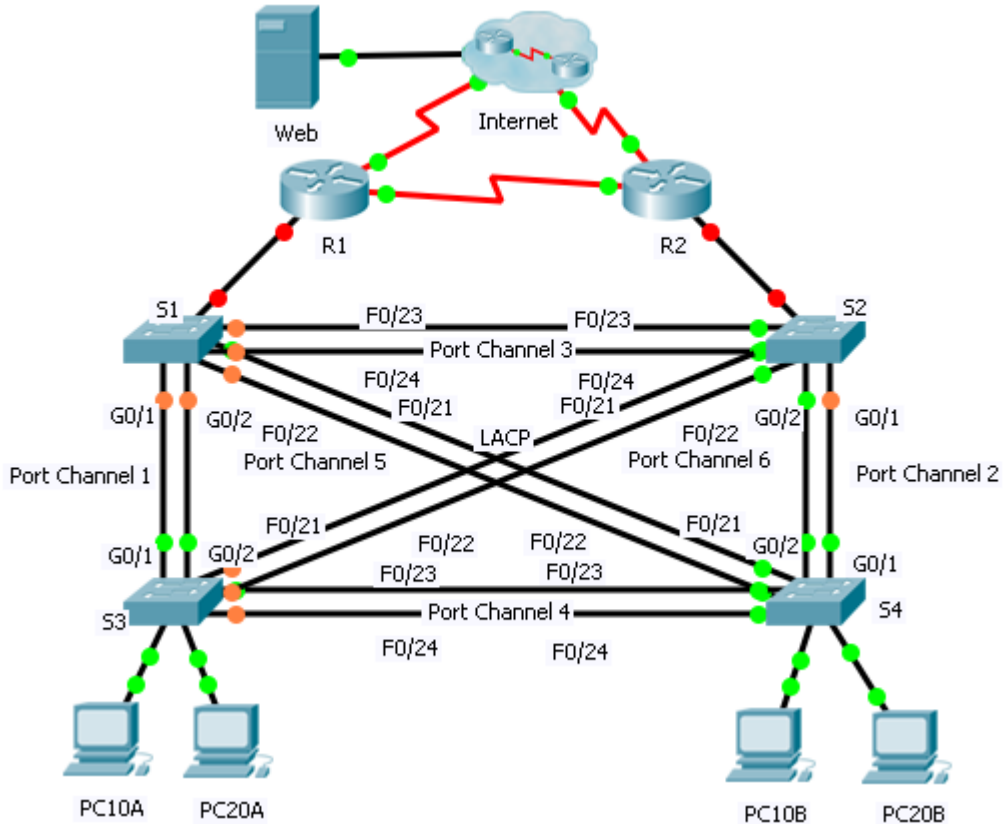


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	Asociación de VLAN
R1	G0/0.1	192.168.99.1	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.1	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.1	255.255.255.0	N/A	VLAN 20
	S0/0/0	209.165.22.222	255.255.255.224	N/A	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A	N/A
R2	G0/0.1	192.168.99.2	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.2	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.2	255.255.255.0	N/A	VLAN 20
	S0/0/0	192.168.1.2	255.255.255.0	N/A	N/A
	S0/0/1	209.165.22.190	255.255.255.224	N/A	N/A
ISP	S0/0/0	209.165.22.193	255.255.255.224	N/A	N/A
	S0/0/1	209.165.22.161	255.255.255.224	N/A	N/A
Web	NIC	64.104.13.130	255.255.255.252	64.104.13.129	N/A
PC10A	NIC	192.168.10.101	255.255.255.0	192.168.10.1	VLAN 10
PC10B	NIC	192.168.10.102	255.255.255.0	192.168.10.1	VLAN 10
PC20A	NIC	192.168.20.101	255.255.255.0	192.168.20.1	VLAN 20
PC20B	NIC	192.168.20.102	255.255.255.0	192.168.20.1	VLAN 20

Situación

En esta actividad, hay dos routers configurados para comunicarse entre sí. Usted es responsable de configurar las subinterfaces para que se comuniquen con los switches. Configurará redes VLAN, enlaces troncales y EtherChannel con PVST. Todos los dispositivos de Internet se configuraron previamente.

Requisitos

Usted es responsable de configurar los routers **R1** y **R2**, y los switches **S1**, **S2**, **S3** y **S4**.

Nota: Packet Tracer no permite asignar valores de punto inferiores a 1. Dado que esta actividad evalúa 154 elementos, no se asigna un valor de punto a todas las configuraciones. Haga clic en **Check Results** (Verificar resultados) > **Assessment Items** (Elementos de evaluación) para verificar que haya configurado correctamente los 154 elementos.

Routing entre VLAN

En el **R1** y el **R2**, habilite y configure las subinterfaces con el siguiente requisito:

- Configure la encapsulación dot1q apropiada.
- configurar VLAN 99 como VLAN nativa.
- Configure la dirección IP de la subinterfaz según la tabla de direccionamiento.

Routing

Configure OSPFv2 con los siguientes requisitos:

- Utilice la ID de proceso 1.
- Anuncie la red para cada subinterfaz.
- Deshabilite las actualizaciones OSPF para cada subinterfaz.

VLAN

- Para todos los switches, cree las VLAN 10, 20 y 99.
- Configure los siguientes puertos estáticos para el **S1** y el **S2**:
  - F0/1 a 9 como puertos de acceso en la VLAN 10.
  - F0/10 a 19 como puertos de acceso en la VLAN 20.
  - F0/20 a F24 y G0/1 a 0/2 como enlace troncal nativo para la VLAN 99.
- Configure los siguientes puertos estáticos para el **S3** y **S4**:
  - F0/1 a 9 como puertos de acceso en la VLAN 10.
  - F0/10 a 20 como puertos de acceso en la VLAN 20.
  - F0/21 a F24 y G0/1 a 0/2 como enlace troncal nativo para la VLAN 99.

EtherChannels

- Todos los EtherChannels se configuran como LACP.
- Todos los EtherChannels se configuran de forma estática como enlace troncal nativo para la VLAN 99.
- Utilice la siguiente tabla para configurar los puertos de switch apropiados para formar EtherChannels:

Canal de puertos	Dispositivo: puertos	Dispositivo: puertos
1	S1: G0/1 – 2	S3: G0/1 – 2
2	S2: G0/1 – 2	S4: G0/1 – 2
3	S1: F0/23 – 24	S2: F0/23 – 24
4	S3: F0/23 – 24	S4: F0/23 – 24
5	S1: F0/21 – 22	S4: F0/21 – 22
6	S2: F0/21 – 22	S3: F0/21 - 22

Árbol de expansión

- Configure el modo de árbol de expansión rápido por VLAN para todos los switches.
- Configure las prioridades del árbol de expansión según la siguiente tabla:

Dispositivo	Prioridad de VLAN 10	Prioridad de VLAN 20
S1	4096	8192
S2	8192	4096
S3	32768	32768
S4	32768	32768

Nota para el instructor: Packet Tracer 6.0.1 no califica el comando **switchport mode trunk** ni el comando switchport trunk native vlan en las interfaces de canal de puertos.

Conectividad

- Todas las computadoras deben poder hacer ping a **Web** y a las otras computadoras.

Respuestas

Router R1

```
!R1
enable
configure t
interface GigabitEthernet0/0
 no shut
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 99 native
 ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
router ospf 1
 passive-interface GigabitEthernet0/0.1
 passive-interface GigabitEthernet0/0.10
 passive-interface GigabitEthernet0/0.20
 network 192.168.99.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
end
copy run start
```

R2 del router

```
!R2
enable
```



```
configure t
!
interface GigabitEthernet0/0
 no shut
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 99 native
 ip address 192.168.99.2 255.255.255.0
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.2 255.255.255.0
!
router ospf 1
 passive-interface GigabitEthernet0/0.1
 passive-interface GigabitEthernet0/0.10
 passive-interface GigabitEthernet0/0.20
 network 192.168.99.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
end
copy run start
```

Switch S1

```
!S1
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
 switchport mode access
 switchport access vlan 10
inte range f0/10 - 19
 switchport mode access
 switchport access vlan 20
interface range f0/20 - 24, g0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
!
interface range g0/1 - 2
 channel-group 1 mode active
interface range f0/21 - 22
 channel-group 5 mode active
interface range f0/23 - 24
```



```
 channel-group 3 mode active
!
interface po 1
 switchport mode trunk
 switchport trunk native vlan 99
interface po 3
 switchport mode trunk
 switchport trunk native vlan 99
interface po 5
 switchport mode trunk
 switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 8192
end
copy run start
```

Switch S2

```
!S2
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
 switchport mode access
 switchport access vlan 10
inte range f0/10 - 19
 switchport mode access
 switchport access vlan 20
inte range f0/20 - 24, g0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
!
interface range g0/1 - 2
 channel-group 2 mode active
interface range f0/21 - 22
 channel-group 6 mode active
interface range f0/23 - 24
 channel-group 3 mode active
!
interface po 2
 switchport mode trunk
 switchport trunk native vlan 99
interface po 3
 switchport mode trunk
 switchport trunk native vlan 99
interface po 6
```



```
 switchport mode trunk
 switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 8192
spanning-tree vlan 20 priority 4096
end
copy run start
```

Switch S3

```
!S3
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
 switchport mode access
 switchport access vlan 10
inte range f0/10 - 20
 switchport mode access
 switchport access vlan 20
inte range f0/21 - 24, g0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
!
interface range g0/1 - 2
 channel-group 1 mode active
interface range f0/21 - 22
 channel-group 6 mode active
interface range f0/23 - 24
 channel-group 4 mode active
!
interface po 1
 switchport mode trunk
 switchport trunk native vlan 99
interface po 4
 switchport mode trunk
 switchport trunk native vlan 99
interface po 6
 switchport mode trunk
 switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 32768
spanning-tree vlan 20 priority 32768
end
copy run start
```


Switch S4

```
!S4
enable
configure t
vlan 10
vlan 20
vlan 99
interface range f0/1 - 9
 switchport mode access
 switchport access vlan 10
inte range f0/10 - 20
 switchport mode access
 switchport access vlan 20
inte range f0/21 - 24, g0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
!
interface range g0/1 - 2
 channel-group 2 mode active
interface range f0/21 - 22
 channel-group 5 mode active
interface range f0/23 - 24
 channel-group 4 mode active
interface po 2
 switchport mode trunk
 switchport trunk native vlan 99
interface po 4
 switchport mode trunk
 switchport trunk native vlan 99
interface po 5
 switchport mode trunk
 switchport trunk native vlan 99
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10 priority 32768
spanning-tree vlan 20 priority 32768
end
copy run start
```


Packet Tracer: Configuración del acceso a una LAN inalámbrica (versión para el instructor)

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

Topología

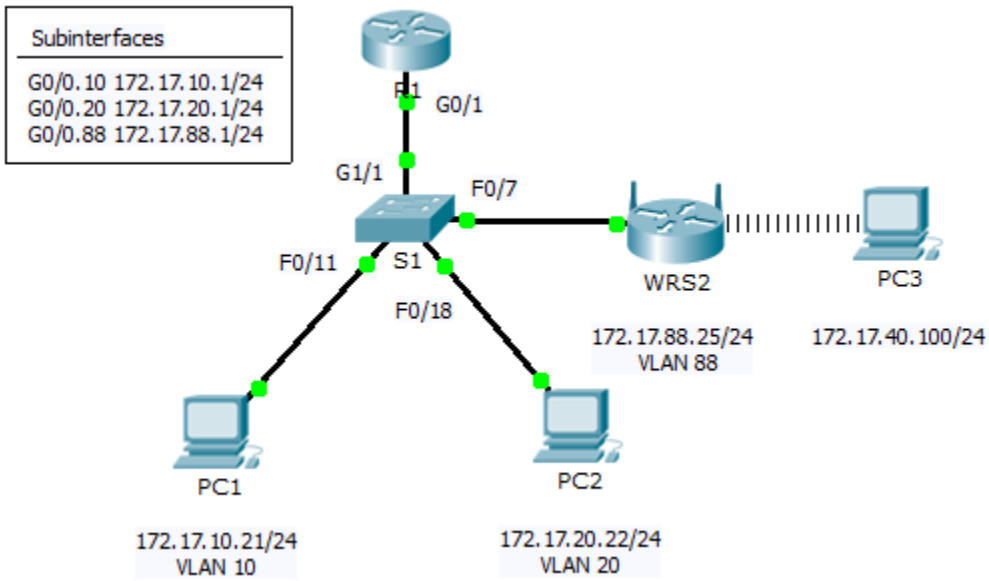


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.20	172.17.20.1	255.255.255.0	N/A
	G0/0.88	172.17.88.1	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
WRS2	NIC	172.17.88.25	255.255.255.0	172.17.88.1

Objetivos

Parte 1: Configurar un router inalámbrico

Parte 2: Configurar un cliente inalámbrico

Parte 3: verificar conectividad

Situación

En esta actividad, se configurará un router inalámbrico Linksys de manera que permita el acceso remoto desde equipos PC, además de la conectividad inalámbrica con seguridad WPA2. Configurará la conectividad inalámbrica de las computadoras de forma manual mediante la introducción del SSID y la contraseña del router Linksys.

Parte 1: Configuración de un router inalámbrico

Paso 1: Conectar la interfaz de Internet de WRS2 al S1.

Conecte la interfaz de Internet **WRS2** a la interfaz F0/7 de **S1**.

Paso 2: Configurar el tipo de conexión a Internet.

a. Haga clic en **WRS2 >** ficha **GUI**.

b. Establezca el **Internet Connection type** (Tipo de conexión a Internet) en **Static IP** (IP estático).

c. Configure el direccionamiento IP según la tabla de direccionamiento.

Paso 3: Establecer la configuración de la red.

a. Desplácese hasta **Network Setup** (Configuración de red). Para la opción **Router IP** (IP del router), establezca la dirección IP **172.17.40.1** y la máscara de subred **255.255.255.0**.

b. Habilite el servidor de DHCP.

c. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**.

Paso 4: Configurar el acceso y la seguridad inalámbricos.

a. En la parte superior de la ventana, haga clic en **Wireless** (Red inalámbrica). Establezca el **Network Mode** (Modo de red) en **Wireless-N Only** (Solo Wireless-N) y cambie el SSID a **WRS_LAN**.

b. Deshabilite la **SSID Broadcast** (Difusión del SSID) y haga clic en **Save Settings** (Guardar configuración).

c. Haga clic en la opción **Wireless Security** (Seguridad inalámbrica).

d. Cambie el **Security Mode** (Modo de seguridad) de **Disabled** (Deshabilitado) a **WPA2 Personal**.

e. Configure **cisco123** como frase de contraseña.

f. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**.

Parte 2: Configuración de un cliente inalámbrico

Paso 1: Configurar la PC3 para obtener conectividad inalámbrica.

Dado que la difusión del SSID está deshabilitada, debe configurar manualmente la **PC3** con el SSID y la frase de contraseña correctos a fin de establecer una conexión con el router.

a. Haga clic en **PC3** > **Desktop** (Escritorio) > **PC Wireless** (Computadora inalámbrica)

b. Haga clic en la ficha **Profiles** (Perfiles).

c. Haga clic en **New** (Nuevo).

d. Asigne el nombre **Wireless Access** al nuevo perfil.

e. En la siguiente pantalla, haga clic en **Advanced Setup** (Configuración avanzada). A continuación, introduzca manualmente el SSID **WRS_LAN** en **Wireless Network Name** (Nombre de red inalámbrica). Haga clic en **Next** (Siguiente).

f. Elija **Obtain network settings automatically (DHCP)** (Obtener la configuración de red de forma automática [DHCP]) como configuración de red y, a continuación, haga clic en **Next** (Siguiente).

g. En **Wireless Security** (Seguridad inalámbrica), seleccione **WPA2-Personal** como método de cifrado y haga clic en **Next**.

h. Introduzca la frase de contraseña **cisco123** y haga clic en **Next**.

i. Haga clic en **Save** (Guardar) y, a continuación, haga clic en **Connect to Network** (Conectar a la red).

