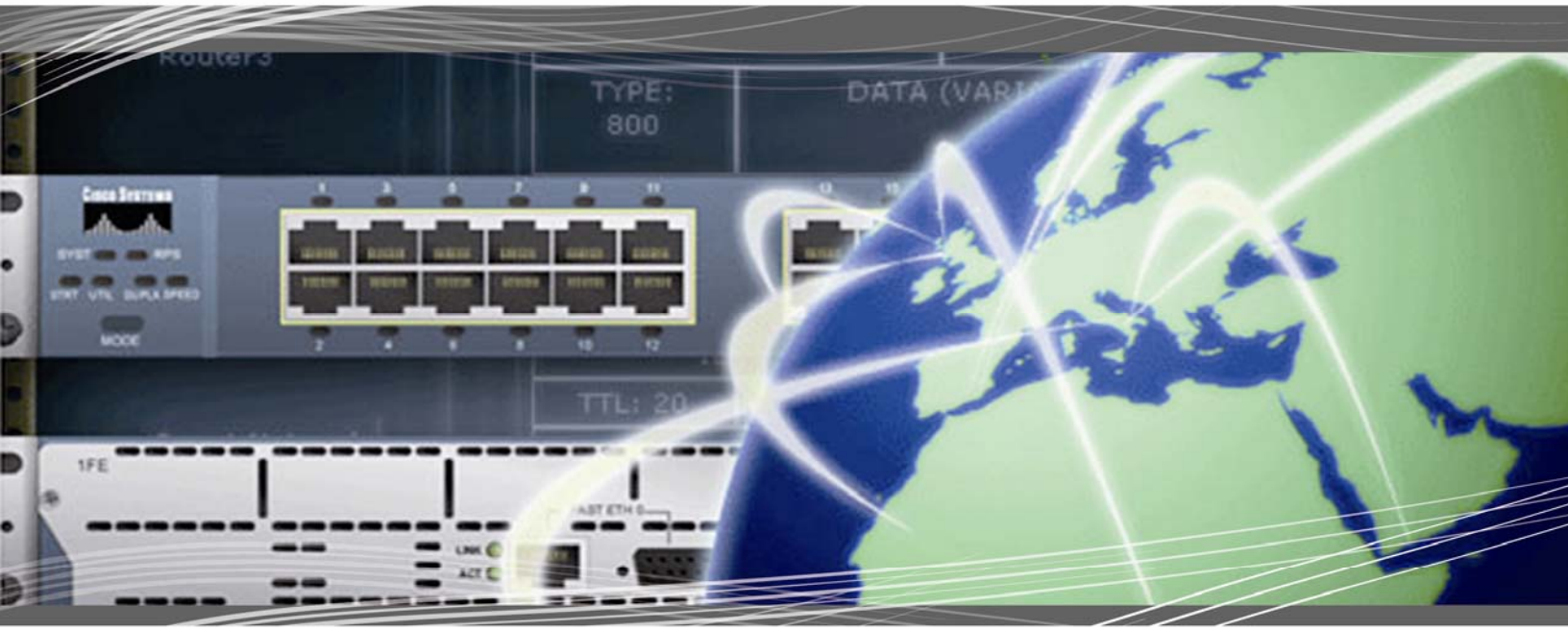
Cisco | Networking Academy®
Mind Wide Open™



CCNA Exploration 4.0

Acceso a la WAN

Manual de prácticas de laboratorio del Packet Tracer para el estudiante

Actividad de PT 1.5.1: Desafío de integración de aptitudes de Packet Tracer

Diagrama de topología