Paso 2: Verificar la configuración de la conectividad inalámbrica y el direccionamiento IP de la PC3.

Los indicadores **Signal Strength** (Intensidad de la señal) y **Link Quality** (Calidad del enlace) deben mostrar que la señal es intensa.

Haga clic en **More Information** (Más información) para ver los detalles de conexión, incluida la información de direccionamiento IP.

Cierre la ventana de configuración **PC Wireless**.

Parte 3: Verificar la conectividad

Todas las PC debe tener conectividad entre ellas.

Nota para el instructor: no hay configuraciones del IOS para esta actividad. Use la contraseña **PT_ccna5** para acceder al asistente de la actividad y ver la red de respuestas.

Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

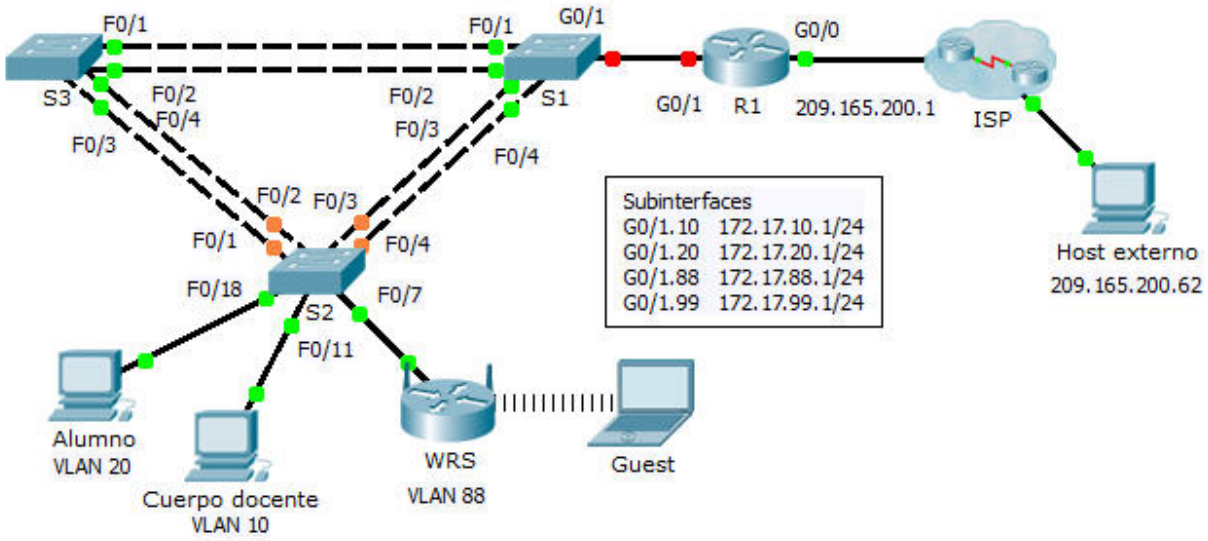


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	209.165.200.1	255.255.255.224	N/A
	G0/1.10	172.17.10.1	255.255.255.0	N/A
	G0/1.20	172.17.20.1	255.255.255.0	N/A
	G0/1.88	172.17.88.1	255.255.255.0	N/A
	G0/1.99	172.17.99.1	255.255.255.0	N/A
S2	VLAN 99	172.17.99.32	255.255.255.0	172.17.99.1
WRS	Internet	DHCP Assigned	DHCP Assigned	DHCP Assigned
	LAN	172.17.40.1	255.255.255.0	N/A

Situación

En esta actividad del desafío, configurará las VLAN y el routing entre VLAN, DHCP, y PVST+ rápido. También se requiere que configure la seguridad inalámbrica en un router Linksys para obtener conectividad inalámbrica. Al final de la actividad, las computadoras no podrán hacer ping entre sí, pero deberán poder hacer ping al host externo.

Requisitos

Configuraciones de la R1

- Habilite y configure las subinterfaces con los siguientes requisitos:
  - Configure el direccionamiento IP de las subinterfaces según la tabla de direccionamiento.
  - Configure la encapsulación dot1q apropiada.
  - configurar VLAN 99 como VLAN nativa.
- Configure pools de DHCP para las VLAN 10, 20 y 88 con los siguientes requisitos:
  - Denomine los pools de DHCP **VLAN10**, **VLAN20** y **VLAN88**.
  - Establezca el router predeterminado dentro de cada pool como la dirección de subinterfaz.
  - Excluya las primeras 20 direcciones para la VLAN 10.
  - Excluya las primeras 20 direcciones para la VLAN 20.
  - Excluya las primeras 10 direcciones para la VLAN 88.

Configuraciones de los switches

- Configure PVST+ rápido en todos los switches.
- Configure el direccionamiento IP en el **S2** según la tabla de direccionamiento.
- Configure el gateway predeterminado en el **S2**.
- La mayoría de las VLAN ya están configuradas. Cree una nueva VLAN 999 en el **S2** y asígnele el nombre **Blackhole**.
- Configure los siguientes puertos estáticos para el **S2**:
  - F0/1 a 4 como puertos de enlace troncal y como enlace troncal nativo para la VLAN 99.
  - F0/7 como puerto de acceso en la VLAN 88.
  - F0/18 como puerto de acceso en la VLAN 20.
  - F0/11 como puerto de acceso en la VLAN 10.
  - Desactive todos los puertos sin utilizar y asígnelos como puertos de acceso en la VLAN 999.

Configuraciones WRS

- Configure **Internet Setup** (Configuración de Internet) para recibir el direccionamiento IP del R1. Es posible que deba ir a la ficha **Status** (Estado) para liberar y renovar el direccionamiento IP. Asegúrese de que **WRS** reciba el direccionamiento IP completo.
- Configure la **Network Setup** (Configuración de red) según la tabla de direccionamiento, de modo que los dispositivos de usuarios invitados reciban el direccionamiento IP.
- Establezca la configuración inalámbrica.
  - Establezca el modo de red en **Wireless N-only** (Solo wireless N).
  - Cambie el nombre del SSID a **WRS_Guest** y deshabilite la transmisión del SSID.
- Configure la seguridad inalámbrica. Establezca el tipo de autenticación en **WPA2 Personal** y configure la frase **guestuser** como frase de contraseña.

Configuraciones PC

- Verifique que las computadoras de **Students** (Estudiantes) y **Faculty** (Cuerpo docente) reciban el direccionamiento completo del **R1**.
- Configure **Guest** (Invitado) para que acceda a la LAN inalámbrica.

- Verifique que **Guest** haya recibido el direccionamiento completo.
- Verifique la conectividad.

Respuestas

```
!!!!!!R1
enable
config t
interface g0/1
 no shutdown
interface g0/1.10
 encapsulation dot 10
 ip address 172.17.10.1 255.255.255.0
interface g0/1.20
 encapsulation dot 20
 ip address 172.17.20.1 255.255.255.0
interface g0/1.88
 encapsulation dot 88
 ip address 172.17.88.1 255.255.255.0
interface g0/1.99
 encapsulation dot 99 native
 ip address 172.17.99.1 255.255.255.0
ip dhcp excluded 172.17.10.1 172.17.10.20
ip dhcp pool VLAN10
 network 172.17.10.0 255.255.255.0
 default-router 172.17.10.1
ip dhcp excluded 172.17.20.1 172.17.20.20
ip dhcp pool VLAN20
 network 172.17.20.0 255.255.255.0
 default-router 172.17.20.1
ip dhcp excluded 172.17.88.1 172.17.88.10
ip dhcp pool VLAN88
 network 172.17.88.0 255.255.255.0
 default-router 172.17.88.1
end
copy run start

!!!!!!S2
enable
configure t
interface vlan 99
 ip address 172.17.99.32 255.255.255.0
ip default-gateway 172.17.99.1
spanning-tree mode rapid-pvst
vlan 999
 name Blackhole
interface range f0/1-4
 switchport mode trunk
 switchport trunk native vlan 99
interface range f0/5-24,g0/1-2
```



```
 switchport mode access
 switchport access vlan 999
 shutdown
interface f0/7
 no shutdown
 switchport access vlan 88
interface f0/18
 no shutdown
 switchport access vlan 20
interface f0/11
 no shutdown
 switchport access vlan 10
end
copy run start
```


Packet Tracer: Determinación del DR y el BDR (versión para el instructor)

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

Topología

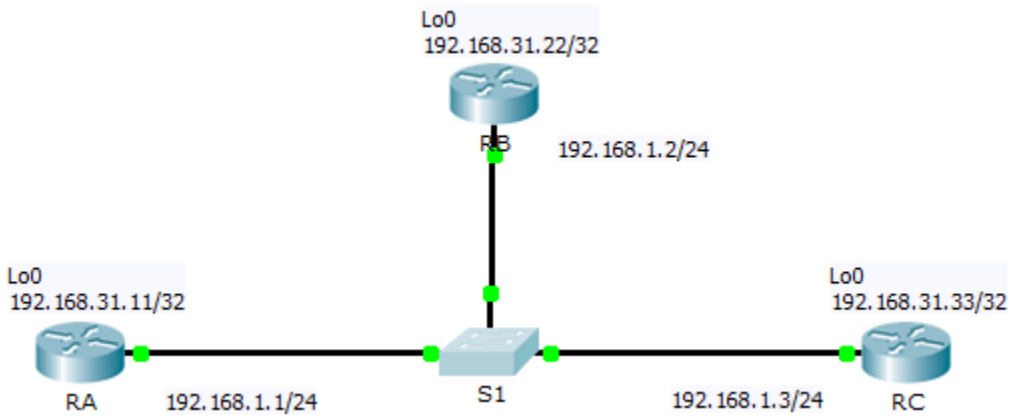


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred
RA	G0/0	192.168.1.1	255.255.255.0
	Lo0	192.168.31.11	255.255.255.255
RB	G0/0	192.168.1.2	255.255.255.0
	Lo0	192.168.31.22	255.255.255.255
RC	G0/0	192.168.1.3	255.255.255.0
	Lo0	192.168.31.33	255.255.255.255

Objetivos

Parte 1: Examinar las funciones cambiantes del DR y el BDR

Parte 2: Modificar la prioridad OSPF y forzar las elecciones

Situación

En esta actividad, examinará las funciones del DR y el BDR, y observará cómo estas cambian cuando se modifica la red. A continuación, modificará la prioridad para controlar las funciones y forzará una nueva elección. Por último, verificará que los routers cumplan las funciones deseadas.

Parte 1: Examinar las funciones cambiantes del DR y el BDR

Paso 1: Esperar hasta que las luces de enlace de color ámbar cambien a color verde.

Cuando abra por primera vez el archivo en Packet Tracer, es posible que advierta que las luces de enlace que corresponden al switch son de color ámbar. Estas luces de enlace permanecerán de color ámbar durante 50 segundos mientras el switch se asegura de que uno de los routers no es otro switch. También puede hacer clic en **Fast Forward Time** (Adelantar el tiempo) para omitir este proceso.

Paso 2: Verificar los estados actuales de los vecinos OSPF.

a. Utilice el comando correspondiente en cada router para examinar el DR y el BDR actuales.

b. ¿Qué router es el DR? RC

c. ¿Qué router es el BDR? RB

Paso 3: Activar la depuración de adyacencias OSPF IP.

a. Puede controlar el proceso de elección del DR y el BDR con un comando **debug**. En el **RA** y el **RB**, introduzca el siguiente comando.

```
RA# debug ip ospf adj
RB# debug ip ospf adj
```

Paso 4: Deshabilitar la interfaz Gigabit Ethernet 0/0 en el RC.

a. Deshabilite el enlace entre el **RC** y el switch para provocar que las funciones cambien.

b. Espere unos 30 segundos a que los temporizadores de tiempo muerto caduquen en el **RA** y el **RB**. Según el resultado de debug, ¿cuál es el router que se eligió como DR y cuál como BDR? El RB ahora es el DR, y el RA ahora es el BDR.

Paso 5: Restaurar la interfaz Gigabit Ethernet 0/0 en el RC.

a. Vuelva a habilitar el enlace entre el **RC** y el switch.

b. Espere hasta que se produzcan las nuevas elecciones de DR/BDR. ¿Cambiaron las funciones del DR y el BDR? ¿Por qué? ¿Por qué no? No, las funciones no cambiaron porque el DR y el BDR actuales siguen activos. Un router que se conecta con una ID de router más alta no cumple la función de DR hasta que este falla.

Paso 6: Deshabilitar la interfaz Gigabit Ethernet 0/0 en el RB.

a. Deshabilite el enlace entre el **RB** y el switch para hacer que las funciones cambien.

b. Espere unos 30 segundos a que los temporizadores de espera caduquen en el **RA** y el **RC**. Según el resultado de debug en el **RA**, ¿cuál es el router que se eligió como DR y cuál como BDR? El RA ahora es el DR, y el RC ahora es el BDR.

Paso 7: Restaurar la interfaz Gigabit Ethernet 0/0 en el RB.

a. Vuelva a habilitar el enlace entre el **RB** y el switch.

b. Espere hasta que se produzcan las nuevas elecciones de DR/BDR. ¿Cambiaron las funciones del DR y el BDR? ¿Por qué? ¿Por qué no? No, las funciones no cambiaron porque el DR y el BDR actuales siguen activos. Un router que se conecta con una ID de router más alta no cumple la función de DR hasta que este falla.

Paso 8: Desactivar la depuración.

Introduzca el comando **undebug all** en el **RA** y el **RB** para deshabilitar la depuración.

Parte 2: Modificar la prioridad OSPF y forzar las elecciones

Paso 1: Configurar las prioridades OSPF en cada router.

Para cambiar el DR y el DBR, configure el puerto Gigabit Ethernet 0/0 de cada router con las siguientes prioridades de interfaz OSPF:

- **RA**: 200
- **RB**: 100
- **RC:** 1 (esta es la prioridad predeterminada)

Paso 2: Volver a cargar el switch para forzar una elección.

Nota: también se puede utilizar el comando **clear ip ospf process** en los routers para restablecer el proceso OSPF.

Paso 3: Verificar si las elecciones del DR y el BDR se realizaron correctamente.

a. Espere el tiempo suficiente para que OSPF converja y se lleve a cabo la elección del DR/BDR. Esto puede tomar unos minutos. Puede hacer clic en **Fast Forward Time** para acelerar el proceso.

b. Según el resultado de un comando apropiado, ¿qué router es el DR actual y cuál el BDR? El RA ahora es el DR, y el RB ahora es el BDR.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar las funciones cambiantes del DR y el BDR	Paso 2b	10	
	Paso 2c	10	
	Paso 4b	10	
	Paso 5b	10	
	Paso 6b	10	
	Paso 7b	10	
Total de la parte 1		**60**	
Parte 2: Modificar la prioridad OSPF y forzar las elecciones	Paso 3b	10	
Total de la parte 2		**10**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

Packet Tracer: Propagación de una ruta predeterminada en OSPFv2 (versión para el instructor)

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

Topología

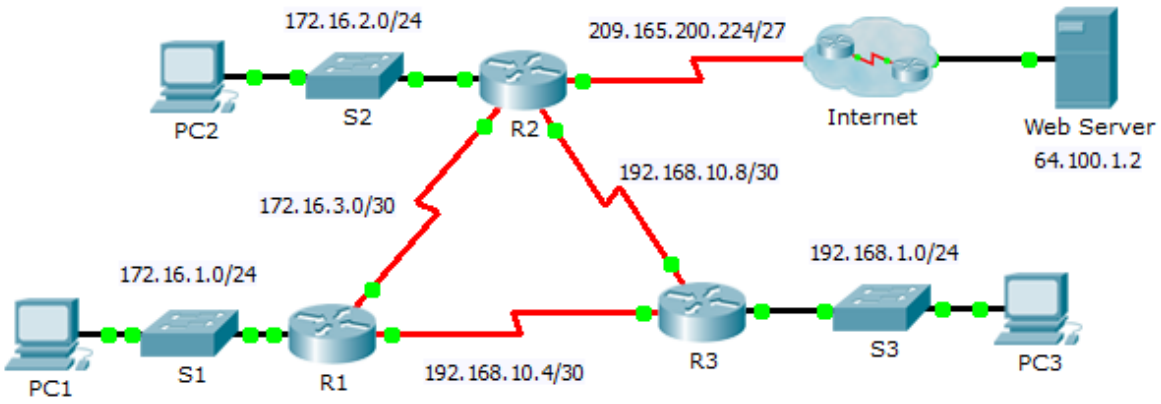


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv4	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
	S0/1/0	209.165.200.225	255.255.255.224	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: Propagar una ruta predeterminada

Parte 2: verificar conectividad

Información básica

En esta actividad, configurará una ruta predeterminada IPv4 a Internet y propagará esa ruta predeterminada a otros routers OSPF. A continuación, verificará que la ruta predeterminada esté en las tablas de routing descendente y que los hosts puedan acceder a un servidor web en Internet.

Parte 1: Propagar una ruta predeterminada

Paso 1: Configurar una ruta predeterminada en el R2.

Configure el **R2** con una ruta predeterminada conectada directamente a Internet.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

Paso 2: Propagar la ruta en OSPF.

Configure OSPF para propagar la ruta predeterminada en las actualizaciones de routing OSPF.

```
R2(config-router)# default-information originate
```

Paso 3: Examinar las tablas de routing del R1 y el R3.

Examine las tablas de routing del **R1** y el **R3** para verificar que se haya propagado la ruta.

```
R1> show ip route
<resultado omitido>
O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:08, Serial0/0/0
!------------------
R3> show ip route
<resultado omitido>
O*E2 0.0.0.0/0 [110/1] via 192.168.10.9, 00:08:15, Serial0/0/1
```

Parte 2: Verificar la conectividad

Verifique que la **PC1**, la **PC2** y la **PC3** puedan hacer ping al servidor web.

Packet Tracer: Configuración de las características avanzadas de OSPF (versión para el instructor)

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

Topología

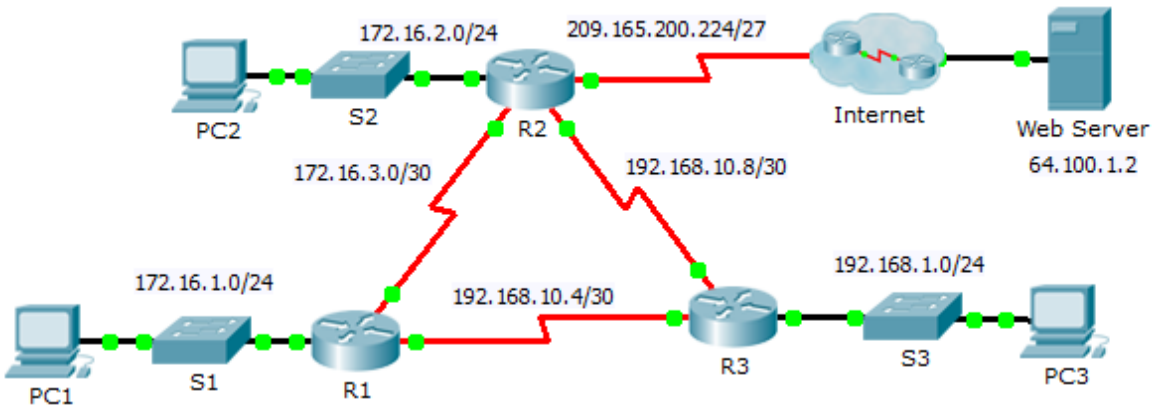


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv4	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
	S0/1/0	209.165.200.225	255.255.255.224	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: Modificar la configuración predeterminada de OSPF

Parte 2: verificar conectividad

Situación

En esta actividad, ya se configuró OSPF, y todas las terminales actualmente tienen plena conectividad. Modificará la configuración predeterminada de routing OSPF mediante la modificación de los temporizadores de saludo y muerto, el ajuste del ancho de banda de un enlace y la habilitación de la autenticación de OSPF. A continuación, verificará que se haya restaurado la plena conectividad para todas las terminales.

Parte 1: Modificar la configuración predeterminada de OSPF

Paso 1: Probar la conectividad entre todas las terminales.

Antes de modificar la configuración OSPF, verifique que todas las computadoras puedan hacer ping al servidor web y entre sí.

Paso 2: Ajustar los temporizadores de saludo y tiempo muerto entre el R1 y el R2.

a. Introduzca los siguientes comandos en el **R1**.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf hello-interval 15
R1(config-if)# ip ospf dead-interval 60
```

b. Después de un breve período, la conexión OSPF con el **R2** falla. Ambos extremos de la conexión deben tener los mismos temporizadores para que se mantenga la adyacencia. Ajuste los temporizadores en el **R2**.

Paso 3: Ajustar la configuración del ancho de banda en el R1.

a. Rastree la ruta entre la **PC1** y el servidor web ubicado en 64.100.1.2. Observe que la ruta de la **PC1** a 64.100.1.2 se enruta a través del **R2**. OSPF prefiere la ruta de menor costo.

b. En la interfaz Serial 0/0/0 del **R1**, establezca el ancho de banda en 64 Kb/s. Esto no modifica la velocidad real del puerto, solo la métrica que utiliza el proceso OSPF en el **R1** para calcular las mejores rutas.

```
R1(config-if)# bandwidth 64
```

c. Rastree la ruta entre la **PC1** y el servidor web ubicado en 64.100.1.2. Observe que la ruta de la **PC1** a 64.100.1.2 se redirige a través del **R3**. OSPF prefiere la ruta de menor costo.

Paso 4: Habilitar la autenticación de OSPF en todas las interfaces seriales.

a. Utilice los siguientes comandos para configurar la autenticación entre el **R1** y el **R2**.

Nota: el texto de la clave **R1-R2** distingue mayúsculas de minúsculas.

```
R1(config-router)# area 0 authentication message-digest
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 R1-R2
```

b. Una vez que caduca el intervalo muerto, se pierde la adyacencia de vecino entre el **R1** y el **R2**. Repita los comandos de autenticación en el **R2**.

c. Utilice el siguiente comando para configurar la autenticación en el **R1** para el enlace que comparte con el **R3**.

```
R1(config-if)# ip ospf message-digest-key 1 md5 R1-R3
```

d. Complete la configuración de autenticación necesaria para restaurar la plena conectividad. La contraseña para el enlace entre el **R2** y el **R3** es **R2-R3**.

e. Verifique que funcione la autenticación entre cada router.

```
R1# show ip ospf interface
Message digest authentication enabled
```

Parte 2: Verificar la conectividad

Verifique que todas las computadoras puedan hacer ping al servidor web y entre sí.

Packet Tracer: Resolución de problemas de OSPFv2 de área única (versión para el instructor)

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

Topología

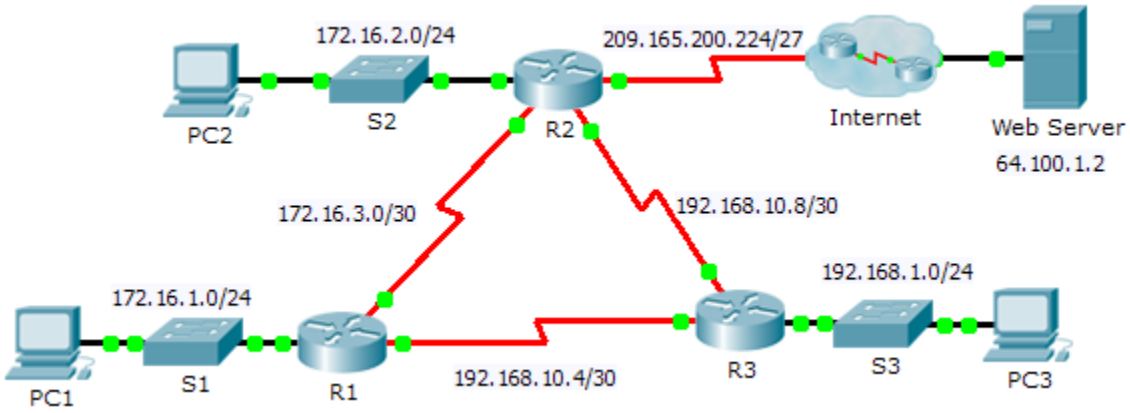


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	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
	S0/1/0	209.165.200.225	255.255.255.224	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

Situación

En esta actividad, resolverá problemas de routing OSPF mediante los comandos **ping** y **show** para identificar errores en la configuración de red. A continuación, registrará los errores que detecte e implementará una solución apropiada. Por último, verificará que se haya restaurado la conectividad de extremo a extremo.

Proceso de resolución de problemas

1. Utilice los comandos de prueba para detectar problemas de conectividad en la red y registre el problema en la tabla de documentación.
2. Utilice los comandos de verificación para determinar el origen del problema e idear una solución apropiada. Documente la solución propuesta en la tabla de documentación.
3. Implemente las soluciones de a una por vez y verifique si el problema se resolvió. Indique el estado de la resolución en la tabla de documentación.
4. Si el problema no se resolvió, es posible que primero deba deshacer la solución implementada antes de volver al paso 2.
5. Una vez que se hayan resuelto todos los problemas identificados, pruebe la conectividad de extremo a extremo.

Tabla de documentación

Dispositivo	Problema identificado	Solución propuesta	¿Se resolvió?
R1	No forma una relación de vecino con el R3.	Eliminar la instrucción network 172.16.10.4 0.0.0.3 area 0 y reemplazarla con network 192.168.10.4 0.0.0.3 area 0.	
R2	No propaga la ruta predeterminada.	Configurar OSPF con el comando **default-information originate**.	
R3	No forma una relación de vecino con el R2.	Eliminar el comando hello-interval en la interfaz S0/0/1 del R3.	

Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

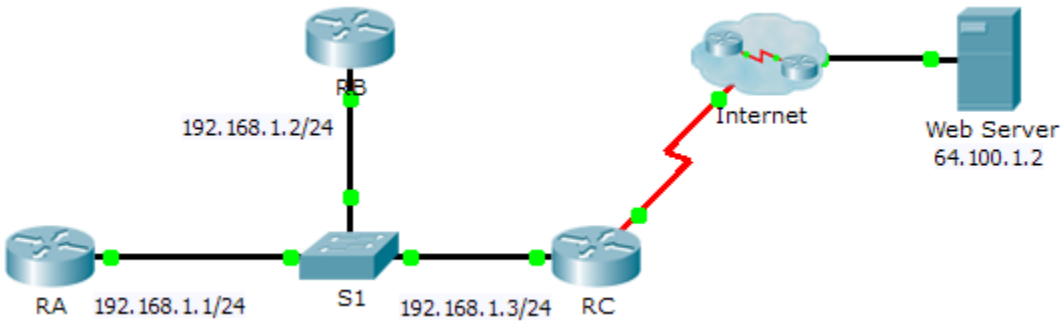


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred
RA	G0/0	192.168.1.1	255.255.255.0
RB	G0/0	192.168.1.2	255.255.255.0
RC	G0/0	192.168.1.3	255.255.255.0
	S0/0/0	209.165.200.225	255.255.255.252

Situación

En este desafío de integración de habilidades, debe concentrarse en las configuraciones avanzadas de OSPFv2. Ya se configuró el direccionamiento IP para todos los dispositivos. Configurará el routing OSPFv2 con interfaces pasivas y la propagación de rutas predeterminadas. Modificará la configuración OSPFv2 mediante el ajuste de los temporizadores y el establecimiento de la autenticación MD5. Por último, verificará las configuraciones y probará la conectividad entre las terminales.

Requisitos

- Utilice los siguientes requisitos para configurar el routing OSPFv2 en el **RA** y el **RB**:
  - Requisitos de routing OSPFv2:
    - ID de proceso 1
    - Dirección de red para cada interfaz
    - Habilitar la autenticación para el área 0
  - Prioridad OSPF establecida en 150 en la interfaz LAN del **RA**
  - Prioridad OSPF establecida en 100 en la interfaz LAN del **RB**
  - ID de la clave de autenticación MD5 de OSPF “1” y clave MD5 “cisco” en las interfaces LAN del RA y el RB

  - Establecer el intervalo de saludo en 5
  - Establecer el intervalo muerto en 20
- Utilice los siguientes requisitos para configurar el routing OSPFv2 del **RC**:
  - Requisitos de routing OSPFv2:
    ID de proceso 1
    Dirección de red para la interfaz LAN
    Habilitar la autenticación para el área 0
    Establecer todas las interfaces como pasivas de manera predeterminada, permitir las actualizaciones OSPF en la LAN activa
    Configurar el router para que distribuya las rutas predeterminadas
  - Configurar una ruta predeterminada conectada directamente a Internet
  - Prioridad OSPF establecida en 50 en la interfaz LAN
  - ID de la clave de autenticación MD5 de OSPF “1” y clave MD5 “cisco” en la interfaz LAN del **RC**
  - Establecer el intervalo de saludo en 5
  - Establecer el intervalo muerto en 20

Nota: emita el comando **clear ip ospf process** en el **RC** si la ruta predeterminada no se propaga.

- Verificación de configuraciones y prueba de conectividad
  - Deben haberse establecido los vecinos OSPF, y las tablas de routing deben estar completas.
  - El **RA** debe ser el DR, y el **RB** debe ser el BDR.
  - Los tres routers deben poder hacer ping al servidor web.

Modelos de respuestas

```
!----------------------
Router RA
!----------------------
en
conf t
interface GigabitEthernet0/0
 ip ospf message-digest 1 md5 cisco
 ip ospf hello-interval 5
 ip ospf dead-interval 20
 ip ospf priority 150
router ospf 1
 area 0 authentication message-digest
 network 192.168.1.0 0.0.0.255 area 0
end

!----------------------
```



```
Router RB
!----------------------
en
conf t
interface GigabitEthernet0/0
 ip ospf message-digest 1 md5 cisco
 ip ospf hello-interval 5
 ip ospf dead-interval 20
 ip ospf priority 100
router ospf 1
 area 0 authentication message-digest
 network 192.168.1.0 0.0.0.255 area 0
end

!----------------------
Router RC
!----------------------
en
conf t
interface GigabitEthernet0/0
 ip ospf message-digest 1 md5 cisco
 ip ospf hello-interval 5
 ip ospf dead-interval 20
 ip ospf priority 50
router ospf 1
 passive-interface default
no passive-interface GigabitEthernet0/0
 area 0 authentication message-digest
 network 192.168.1.0 0.0.0.255 area 0
 default-information originate
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
end
```


Packet Tracer: Configuración de OSPFv2 multiárea (versión para el instructor)

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

Topología

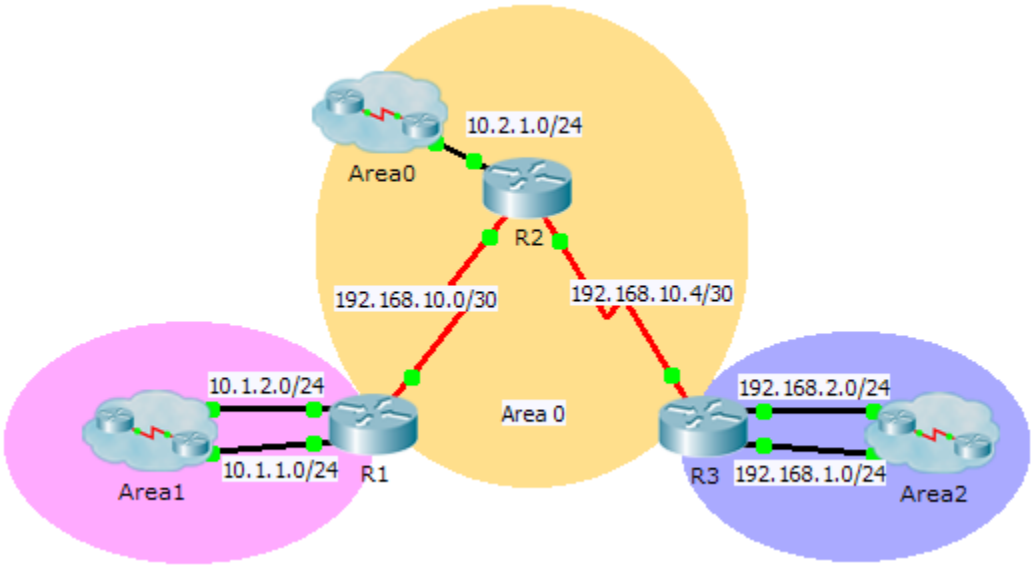


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Área del protocolo OSPFv2:
R1	G0/0	10.1.1.1	255.255.255.0	1
	G0/1	10.1.2.1	255.255.255.0	1
	S0/0/0	192.168.10.2	255.255.255.252	0
R2	G0/0	10.2.1.1	255.255.255.0	0
	S0/0/0	192.168.10.1	255.255.255.252	0
	S0/0/1	192.168.10.5	255.255.255.252	0
R3	G0/0	192.168.2.1	255.255.255.0	2
	G0/1	192.168.1.1	255.255.255.0	2
	S0/0/1	192.168.10.6	255.255.255.252	0

Objetivos

Parte 1: Configurar OSPFv2 multiárea

Parte 2: Verificar y examinar OSPFv2 multiárea

Información básica

En esta actividad, configurará OSPFv2 multiárea. La red ya está conectada, y las interfaces están configuradas con el direccionamiento IPv4. Su trabajo es habilitar OSPFv2 multiárea, verificar la conectividad y examinar el funcionamiento de OSPFv2 multiárea.

Parte 1: Configurar OSPFv2

Paso 1: Configure OSPFv2 en R1.

Configure OSPFv2 en el R1 con una ID de proceso 1 y una ID de router 1.1.1.1.

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
```

Paso 2: Anunciar cada red conectada directamente en OSPFv2 en el R1.

Configure cada red en OSPFv2 mediante la asignación de áreas según la **tabla de direccionamiento**.

```
R1(config-router)# network 10.1.1.0 0.0.0.255 area 1
R1(config-router)# network 10.1.2.0 0.0.0.255 area 1
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
```

Paso 3: Configurar OSPFv2 en el R2 y el R3.

Repita los pasos anteriores para el **R2** y el **R3** con las ID de router 2.2.2.2 y 3.3.3.3, respectivamente.

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.2.1.0 0.0.0.255 area 0
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.4 0.0.0.3 area 0
!
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
R3(config-router)# network 192.168.1.0 0.0.0.255 area 2
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

Parte 2: Verificar y examinar OSPFv2 multiárea

Paso 1: Verificar la conectividad a cada una de las áreas OSPFv2.

Desde el R1, haga ping a cada uno de los siguientes dispositivos remotos en el área 0 y el área 2: 192.168.1.2, 192.168.2.2 y 10.2.1.2.

Paso 2: Utilizar los comandos show para examinar las operaciones de OSPFv2 actuales.

Utilice los siguientes comandos para recopilar información sobre la implementación de OSPFv2 multiárea.

```
show ip protocols
show ip route
```



```
show ip ospf database
show ip ospf interface
show ip ospf neighbor
```

Preguntas de reflexión

1. ¿Cuáles de los routers son internos? R2
2. ¿Cuáles de los routers son de respaldo? El R1, el R2 y el R3 son routers de respaldo.
3. ¿Cuáles de los routers son de área perimetral? El R1 y el R3.
4. ¿Cuáles de los routers son de sistema autónomo? Ninguno, todas las interfaces activas en los tres routers se conectan a un área OSPF.
5. ¿Cuáles de los routers generan LSA de tipo 1? Todos los routers OSPF generan LSA de tipo 1.
6. ¿Cuáles de los routers generan LSA de tipo 2? Los routers ocultos que son DR en cada una de las áreas. ID de router 4.4.4.4, 5.5.5.5, 6.6.6.6, 9.9.9.9.
7. ¿Cuáles de los routers generan LSA de tipo 3? El R1 y el R3, ya que ambos son ABR y deben saturar las áreas con información de las demás áreas.
8. ¿Cuáles de los routers generan LSA de tipo 4 y 5? Ninguno, porque no hay ningún ASBR en la red.
9. ¿Cuántas rutas interárea tiene cada router? El R1 y el R3 tienen dos IA, y el R2 tiene cuatro.
10. ¿Por qué hay, en general, un ASBR en este tipo de red? Los ASBR se utilizan para conectar dominios de routing externos.

Tabla de calificación sugerida

Packet Tracer suma 80 puntos. Cada una de las preguntas de reflexión vale 2 puntos.

Packet Tracer: Configuración de OSPFv3 multiárea (versión para el instructor)

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

Topología

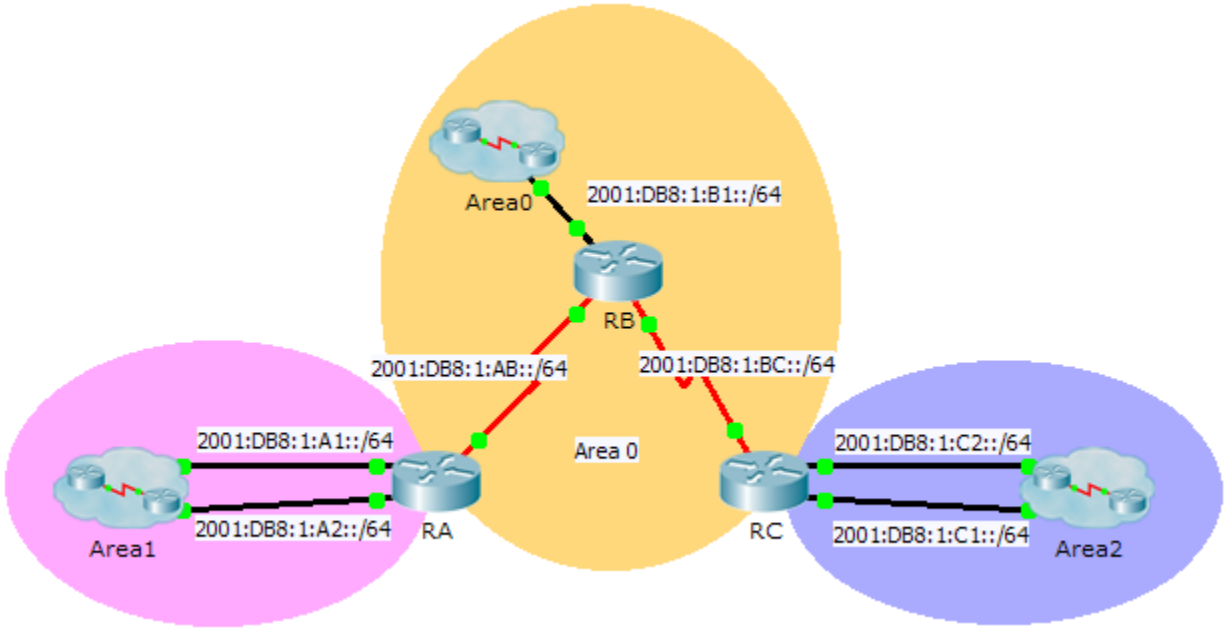


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv6	Área OSPF
RA	G0/0	2001:DB8:1:A1::1/64	1
	G0/1	2001:DB8:1:A2::1/64	1
	S0/0/0	2001:DB8:1:AB::2/64	0
	Link-Local	FE80::A	N/A
RB	G0/0	2001:DB8:1:B1::1/64	0
	S0/0/0	2001:DB8:1:AB::1/64	0
	S0/0/1	2001:DB8:1:BC::1/64	0
	Link-Local	FE80::B	N/A
RC	G0/0	2001:DB8:1:C1::1/64	2
	G0/1	2001:DB8:1:C2::1/64	2
	S0/0/1	2001:DB8:1:BC::2/64	0
	Link-Local	FE80::C	N/A

Objetivos

Parte 1: configurar OSPFv3

Parte 2: Verificar el funcionamiento de OSPFv3 multiárea

Información básica

En esta actividad, configurará OSPFv3 multiárea. La red ya está conectada, y las interfaces están configuradas con el direccionamiento IPv6. Su trabajo es habilitar OSPFv3 multiárea, verificar la conectividad y examinar el funcionamiento de OSPFv3 multiárea.

Parte 1: Configurar OSPFv3

Paso 1: Habilitar el routing IPv6 y configurar OSPFv3 en el RA.

a. Activar routing IPv6.

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

b. Configure OSPFv3 en el RA con una ID de proceso 1 y una ID de router 1.1.1.1.

```
RA(config)# ipv6 router ospf 1
RA(config-rtr)# router-id 1.1.1.1
```

Paso 2: Anunciar cada red conectada directamente en OSPFv3 en el RA.

Configure todas las interfaces IPv6 activas con OSPFv3 mediante la asignación de estas al área que se indica en la **tabla de direccionamiento**.

```
RA(config)# interface GigabitEthernet 0/0
RA(config-if)# ipv6 ospf 1 area 1
RA(config-if)# interface GigabitEthernet 0/1
RA(config-if)# ipv6 ospf 1 area 1
RA(config-if)# interface Serial 0/0/0
RA(config-if)# ipv6 ospf 1 area 0
```

Paso 3: Configurar OSPFv3 en el RB y el RC.

Repita los pasos 1 y 2 para el **RB** y el **RC**, y cambie las ID de router por 2.2.2.2 y 3.3.3.3, respectivamente.

```
RB(config)# ipv6 unicast-routing
RB(config)# ipv6 router ospf 1
RB(config-rtr)# router-id 2.2.2.2
RB(config-rtr)# interface GigabitEthernet0/0
RB(config-if)# ipv6 ospf 1 area 0
RB(config-if)# interface Serial0/0/0
RB(config-if)# ipv6 ospf 1 area 0
RB(config-if)# interface Serial0/0/1
RB(config-if)# ipv6 ospf 1 area 0
!
RC(config)# ipv6 unicast-routing
```



```
RC(config)# ipv6 router ospf 1
RC(config-rtr)# router-id 3.3.3.3
RC(config-rtr)# interface GigabitEthernet 0/0
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface GigabitEthernet 0/1
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface Serial 0/0/1
RC(config-if)# ipv6 ospf 1 area 0
```

Parte 2: Verificar las operaciones de OSPFv3 multiárea

Paso 1: Verificar la conectividad a cada una de las áreas OSPFv3.

Desde el RA, haga ping a cada uno de los siguientes dispositivos remotos en el área 0 y el área 2: 2001:DB8:1:B1::2, 2001:DB8:1:A1::2, 2001:DB8:1:A2::2, 2001:DB8:1:C1::2 y 2001:DB8:1:C2::2.

Paso 2: Utilizar los comandos show para examinar las operaciones de OSPFv3 actuales.

Utilice los siguientes comandos para recopilar información sobre la implementación de OSPFv3 multiárea.

```
show ipv6 ospf
show ipv6 route
show ipv6 ospf database
show ipv6 ospf interface
show ipv6 ospf neighbor
```

Nota: el resultado de Packet Tracer para **show ipv6 protocols** actualmente no concuerda con el resultado del IOS 15. Consulte las prácticas de laboratorio con equipos reales para obtener el resultado correcto del comando **show**.

Packet Tracer: Configuración de EIGRP básico con IPv4 (versión para el instructor)

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

Topología

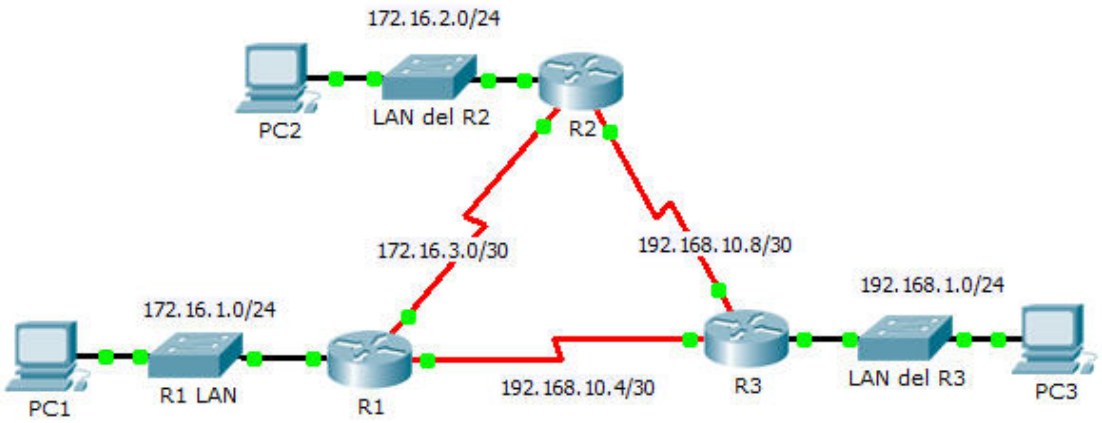


Tabla de asignación de direcciones

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	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: configurar EIGRP

Parte 2: Verificar el routing EIGRP

Información básica

En esta actividad, implementará la configuración de EIGRP básico, incluidos los comandos network, las interfaces pasivas y la deshabilitación de la sumarización automática. A continuación, verificará la configuración EIGRP mediante una variedad de comandos show y la prueba de conectividad de extremo a extremo.

Parte 1: Configure EIGRP

Paso 1: Habilite el proceso de enrutamiento EIGRP.

Habilite el proceso de routing EIGRP en cada router con el número de AS 1. Se muestra la configuración para el **R1**.

```
R1(config)# router eigrp 1
R2(config)# router eigrp 1
R3(config)# router eigrp 1
```

¿Cuál es el rango de números que se pueden utilizar como números de AS? 1 a 65 535

Nota: actualmente, Packet Tracer no admite la configuración de una ID de router EIGRP.

Paso 2: Anunciar las redes conectadas directamente.

a. Utilice el comando **show ip route** para mostrar las redes conectadas directamente en cada router.

¿Cómo se puede diferenciar entre las direcciones de subred y las direcciones de interfaz? Las subredes se identifican con una “C”, y las direcciones de enlaces se identifican con una “L”.

b. En cada router, configure EIGRP para anunciar las subredes específicas conectadas directamente. Se muestra la configuración para el **R1**.

```
R1(config-router)# network 172.16.1.0 0.0.0.255
R1(config-router)# network 172.16.3.0 0.0.0.3
R1(config-router)# network 192.168.10.4 0.0.0.3

R2(config-router)# network 172.16.2.0 0.0.0.255
R2(config-router)# network 172.16.3.0 0.0.0.3
R2(config-router)# network 192.168.10.8 0.0.0.3

R3(config-router)# network 192.168.1.0 0.0.0.255
R3(config-router)# network 192.168.10.4 0.0.0.3
R3(config-router)# network 192.168.10.8 0.0.0.3
```

Paso 3: Configurar las interfaces pasivas.

Configure las interfaces LAN para que no se anuncien las actualizaciones de EIGRP. Se muestra la configuración para el **R1**.

```
R1(config-router)# passive-interface g0/0
R2(config-router)# passive-interface g0/0
R3(config-router)# passive-interface g0/0
```


Paso 4: Desactive el resumen automático.

La topología contiene redes no contiguas. Por lo tanto, deshabilite la sumarización automática en cada router. Se muestra la configuración para el **R1**.

```
R1(config-router)# no auto-summary
R2(config-router)# no auto-summary
R3(config-router)# no auto-summary
```

Nota: antes del IOS 15, la sumarización automática se debía deshabilitar de forma manual.

Paso 5: Guarde la configuración.

Parte 2: Verificar el routing EIGRP

Paso 1: Analizar las adyacencias de vecinos.

a. ¿Con qué comando se muestran los vecinos que detectó EIGRP? **show ip eigrp neighbors**

b. Los tres routers deberán poseer dos vecinos en la lista. El resultado para el **R1** debe ser similar al siguiente:

```
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt  Num
0   172.16.3.2      Se0/0/0        14   00:25:05  40     1000  0   28
1   192.168.10.6    Se0/0/1        12   00:13:29  40     1000  0   31
```

Paso 2: Mostrar los parámetros del protocolo de routing EIGRP.

a. ¿Con qué comando se muestran los parámetros y otra información sobre el estado actual de cualquier proceso de protocolo de routing IPv4 activo configurado en el router? **show ip protocols**

b. En el **R2**, introduzca el comando que indicó para el paso 2a y responda las siguientes preguntas:

¿Cuántos routers comparten información de routing con el **R2**? 2

¿Dónde se encuentra esta información? Routing Information Sources

¿Cuál es el máximo conteo de saltos? 100

Paso 3: Verificar la conectividad de extremo a extremo

Ahora la PC1, la PC2 y la PC3 deben poder hacer ping entre sí. De lo contrario, resuelva los problemas de configuración EIGRP.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: configurar EIGRP	Paso 1	2	
	Paso 2a	2	
	Total de la parte 1	**4**	
Parte 2: Verificar el routing EIGRP	Paso 1a	5	
	Paso 2a	5	
	Paso 2b	6	
	Total de la parte 2	**16**	
	Puntuación de Packet Tracer	**80**	
	Puntuación total	**100**	

Packet Tracer: Investigación de la FSM DUAL (versión para el instructor)

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

Topología

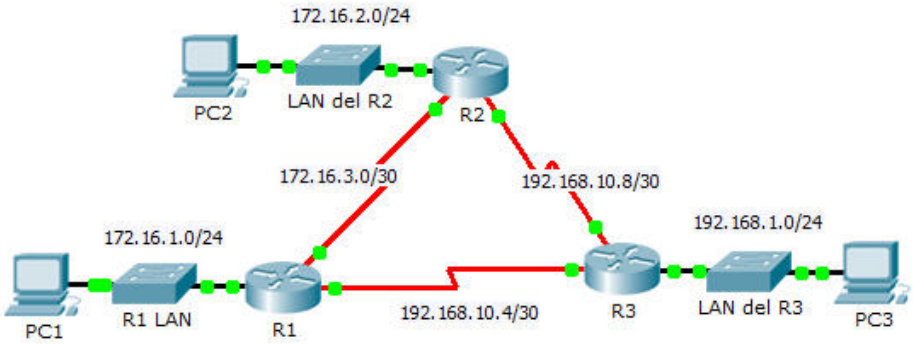


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.16.1.254	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	172.16.2.254	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	192.168.1.254	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	172.16.1.1	255.255.255.0	172.16.1.254
PC2	NIC	192.168.1.1	255.255.255.0	192.168.1.254
PC3	NIC	192.168.2.1	255.255.255.0	192.168.2.254

Objetivos

Parte 1: Verificar la configuración EIGRP

Parte 2: Observar la FSM DUAL de EIGRP

Información básica

En esta actividad, modificará la fórmula de la métrica de EIGRP para generar un cambio en la topología. Esto le permitirá observar cómo reacciona EIGRP cuando un vecino se desconecta debido a circunstancias inesperadas. A continuación, utilizará el comando **debug** para ver los cambios en la topología y la forma en que la máquina de estados finitos de DUAL determina las rutas de sucesor y de sucesor factible para volver a converger la red.

Parte 1: Verificar la configuración EIGRP

Paso 1: Analizar las tablas de routing de cada router y verificar que haya una ruta a cada red en la topología.

¿Con qué comando se muestra la tabla de routing? **show ip route**

¿Alguno de los routers realiza el balanceo de carga entre algunas de las redes? Sí, el R1 a la red 192.168.10.8, el R2 a la red 192.168.10.4, y el R3 a la red 172.16.3.0.

Paso 2: Verificar que cada router tenga entradas en su tabla de vecinos.

¿Con qué comando se muestra la tabla de vecinos? **show ip eigrp neighbors**

¿Cuántos vecinos tiene cada router? Todos los routers tienen dos vecinos.

Paso 3: Analizar la tabla de topología de cada router.

a. ¿Con qué comando se muestra la tabla de topología? **show ip eigrp topology**

   Sobre la base del resultado de la tabla de topología, ¿cuántas rutas de sucesor tiene cada router? 7

   ¿Por qué hay más rutas de sucesor que redes? Hay seis rutas en la topología, pero cada router tiene dos rutas sucesoras a una red (el R1 tiene dos rutas sucesoras a 192.168.10.8).

b. Copie el resultado de la tabla de topología del **R1** en un editor de texto de modo que pueda consultarlo más adelante.

Parte 2: Observar la FSM DUAL de EIGRP

Paso 1: En el R1, activar la característica de depuración que mostrará las notificaciones de la FSM DUAL.

¿Con qué comando se habilita la depuración para la FSM DUAL de EIGRP? **debug eigrp fsm**

Paso 2: Forzar una actualización de la FSM DUAL para generar un resultado de debug.

a. Coloque las ventanas del R1 y el R3 una junto a la otra de modo que pueda observar el resultado de debug. A continuación, deshabilite la interfaz serial 0/0/0 en el R3.

```
R3(config)# interface s0/0/0
R3(config-if)# shutdown
```

b. Todavía no deshabilite la depuración. ¿Qué resultado de debug indicó cambios en la tabla de routing?

```
<resultado omitido>
DUAL: Dest 192.168.10.4/30 (No peers) not entering active state.
DUAL: Removing dest 192.168.10.4/30, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.10.4/30
```


Paso 3: Mostrar la tabla de routing del R1.

Verifique que la red 192.168.10.4/30 ya no esté en la tabla de routing del **R1**.

Describa cualquier otro cambio en la tabla de routing del **R1**. La 192.168.10.8 solo tiene una ruta en lugar de dos.

Paso 4: Determinar la diferencia en la tabla de topología.

Analice la tabla de topología del **R1** y compárela con el resultado anterior de la parte 1.

¿Hay algún otro cambio en la tabla de topología del **R1**? Si, 192.168.10.4/30 ya no está en la tabla de topología y solo hay un sucesor a la 192.168.10.8/30.

Paso 5: Registrar los cambios en la tabla de vecinos de cada router.

Analice la tabla de vecinos de cada router y compárela con la anterior de la parte 1.

¿Hay algún cambio en la tabla de vecinos? Si, 192.168.10.6 del R1 ya no tiene la ruta 192.168.10.5 del R3 como vecino.

Paso 6: Restaurar la conectividad entre el R1 y el R2.

a. Con las ventanas del R1 y el R3 una junto a la otra, active la interfaz serial 0/0/0 en el R3 y observe el resultado de debug en el R1.

b. Deshabilite la depuración mediante la introducción de la versión **no** del comando debug o simplemente introduzca **undebug** all. ¿Qué resultado de debug indicó cambios en la tabla de routing?

```
DUAL: Find FS for dest: 192.168.1.0/24. FD is 2682112, RD is 2170112
DUAL: RT installed 192.168.1.0/24 via 192.168.10.6
```

¿Cómo manejó la FSM DUAL el cambio en la topología cuando volvió la ruta al **R1**? La ruta entre el R1 y el R3 en la red 192.167.10.4/30 volvió a activarse, y se formaron adyacencias.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Verificar la configuración EIGRP	Paso 1	12	
	Paso 2	12	
	Paso 3	12	
	Total de la parte 1	**36**	
Parte 2: Observar la FSM DUAL de EIGRP	Paso 1	10	
	Paso 2	12	
	Paso 3	10	
	Paso 4	10	
	Paso 5	10	
	Paso 6	12	
	Total de la parte 2	**64**	
	Puntuación total	**100**	

Packet Tracer: Configuración de EIGRP básico con IPv6 (versión para el instructor)

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

Topología

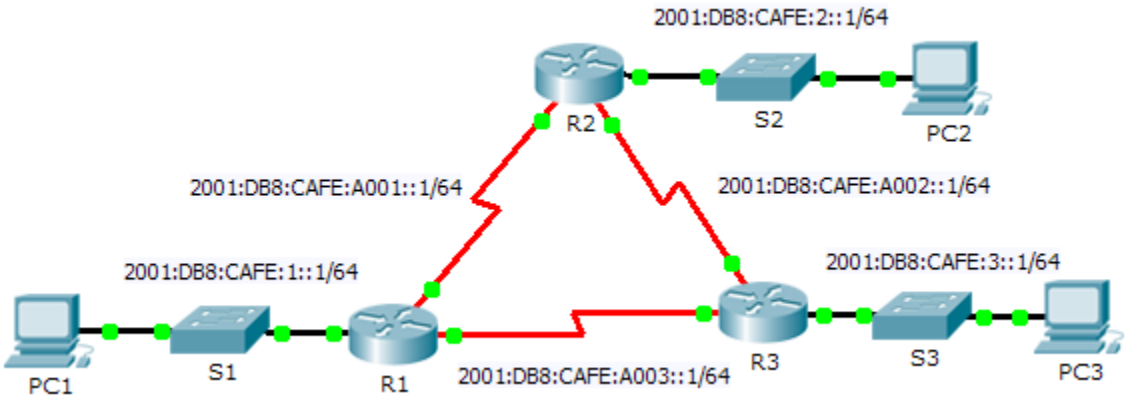


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	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
	Link-local	FE80::1	N/A
R2	G0/0	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
	Link-local	FE80::2	N/A
R3	G0/0	2001:DB8:CAFE:3::1/64	N/A
	S0/0/0	2001:DB8:CAFE:A003::2/64	N/A
	S0/0/1	2001:DB8:CAFE:A002::2/64	N/A
	Link-local	FE80::3	N/A
PC1	NIC	2001:DB8:CAFE:1::3/64	Fe80::1
PC2	NIC	2001:DB8:CAFE:2::3/64	Fe80::2
PC3	NIC	2001:DB8:CAFE:3::3/64	Fe80::3

Objetivos

Parte 1: Configurar el routing EIGRP para IPv6

Parte 2: Verificar el routing EIGRP para IPv6

Situación

En esta actividad, configurará la red con el routing EIGRP para IPv6. También asignará las ID de los routers, configurará interfaces pasivas, verificará que la red haya convergido por completo y mostrará información de routing mediante los comandos **show**.

EIGRP para IPv6 tiene el mismo funcionamiento y las mismas características generales que EIGRP para IPv4. Existen algunas diferencias importantes entre ellos:

- EIGRP para IPv6 se configura directamente en las interfaces del router.
- Con EIGRP para IPv6, se necesita una ID en cada router; de lo contrario, no se inicia el proceso de routing.
- El proceso de routing EIGRP para IPv6 utiliza una característica “shutdown”.

Parte 1: Configurar el routing EIGRP para IPv6

Paso 1: Habilite el routing IPv6 en cada router.

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

R2(config)# ipv6 unicast-routing

R3(config)# ipv6 unicast-routing
```

Paso 2: Habilitar el routing EIGRP para IPv6 en cada router.

El proceso de routing IPv6 está desactivado de manera predeterminada. Emita un comando que habilite el routing EIGRP para IPv6 en el R1, el R2 y el R3.

Habilite el proceso EIGRP en todos los routers y utilice el número **1** como número de sistema autónomo.

```
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# no shutdown

R2(config)# ipv6 router eigrp 1
R2(config-rtr)# no shutdown

R3(config)# ipv6 router eigrp 1
R3(config-rtr)# no shutdown
```

Paso 3: Asignar una ID a cada router.

Las ID de los routers son las siguientes:

- R1: 1.1.1.1
- R2: 2.2.2.2
- R3: 3.3.3.3

```
R1(config-rtr)# router-id 1.1.1.1
```



```
R2(config-rtr)# router-id 2.2.2.2

R3(config-rtr)# router-id 3.3.3.3
```

Paso 4: Configurar EIGRP para IPv6 usando 1 como AS en cada interfaz.

```
R1(config)# int g0/0
R1(config-if)# ipv6 eigrp 1
R1(config)# int s0/0/0
R1(config-if)# ipv6 eigrp 1
R1(config)# int s0/0/1
R1(config-if)# ipv6 eigrp 1

R2(config)# int g0/0
R2(config-if)# ipv6 eigrp 1
R2(config)# int s0/0/0
R2(config-if)# ipv6 eigrp 1
R2(config)# int s0/0/1
R2(config-if)# ipv6 eigrp 1

R3(config)# int g0/0
R3(config-if)# ipv6 eigrp 1
R3(config)# int s0/0/0
R3(config-if)# ipv6 eigrp 1
R3(config)# int s0/0/1
R3(config-if)# ipv6 eigrp 1
```

Parte 2: Verificar el routing EIGRP para IPv6

Paso 1: Analizar las adyacencias de vecinos.

Utilice el comando **show ipv6 eigrp neighbors** para verificar que se haya establecido la adyacencia con los routers vecinos. Las direcciones link-local de los routers vecinos se muestran en la tabla de adyacencias.

Paso 2: Analizar la tabla de routing EIGRP para IPv6.

Utilice el comando **show ipv6 route** para mostrar la tabla de routing IPv6 en todos los routers. Las rutas EIGRP para IPv6 se indican en la tabla de routing con una **D**.

Paso 3: Verificar los parámetros y el estado actual de los procesos del protocolo de routing IPv6 activo.

Utilice el comando **show ipv6 protocols** para verificar el parámetro configurado.

Paso 4: Verifique la conectividad de extremo a extremo.

Ahora la PC1, la PC2 y la PC3 deben poder hacer ping entre sí. De lo contrario, resuelva los problemas de configuración EIGRP.

Packet Tracer: Configuración de rutas resumidas manuales EIGRP para IPv4 e IPv6 (versión para el instructor)

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

Topología

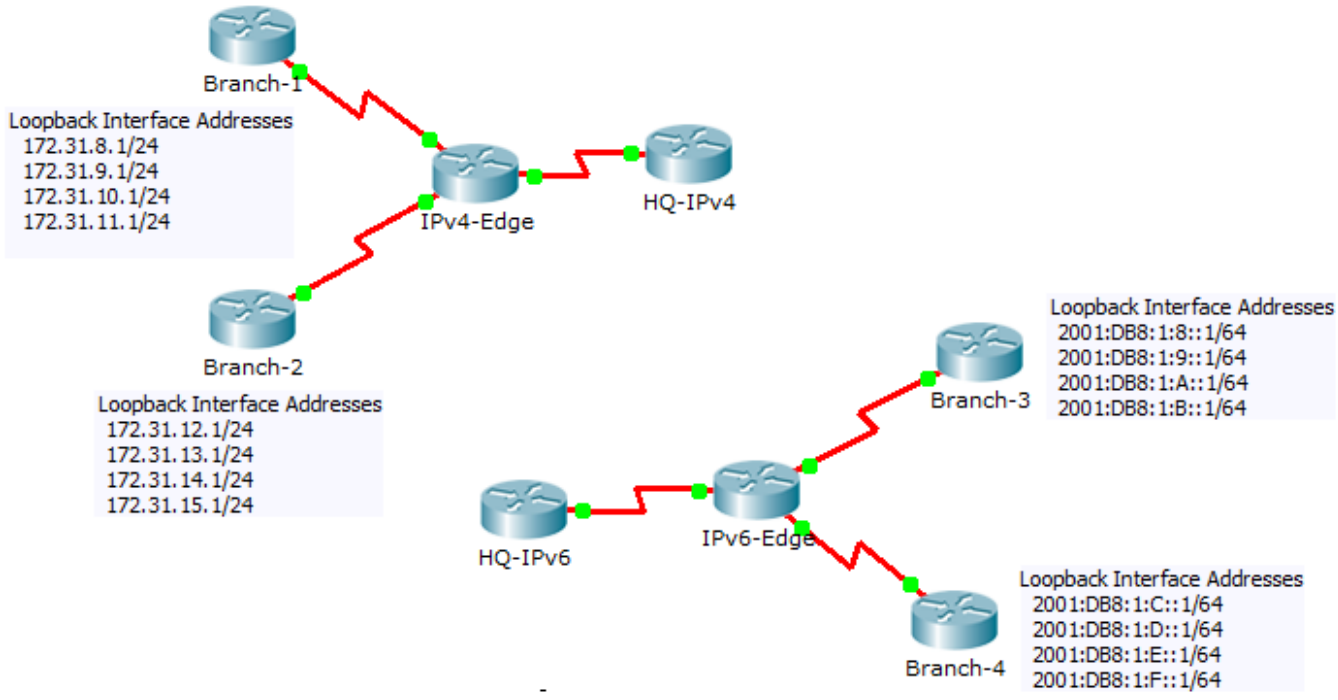


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred
		Dirección/Prefijo IPv6	
HQ-IPv4	S0/0/1	10.10.10.1	255.255.255.0
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.0
	S0/0/1	172.31.7.1	255.255.255.0
	S0/1/0	10.10.10.2	255.255.255.0
Branch-1	S0/0/0	172.31.6.2	255.255.255.0
Branch-2	S0/0/1	172.31.7.2	255.255.255.0
HQ-IPv6	S0/0/1	2001:DB8:1:A001::1/64	
IPv6-Edge	S0/0/0	2001:DB8:1:7::1/64	
	S0/0/1	2001:DB8:1:6::1/64	
	S0/1/0	2001:DB8:1:A001::2/164	
Branch-3	S0/0/0	2001:DB8:1:7::2/64	
Branch-4	S0/0/1	2001:DB8:1:6::2/64	

Objetivos

Parte 1: Configurar rutas resumidas manuales EIGRP para IPv4

Parte 2: Configurar rutas resumidas manuales EIGRP para IPv6

Situación

En esta actividad, calculará y configurará rutas resumidas para las redes IPv4 e IPv6. EIGRP ya está configurado; sin embargo, debe configurar las rutas resumidas IPv4 e IPv6 en las interfaces especificadas. EIGRP reemplaza las rutas actuales por una ruta resumida más específica, lo que reduce el tamaño de las tablas de routing.

Parte 1: Configurar rutas resumidas manuales EIGRP para IPv4

Paso 1: Verificar la configuración EIGRP en cada router habilitado para IPv4.

Muestre la tabla de routing en cada router habilitado para IPv4 y verifique que todas las rutas IPv4 sean visibles. Haga ping a las interfaces loopback desde **HQ-IPv4** para verificar la conectividad.

Paso 2: Calcular, configurar y verificar una ruta resumida en Branch-1.

Al observar la tabla de routing en **IPv4-Edge** (Perimetral-IPv4) verifique que **Branch-1** (Sucursal-1) anuncie las cuatro redes representadas por las interfaces loopback.

a. Calcule una dirección de resumen para las cuatro interfaces loopback en **Branch-1**.

172.31.8.0/22

b. Configure **Branch-1** para que se anuncie una ruta resumida EIGRP a **IPv4-Edge**.

```
Branch-1(config)# interface Serial0/0/0
Branch-1(config-if)# ip summary-address eigrp 1 172.31.8.0 255.255.252.0
```

c. Verifique que **IPv4-Edge** ahora tenga solo una ruta resumida para las cuatro redes de loopback en **Branch-1**.

```
IPv4-Edge# show ip route
<resultado omitido>
D       172.31.8.0/22 [90/2297856] via 172.31.6.2, 00:00:40, Serial0/0/0
D       172.31.12.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
D       172.31.13.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
D       172.31.14.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
D       172.31.15.1/32 [90/2297856] via 172.31.7.2, 00:01:25, Serial0/0/1
```

Paso 3: Calcular, configurar y verificar una ruta resumida en Branch-2.

Al observar la tabla de routing en **IPv4-Edge**, verifique que **Branch-2** (Sucursal-2) anuncie las cuatro redes representadas por las interfaces loopback.

a. Calcule una dirección de resumen para las cuatro interfaces loopback en **Branch-2**.

172.31.12.0/22

b. Configure **Branch-2** para que se anuncie una ruta resumida EIGRP a **IPv4-Edge**.

```
Branch-2(config)# interface Serial0/0/1
Branch-2(config-if)# ip summary-address eigrp 1 172.31.12.0 255.255.252.0
```

c. Verifique que **IPv4-Edge** ahora tenga solo una ruta resumida para las cuatro redes de loopback en **Branch-2**.

```
IPv4-Edge# show ip route
<resultado omitido>
D       172.31.8.0/22 [90/2297856] via 172.31.6.2, 00:02:55, Serial0/0/0
D       172.31.12.0/22 [90/2297856] via 172.31.7.2, 00:00:07, Serial0/0/1
```

Paso 4: Calcular, configurar y verificar una ruta resumida en IPv4-Edge.

Aunque **HQ-IPv4** tenga dos rutas que representan las ocho redes de loopback, estas dos rutas se pueden resumir en una sola.

a. Calcule una dirección de resumen para las dos rutas resumidas en la tabla de routing de **IPv4-Edge**.

172.31.8.0/21

b. Configure **IPv4-Edge** para que se anuncie una ruta resumida EIGRP a **HQ-IPv4**.

```
IPv4-Edge(config)# interface Serial0/1/0
IPv4-Edge(config-if)# ip summary-address eigrp 1 172.31.8.0 255.255.248.0
```

c. Verifique que **HQ-IPv4** ahora tenga solo una ruta resumida que represente las ocho redes de loopback en Branch-1 y Branch-2.

Nota: puede ser necesario restablecer la interfaz que conecta **HQ-IPv4** a **IPv4-Edge**.

```
HQ-IPv4# show ip route
```



```
<resultado omitido>
D       172.31.8.0/21 [90/2681856] via 10.10.10.2, 00:06:42, Serial0/0/1
```

d. Debería poder hacer ping a todas las interfaces loopback IPv4 desde **HQ-IPv4**.

Parte 2: Configurar rutas resumidas manuales EIGRP para IPv6

Paso 1: Verificar la configuración EIGRP en cada router habilitado para IPv6.

Muestre la tabla de routing en cada router habilitado para IPv6 y verifique que todas las rutas IPv6 sean visibles. Haga ping a las interfaces loopback desde **HQ-IPv6** para verificar la conectividad.

Paso 2: Calcular, configurar y verificar una ruta resumida en Branch-3.

Al observar la tabla de routing en **IPv6-Edge** (Perimetral-IPv6), verifique que **Branch-3** (Sucursal-3) anuncie las cuatro redes representadas por las interfaces loopback.

a. Calcule una dirección de resumen para las cuatro interfaces loopback en **Branch-3**.

```
2001:DB8:1:8::/62
```

b. Configure **Branch-3** para que se anuncie una ruta resumida EIGRP a **IPv6-Edge**.

```
Branch-3(config)# interface Serial0/0/0
Branch-3(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:8::/62
```

c. Verifique que **IPv6-Edge** ahora tenga solo una ruta resumida para las cuatro redes de loopback en **Branch-3**.

Nota: actualmente, Packet Tracer no califica EIGRP para las rutas resumidas IPv6. Sin embargo, el router **IPv6-Edge** ahora debería tener solo cinco rutas EIGRP, una de las cuales es la ruta resumida que configuró en **Branch-3**.

```
IPv6-Edge# show ipv6 route
<resultado omitido>
D   2001:DB8:1:8::/62 [90/2297856]
     via FE80::3, Serial0/0/0
D   2001:DB8:1:C::/64 [90/2297856]
     via FE80::4, Serial0/0/1
D   2001:DB8:1:D::/64 [90/2297856]
     via FE80::4, Serial0/0/1
D   2001:DB8:1:E::/64 [90/2297856]
     via FE80::4, Serial0/0/1
D   2001:DB8:1:F::/64 [90/2297856]
     via FE80::4, Serial0/0/1
```

Paso 3: Calcular, configurar y verificar una ruta resumida en Branch-4.

Al observar la tabla de routing en **IPv6-Edge**, verifique que **Branch-4** (Sucursal-4) anuncie las cuatro redes representadas por las interfaces loopback.

a. Calcule una dirección de resumen para las cuatro interfaces loopback en **Branch-4**.

```
2001:DB8:1:C::/62
```


b. Configure **Branch-4** para que se anuncie una ruta resumida EIGRP a **IPv6-Edge**.

```
Branch-4(config)# interface Serial0/0/1
Branch-4(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:C::/62
```

c. Verifique que **IPv6-Edge** ahora tenga solo una ruta resumida para las cuatro redes de loopback en **Branch-4**.

Nota: actualmente, Packet Tracer no califica EIGRP para las rutas resumidas IPv6. Sin embargo, el router **IPv6-Edge** ahora debería tener solo dos rutas EIGRP, una ruta resumida de cada uno de los routers de sucursal IPv6.

```
IPv6-Edge# show ipv6 route
<resultado omitido>
D   2001:DB8:1:8::/62 [90/2297856]
     via FE80::3, Serial0/0/0
D   2001:DB8:1:C::/62 [90/2297856]
     via FE80::4, Serial0/0/1
```

Paso 4: Calcular, configurar y verificar una ruta resumida en IPv6-Edge.

Aunque **HQ-IPv6** tenga dos rutas que representan las ocho redes de loopback, estas dos rutas se pueden resumir en una sola.

a. Calcule una dirección de resumen para las dos rutas resumidas en la tabla de routing de **IPv6-Edge**.

2001:DB8:1:8::/61

b. Configure **IPv6-Edge** para que se anuncie una ruta resumida EIGRP a **HQ-IPv6**.

```
IPv6-Edge(config)# interface Serial0/1/0
IPv6-Edge(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:8::/61
```

c. Verifique que **HQ-IPv6** ahora tenga solo una ruta resumida que represente las ocho redes de loopback en **Branch-3** y **Branch-4**.

Nota: puede ser necesario restablecer la interfaz que conecta **HQ-IPv6** a **IPv6-Edge**.

```
HQ-IPv6# show ipv6 route
<resultado omitido>
D   2001:DB8:1:8::/61 [90/2681856]
     via FE80::2, Serial0/0/1
```

d. Debería poder hacer ping a todas las interfaces loopback IPv6 desde **HQ-IPv6**.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Configurar rutas resumidas manuales EIGRP para IPv6	Paso 2	20	
	Paso 3	20	
	Paso 4	10	
	Total de la parte 2	**50**	
	Puntuación de Packet Tracer	**50**	
	Puntuación total	**100**	

Packet Tracer: Propagación de una ruta predeterminada en EIGRP para IPv4 e IPv6 (versión para el instructor)

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

Topología

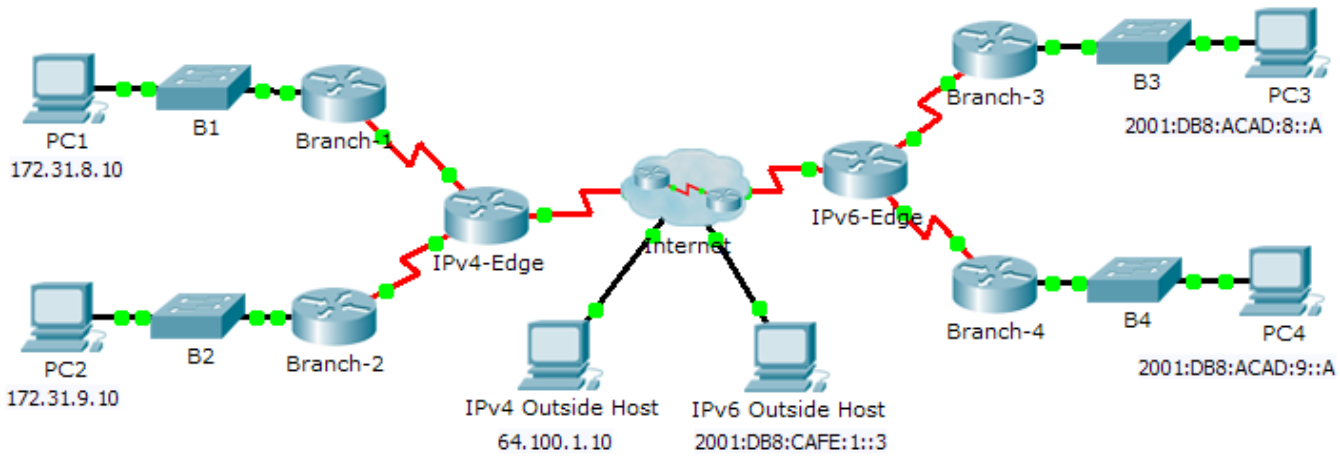


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred
		Dirección/Prefijo IPv6	
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.0
	S0/0/1	172.31.7.1	255.255.255.0
	S0/1/0	209.165.200.226	255.255.255.224
Branch-1	G0/0	172.31.8.1	255.255.255.0
	S0/0/0	172.31.6.2	255.255.255.0
Branch-2	G0/0	172.31.9.1	255.255.255.0
	S0/0/1	172.31.7.2	255.255.255.0
IPv6-Edge	S0/0/0	2001:DB8:ACAD:7::1/64	
	S0/0/1	2001:DB8:ACAD:6::1/64	
	S0/1/0	2001:DB8:CAFE:ABCD::2/164	
Branch-3	G0/0	2001:DB8:ACAD:8::1/64	
	S0/0/0	2001:DB8:ACAD:7::2/64	
Branch-4	G0/0	2001:DB8:ACAD:9::1/64	
	S0/0/1	2001:DB8:ACAD:6:::2/64	

Objetivos

Parte 1: Propagar una ruta predeterminada IPv4

Parte 2: Propagar una ruta predeterminada IPv6

Parte 3: Verificar la conectividad a los hosts externos

Situación

En esta actividad, configurará y propagará una ruta predeterminada en EIGRP para las redes IPv4 e IPv6. El EIGRP ya está configurado. Sin embargo, debe configurar una ruta predeterminada IPv4 y una IPv6. A continuación, configurará el proceso de routing EIGRP para propagar la ruta predeterminada a los vecinos EIGRP descendentes. Por último, verificará las rutas predeterminadas haciendo ping a los hosts fuera del dominio de routing EIGRP.

Parte 1: Propagar una ruta predeterminada en EIGRP para IPv4

Paso 1: Verificar la configuración EIGRP en cada router habilitado para IPv4.

Muestre la tabla de routing de cada router habilitado para IPv4 y verifique que todas las rutas IPv4 sean visibles.

Paso 2: Configurar una ruta predeterminada IPv4.

Configure una ruta predeterminada IPv4 conectada directamente en **IPv4-Edge**.

```
IPv4-Edge(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

Paso 3: Propagar la ruta predeterminada en EIGRP

Configure el proceso de routing EIGRP para propagar la ruta predeterminada.

```
IPv4-Edge(config)# router eigrp 1
IPv4-Edge(config-router)# redistribute static
```

Paso 4: Verificar que la ruta predeterminada IPv4 se propague.

Muestre las tablas de routing para **Branch-1** y **Branch-2** para verificar que la ruta predeterminada ahora esté instalada.

```
Branch-1# show ip route
<resultado omitido>
D*EX 0.0.0.0/0 [170/7289856] via 172.31.6.1, 00:01:24, Serial0/0/0

Branch-2# show ip route
<resultado omitido>
D*EX 0.0.0.0/0 [170/7289856] via 172.31.7.1, 00:01:45, Serial0/0/1
```

Parte 2: Propagar una ruta predeterminada en EIGRP para IPv6

Paso 1: Verificar la configuración EIGRP en cada router habilitado para IPv6.

Muestre la tabla de routing de cada router habilitado para IPv6 y verifique que todas las rutas IPv6 sean visibles.

Paso 2: Configurar una ruta predeterminada IPv6.

Configure una ruta predeterminada IPv6 conectada directamente en **IPv6-Edge**.

```
IPv6-Edge(config)# ipv6 route ::/0 Serial0/1/0
```

Paso 3: Propagar la ruta predeterminada en EIGRP

Configure el proceso de routing EIGRP para propagar la ruta predeterminada.

```
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# redistribute static
```

Paso 4: Verificar que la ruta predeterminada IPv6 se propague.

Muestre las tablas de routing para **Branch-3** y **Branch-4** para verificar que la ruta predeterminada ahora esté instalada.

```
Branch-3> en
Branch-3# show ipv6 route
<resultado omitido>
```



```
EX  ::/0 [170/7289856]
     via FE80::1, Serial0/0/0

Branch-4# show ipv6 route
<resultado omitido>
EX  ::/0 [170/7289856]
     via FE80::1, Serial0/0/1
```

Parte 3: Verificar la conectividad a los hosts externos

- Ahora, la **PC1** y la **PC2** deberían poder hacer ping al **IPv4 Outside Host** (Host externo IPv4).
- Ahora, la **PC3** y la **PC4** deberían poder hacer ping al **IPv6 Outside Host** (Host externo IPv6).

Packet Tracer: Resolución de problemas de EIGRP para IPv4 (versión para el instructor)

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

Topología

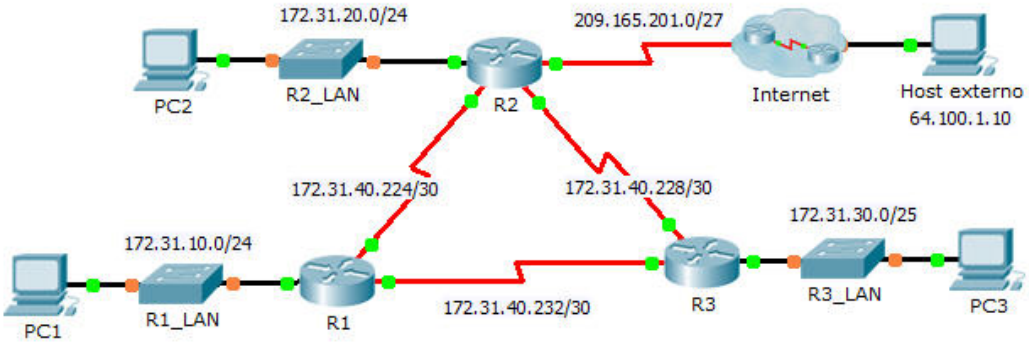


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.10.1	255.255.255.0	N/A
	S0/0/0	172.31.40.225	255.255.255.252	N/A
	S0/0/1	172.31.40.233	255.255.255.252	N/A
R2	G0/0	172.30.20.1	255.255.255.0	N/A
	S0/0/0	172.31.40.226	255.255.255.252	N/A
	S0/0/1	172.31.40.229	255.255.255.252	N/A
	S0/1/0	209.165.201.1	255.255.255.224	N/A
R3	G0/0	172.31.30.1	255.255.255.0	N/A
	S0/0/0	172.31.40.234	255.255.255.252	N/A
	S0/0/1	172.31.40.230	255.255.255.252	N/A
PC1	NIC	172.31.10.10	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.10	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.10	255.255.255.0	172.31.30.1

Situación

En esta actividad, resolverá problemas de vecinos EIGRP. Utilice los comandos show para identificar errores en la configuración de red. A continuación, registrará los errores que detecte e implementará una solución apropiada. Por último, verificará que se haya restaurado la plena conectividad de extremo a extremo.

Proceso de resolución de problemas

1. Utilice los comandos de prueba para detectar problemas de conectividad en la red y registre el problema en la tabla de documentación.
2. Utilice los comandos de verificación para determinar el origen del problema e idear una solución apropiada. Documente la solución propuesta en la tabla de documentación.
3. Implemente las soluciones de a una por vez y verifique si el problema se resolvió. Indique el estado de la resolución en la tabla de documentación.
4. Si el problema no se resolvió, es posible que primero deba deshacer la solución implementada antes de volver al paso 2.
5. Una vez que se hayan resuelto todos los problemas identificados, pruebe la plena conectividad de extremo a extremo.

Tabla de documentación

Dispositivo	Problema identificado	Solución propuesta	¿Se resolvió?
R1	No estableció adyacencias.	Eliminar EIGRP 11 y configurar EIGRP 1, anunciar las redes conectadas directamente y la interfaz pasiva g0/0, y deshabilitar la sumarización automática.	
R2	No forma una adyacencia con el R3.	Anunciar la red 172.31.40.228/30.	
R3	Efectúa sumarización automática.	Deshabilitar la sumarización automática con el subcomando de EIGRP no auto-summary.	

Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

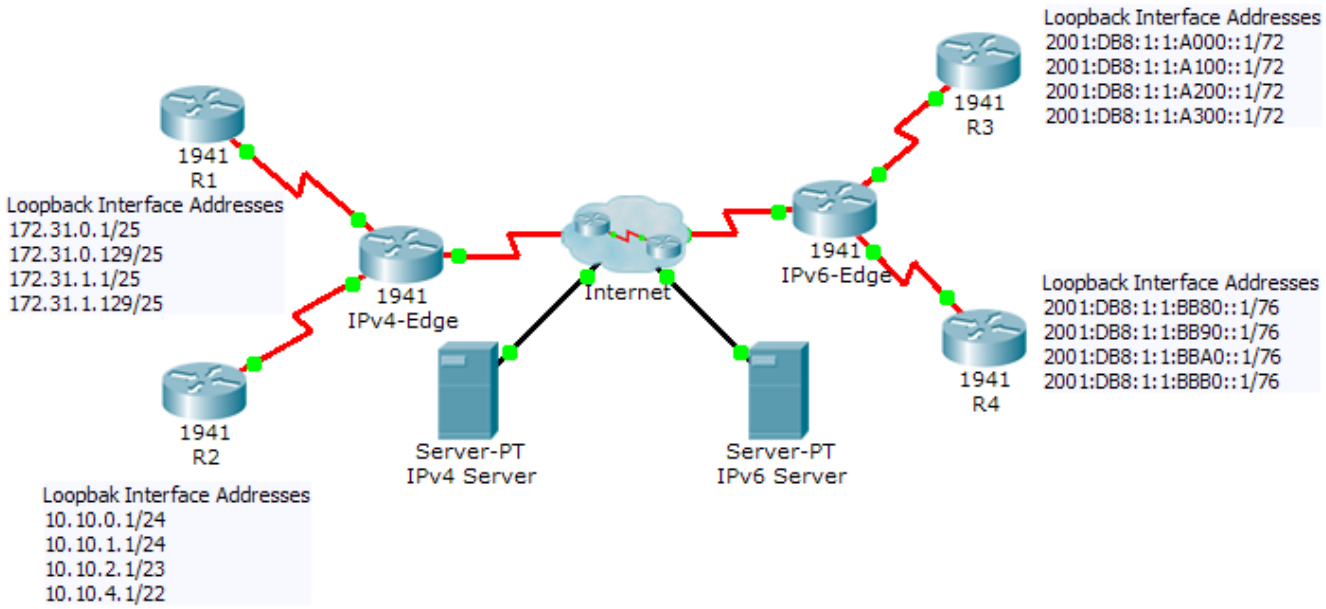


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred
		Dirección/Prefijo IPv6	
IPv4-Edge	S0/0/0	172.31.6.1	255.255.255.252
	S0/0/1	10.10.8.1	255.255.255.252
	S0/1/0	209.165.200.226	255.255.255.224
R1	S0/0/0	172.31.6.2	255.255.255.252
R2	S0/0/1	10.10.8.2	255.255.255.252
IPv6-Edge	S0/0/0	2001:DB8:A001:6::1/64	
	S0/0/1	2001:DB8:A001:7::1/64	
	S0/1/0	2001:DB8:CAFE:1::2/64	
R3	S0/0/0	2001:DB8:A001:7::2/64	
R4	S0/0/1	2001:DB8:A001:6::2/64	

Situación

En esta actividad, debe implementar EIGRP para IPv4 e IPv6 en dos redes diferentes. Parte de su tarea consiste en habilitar EIGRP, asignar las ID de los routers, cambiar los temporizadores de saludo, configurar las rutas resumidas EIGRP y limitar los anuncios de EIGRP.

Requisitos

EIGRP para IPv4

- Implemente EIGRP en los routers habilitados para IPv4 mediante el número de sistema autónomo 1.
  - Use la dirección de red con clase para las interfaces loopback.
  - Use la máscara wildcard para anunciar las redes /30 entre el **R1**, el **R2** e **IPv4-Edge**.
  - Use el método **predeterminado** para permitir el envío de actualizaciones de EIGRP únicamente por las interfaces seriales EIGRP activas.
  - Los anuncios no deben resumirse.

```
R1(config)# router eigrp 1
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface Serial0/0/0
R1(config-router)# network 172.31.0.0
R1(config-router)# no auto-summary

R2(config)# router eigrp 1
R2(config-router)# passive-interface default
R2(config-router)# no passive-interface Serial0/0/1
```



```
R2(config-router)# network 10.0.0.0
R2(config-router)# no auto-summary

IPv4-Edge(config)# router eigrp 1
IPv4-Edge(config-router)# passive-interface default
IPv4-Edge(config-router)# no passive-interface Serial0/0/0
IPv4-Edge(config-router)# no passive-interface Serial0/0/1
IPv4-Edge(config-router)# network 172.31.6.0 0.0.0.3
IPv4-Edge(config-router)# network 10.10.8.0 0.0.0.3
IPv4-Edge(config-router)# no auto-summary
```

- Configure una ruta predeterminada conectada directamente en **IPv4-Edge** y propáguela en las actualizaciones de EIGRP.

```
IPv4-Edge(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0
IPv4-Edge(config)# router eigrp 1
IPv4-Edge(config-router)# redistribute static
```

- Configure las interfaces seriales entre el **R1**, el **R2** e **IPv4-Edge** para enviar saludos cada 10 segundos.

```
R1(config)# interface s0/0/0
R1(config-if)# ip hello-interval eigrp 1 10

R2(config)# interface s0/0/1
R2(config-if)# ip hello-interval eigrp 1 10

IPv4-Edge(config)# interface s0/0/0
IPv4-Edge(config-if)# ip hello-interval eigrp 1 10
IPv4-Edge(config-if)# interface s0/0/1
IPv4-Edge(config-if)# ip hello-interval eigrp 1 10
```

- En el **R1** y el **R2**, configure una ruta resumida EIGRP para las redes de loopback.

Redes de loopback del R1	Redes de loopback del R2
172.31.0.0/25	10.10.0.0/24
172.31.0.128/25	10.10.1.0/24
172.31.1.0/25	10.10.2.0/23
172.31.1.128/25	10.10.4.0/22
Resumen: 172.31.0.0/23	Resumen: 10.10.0.0/21

```
R1(config)# interface Serial0/0/0
R1(config-if)# ip summary-address eigrp 1 172.31.0.0 255.255.254.0
```



```
R2(config)# interface Serial0/0/1
R2(config-if)# ip summary-address eigrp 1 10.10.0.0 255.255.248.0
```

- El **R1** y el **R2** deben tener solo cuatro rutas EIGRP en la tabla de routing, una de las cuales es la ruta predeterminada (`D*EX`). **IPv4-Edge** debe tener solo dos rutas EIGRP en la tabla de routing.
- Verifique que el **R1** y el **R2** puedan hacer ping al **Server IPv4** (Servidor IPv4). El **Server IPv4** también debe poder hacer ping a cada dirección de loopback en el **R1** y el **R2**.

EIGRP para IPv6

- Implemente EIGRP en los routers habilitados para IPv6 mediante el número de sistema autónomo 1.
  - Asigne a **IPv6-Edge** la ID del router 1.1.1.1.
  - Asigne al **R3** la ID del router 3.3.3.3.
  - Asigne al **R4** la ID del router 4.4.4.4.

```
IPv6-Edge(config)# ipv6 unicast-routing
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# router-id 1.1.1.1
IPv6-Edge(config-rtr)# no shutdown
IPv6-Edge(config-rtr)# interface Serial0/0/0
IPv6-Edge(config-if)# ipv6 eigrp 1
IPv6-Edge(config-if)# interface Serial0/0/1
IPv6-Edge(config-if)# ipv6 eigrp 1

R3(config)# ipv6 unicast-routing
R3(config)# ipv6 router eigrp 1
R3(config-rtr)# router-id 3.3.3.3
R3(config-rtr)# no shutdown
R3(config-rtr)# interface Loopback0
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback1
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback2
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Loopback3
R3(config-if)# ipv6 eigrp 1
R3(config-if)# interface Serial0/0/0
R3(config-if)# ipv6 eigrp 1

R4(config)# ipv6 unicast-routing
R4(config)# ipv6 router eigrp 1
R4(config-rtr)# router-id 4.4.4.4
```



```
R4(config-rtr)# no shutdown
R4(config-rtr)# interface Loopback8
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback9
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback10
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Loopback11
R4(config-if)# ipv6 eigrp 1
R4(config-if)# interface Serial0/0/1
R4(config-if)# ipv6 eigrp 1
```

- Configure una ruta predeterminada conectada directamente en **IPv6-Edge** y propáguela en las actualizaciones de EIGRP.

```
IPv6-Edge(config)# ipv6 route ::/0 Serial0/1/0
IPv6-Edge(config)# ipv6 router eigrp 1
IPv6-Edge(config-rtr)# redistribute static
```

- En el **R3** y el **R4**, configure una ruta resumida EIGRP para las redes de loopback.

Redes de loopback del R3	Redes de loopback del R4
2001:DB8:1:1:A000::1/72	2001:DB8:1:1:BB80::1/76
2001:DB8:1:1:A100::1/72	2001:DB8:1:1:BB90::1/76
2001:DB8:1:1:A200::1/72	2001:DB8:1:1:BBA0::1/76
2001:DB8:1:1:A300::1/72	2001:DB8:1:1:BBB0::1/76
Resumen: 2001:DB8:1:1:A000::/70	Resumen: 2001:DB8:1:1:BB80::/74

```
R3(config)# interface Serial0/0/0
R3(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:1:A000::/70

R4(config)# interface Serial0/0/1
R4(config-if)# ipv6 summary-address eigrp 1 2001:DB8:1:1:BB80::/74
```

- El **R3** y el **R4** deben tener solo cuatro rutas EIGRP en la tabla de routing, contando la ruta externa predeterminada. **IPv6-Edge** debe tener solo dos rutas EIGRP en la tabla de routing.
- Verifique que el **R3** y el **R4** puedan hacer ping al **Server IPv6** (Servidor IPv6). El **Server IPv6** también debe poder hacer ping a cada dirección de loopback en el **R3** y el **R4**.

Tabla de calificación sugerida

Nota: actualmente, Packet Tracer no califica EIGRP para las rutas resumidas IPv6. Por lo tanto, parte de su calificación depende de la verificación de la tabla de routing por parte del instructor.

Trabajo calificado	Posibles puntos	Puntos obtenidos
Tabla de routing del IPv6-Edge	**10**	
Puntuación de Packet Tracer	**90**	
Puntuación total	**100**	

El router **IPv6-Edge** debería mostrar las siguientes rutas resumidas y no otras rutas **D**:

```
IPv6-Edge# show ipv6 route
<resultado omitido>
D   2001:DB8:1:1:A000::/70 [90/2297856]
     via FE80::2E0:F7FF:FE41:B901, Serial0/0/1
D   2001:DB8:1:1:BB80::/74 [90/2297856]
     via FE80::20A:41FF:FE80:4002, Serial0/0/0
```


Packet Tracer: Decodificación de nombres de la imagen del IOS (versión para el instructor)

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

Topología

Objetivos

Parte 1: Convención de nomenclatura para las imágenes del IOS 12.4

Parte 2: Convención de nomenclatura para las imágenes del IOS 15

Parte 3: Utilizar el comando show version para buscar las imágenes del IOS

Situación

Como técnico de red, es importante que conozca la convención de nomenclatura de la imagen del IOS, de modo que pueda determinar con rapidez la información importante sobre los sistemas operativos que se ejecutan actualmente en un dispositivo. En esta situación, la Company A (Empresa A) se fusionó con la Company B (Empresa B). La Company A heredó el equipo de red de la Company B. Se le asignó que registre las características para las imágenes del IOS en estos dispositivos.

Parte 1: Convención de nomenclatura para las imágenes del IOS 12.4

En la siguiente tabla, encontrará una lista con las imágenes del IOS 12.4. Decodifique el nombre de la imagen del IOS introduciendo la información correspondiente en cada columna.

Imágenes de IOS	Hardware	Conjunto de funciones	N.º de tren	Versión de mantenimiento	Identificador de tren	Identificador de recopilación
c1841-advipservicesk9-mz.124-24.T6.bin	1841	Advipservicesk9 (Advanced IP Services con cifrado seguro)	12.4	24	T	6
c1841-ipbasek9-mz.124-12.bin	1841	Ipbasek9 (servicios de IP Base con cifrado seguro)	12.4	12	M	
c2800nm-advipservicesk9-mz.124-15.T9.bin	2811	advipservicesk9	12.4	15	T	9
c2801-ipbasek9-mz.124-25f.bin	2801	ipbasek9	12.4	25	M	f
c2801-advsecurityk9-mz.124-18e.bin	2801	advsecurityk9 (Advanced Security con cifrado seguro)	12.4	18	M	e

¿Qué información brindan las letras “mz” en el nombre del archivo? La letra “m” indica que la imagen se ejecuta en la memoria de acceso aleatorio (RAM). La letra “z” indica que el archivo está en formato comprimido.

Parte 2: Convención de nomenclatura para las imágenes del IOS 15

En la siguiente tabla, encontrará una lista con las imágenes del IOS 15. Decodifique el nombre de la imagen del IOS introduciendo la información correspondiente en cada columna.

Imágenes de IOS	Hardware	Conjunto de funciones	Versión principal	Versión secundaria	Versión con nuevas características	Versión de mantenimiento	Recopilación de mantenimiento
c1900-universalk9-mz.SPA.153-2.T.bin	1900	universal	15	3	2	T	
c1900-universalk9-mz.SPA.152-4.M2.bin	1900	universal	15	2	4	M	2
c2900-universalk9-mz.SPA.151-4.M4.bin	2900	universal	15	1	4	M	4
c2900-universalk9-mz.SPA.152-3.T3.bin	2900	universal	15	2	3	T	3

Parte 3: Utilizar el comando show version para buscar las imágenes del IOS

Acceda a los routers en la topología. En el símbolo del sistema, emita el comando **show version** en ambos routers e indique la imagen del IOS de cada router en la tabla. Decodifique el nombre de la imagen del IOS introduciendo la información correspondiente en cada columna.

Imagen del IOS 12.4	Hardware	Conjunto de funciones	N.º de tren	Versión de mantenimiento	Identificador de tren	Identificador de recopilación
c1841-advipservicesk9-mz.124-15.T1.bin	1841	Advipservicesk9	12.4	15	T	1

Imagen del IOS 15	Hardware	Conjunto de funciones	Versión principal	Versión secundaria	Versión con nuevas características	Versión de mantenimiento	Recopilación de mantenimiento
c1900-universalk9-mz.SPA.151-1.M4.bin	1941	universal	15	1	1	M	4

Tabla de calificación sugerida

Sección de la actividad	Posibles puntos	Puntos obtenidos
Parte 1: Convención de nomenclatura para las imágenes del IOS 12.4	**30**	
Parte 2: Convención de nomenclatura para las imágenes del IOS 15	**20**	
Parte 3: Utilizar el comando show version para buscar las imágenes del IOS	**50**	
Puntuación total	**100**	

Packet Tracer: Uso de un servidor TFTP para actualizar una imagen del IOS de Cisco (versión para el instructor)

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

Topología

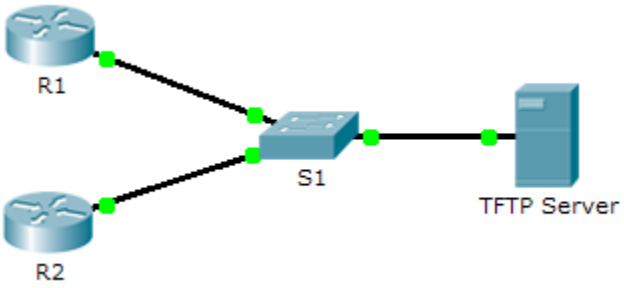


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.0	N/A
S1	VLAN 1	192.168.2.3	255.255.255.0	192.168.2.1
TFTP Server	NIC	192.168.2.254	255.255.255.0	192.168.2.1

Objetivos

Parte 1: Actualizar una imagen del IOS en un dispositivo de Cisco

Parte 2: Realizar una copia de seguridad de una imagen del IOS en un servidor TFTP

Situación

Un servidor TFTP puede contribuir a administrar el almacenamiento y las revisiones de las imágenes del IOS. Para cualquier red, es aconsejable tener una copia de seguridad de la imagen del software IOS de Cisco en caso de que la imagen de sistema en el router se dañe o se elimine accidentalmente. Un servidor TFTP también se puede utilizar para almacenar nuevas actualizaciones del IOS y, luego, se puede implementar en la red donde sea necesario. En esta actividad, actualizará las imágenes del IOS en los dispositivos de Cisco mediante un servidor TFTP. También realizará copias de seguridad de una imagen del IOS con el uso de un servidor TFTP.

Parte 1: Actualizar una imagen del IOS en un dispositivo de Cisco

Paso 1: Actualizar una imagen del IOS en un router.

a. Acceda al servidor TFTP y habilite el servicio TFTP.

b. Observe las imágenes del IOS que están disponibles en el servidor TFTP.

¿Cuáles son las imágenes del IOS almacenadas en el servidor que son compatibles con 1841? c1841-ipbase-mz.123-14.T7.bin, c1841-ipbasek9-mz.124-12.bin, and c1841-advipservicesk9-mz.124-15.T1.bin

c. Desde el **R1**, emita el comando **show flash:** y registre la memoria flash disponible. 49928533 bytes

d. Copie la imagen del IOS IPBase con cifrado seguro (ipbasek9) para el router 1841 del servidor TFTP al **R1**.

```
R1# copy tftp: flash:
Address or name of remote host []? 192.168.2.254
Source filename []? c1841-ipbasek9-mz.124-12.bin
Destination filename [c1841-ipbasek9-mz.124-12.bin]?

Accessing tftp://192.168.2.254/c1841-ipbasek9-mz.124-12.bin....
Loading c1841-ipbasek9-mz.124-12.bin from 192.168.2.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 16599160 bytes]

16599160 bytes copied in 3.44 secs (1079726 bytes/sec)
```

e. Verifique que la imagen del IOS se haya copiado en la memoria flash. ¿Cuántas imágenes del IOS se encuentran en la memoria flash:? 2

f. Utilice el comando **boot system** para cargar la imagen IPBase en la siguiente recarga.

```
R1(config)# boot system flash c1841-ipbasek9-mz.124-12.bin
```

g. Guarde la configuración y vuelva a cargar el **R1**.

h. Verifique que se haya cargado la imagen del IOS actualizada después de que se reinicie el **R1**.

Paso 2: Actualizar una imagen del IOS en un switch.

a. Acceda al servidor TFTP y copie la imagen c2960-lanbase-mz.122-25.FX.bin en el **S1**.

```
S1# copy tftp: flash:
```

b. Verifique que esta nueva imagen se indique primera en la lista del resultado de **show flash:**.

Nota: la primera imagen que se indica en el resultado de **show flash:** está cargada de manera predeterminada.

c. Vuelva a cargar el S1 y verifique que se haya cargado la nueva imagen en la memoria.

Parte 2: Realizar una copia de seguridad de una imagen del IOS en un servidor TFTP

a. En el R2, muestre el contenido de la memoria flash y registre la imagen del IOS. c1900-universalk9-mz.SPA.151-4.M4.bin

```
R2# show flash:
```

b. Utilice el comando **copy** para realizar una copia de seguridad de la imagen del IOS de la memoria flash del **R2** en un servidor TFTP.

```
R2# copy flash: tftp:
```

c. Acceda al servidor TFTP y verifique que se haya copiado la imagen del IOS en el servidor TFTP.

Packet Tracer: desafío de integración de habilidades (versión para el instructor)

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

Topología

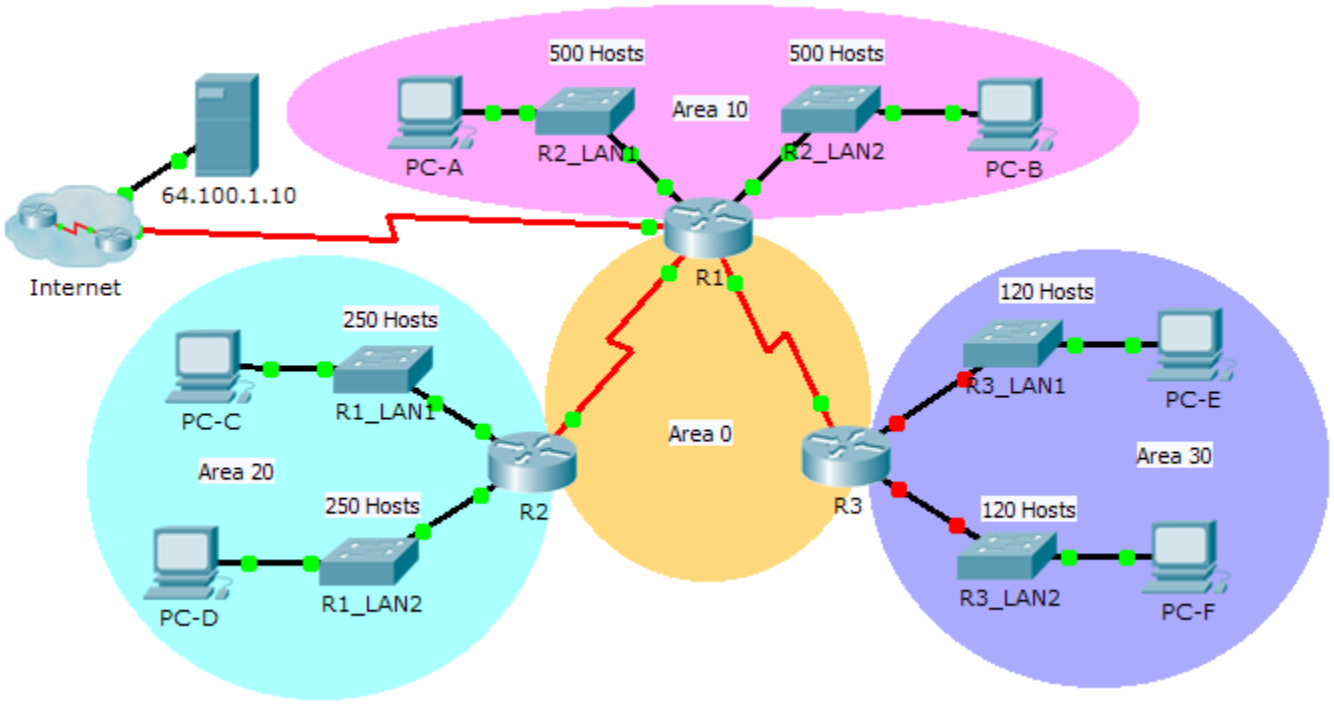


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.25.254	255.255.254.0	N/A
	G0/1	172.31.27.254	255.255.254.0	N/A
	S0/0/0	172.31.31.249	255.255.255.252	N/A
	S0/0/1	172.31.31.253	255.255.255.252	N/A
	S0/1/0	209.165.201.2	255.255.255.252	N/A
R2	G0/0	172.31.28.254	255.255.255.0	N/A
	G0/1	172.31.29.254	255.255.255.0	N/A
	S0/0/0	172.31.31.250	255.255.255.252	N/A
R3	G0/0	172.31.30.126	255.255.255.128	N/A
	G0/1	172.31.30.254	255.255.255.128	N/A
	S0/0/1	172.31.31.254	255.255.255.252	N/A
PC-A	NIC	172.31.24.1	255.255.254.0	172.31.25.254
PC-B	NIC	172.31.26.1	255.255.254.0	172.31.27.254
PC-C	NIC	172.31.28.1	255.255.255.0	172.31.28.254
PC-D	NIC	172.31.29.1	255.255.255.0	172.31.29.254
PC-E	NIC	172.31.30.1	255.255.255.128	172.31.30.126
PC-F	NIC	172.31.30.129	255.255.255.128	172.31.30.254

Situación

Como técnico de red familiarizado con el direccionamiento, el routing y la seguridad de red IPv4, ya está preparado para aplicar sus conocimientos y habilidades a una infraestructura de red. Su tarea es terminar de diseñar el esquema de direccionamiento IPv4 VLSM, implementar OSPF multiárea y proteger el acceso a las líneas VTY mediante listas de control de acceso.

Requisitos

- Las LAN del **R3** necesitan direccionamiento. Complete el diseño VLSM mediante las siguientes subredes disponibles en el espacio de direcciones **172.31.30.0/23** restante.
  1) Asigne la primera subred para 120 hosts a la LAN1 del **R3**.
  2) Asigne la segunda subred para 120 hosts a la LAN2 del **R3.**
- Registrar el esquema de direccionamiento completando la **tabla de direccionamiento**.
  - Asigne la última dirección IP en la subred a la interfaz del **R3** adecuada.
  - Asigne la primera dirección IP en la subred a la computadora.
- Configurar el direccionamiento para el **R3**, la **PC-E** y la **PC-F**.
- Implementar OSPF multiárea con la ID de proceso 1.

  - Asigne los enlaces seriales al área OSPF 0.
  - Configure la ID del router como **x.x.x.x** donde **x** es el número del router. Por ejemplo, la ID del router para el **R1** es 1.1.1.1.
  - Resuma las LAN en cada área y anúncielas usando una instrucción network.
    1) Asigne las LAN del R1 al área OSPF 10.
    2) Asigne las LAN del R2 al área OSPF 20.
    3) Asigne las LAN del R3 al área OSPF 30.
  - Evite que se envíen actualizaciones de routing a través de las interfaces LAN. No utilizar el argumento **predeterminado**.
- Implementar el routing predeterminado en Internet.
  - Configure el **R1** con una ruta predeterminada conectada directamente.
  - Anuncie la ruta predeterminada al **R2** y al **R3**.
- Configurar la autenticación MD5 en las interfaces seriales.
  - Utilice **1** como la clave.
  - Utilice **cisco123** como la cadena de clave.
- Limitar el acceso a VTY al **R1**.
  - Configure una ACL n.º 1.
  - Solamente la **PC-A** tiene permitido acceder al **R1** mediante telnet.

```
!------------------------
!R1
!------------------------
en
conf t
!
interface Serial0/0/0
 ip ospf message-digest-key 1 md5 cisco123
!
interface Serial0/0/1
 ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
 router-id 1.1.1.1
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 172.31.31.248 0.0.0.3 area 0
 network 172.31.31.252 0.0.0.3 area 0
 network 172.31.24.0 0.0.3.255 area 10
 default-info orig
```



```
!
access-list 1 permit host 172.31.24.1
access-list 1 deny any
!or without the implicity deny is also acceptable
!access-list 1 permit host 172.31.24.1
!
ip route 0.0.0.0 0.0.0.0 s0/1/0
!
line vty 0 15
 access-class 1 in
!
end

!----------------------------
!R2
!----------------------------
!
en
conf t
!
interface Serial0/0/0
 ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
 router-id 2.2.2.2
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 172.31.31.248 0.0.0.3 area 0
 network 172.31.28.0 0.0.1.255 area 20
!
!
end

!--------------------------------
!R3
!--------------------------------
!
en
conf t
```



```
!
interface GigabitEthernet0/0
 ip address 172.31.30.126 255.255.255.128
 no shut
!
interface GigabitEthernet0/1
 ip address 172.31.30.254 255.255.255.128
 no shut
!
interface Serial0/0/1
 ip ospf message-digest-key 1 md5 cisco123
!
router ospf 1
 router-id 3.3.3.3
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 172.31.31.252 0.0.0.3 area 0
 network 172.31.30.0 0.0.0.255 area 30
!
end
```

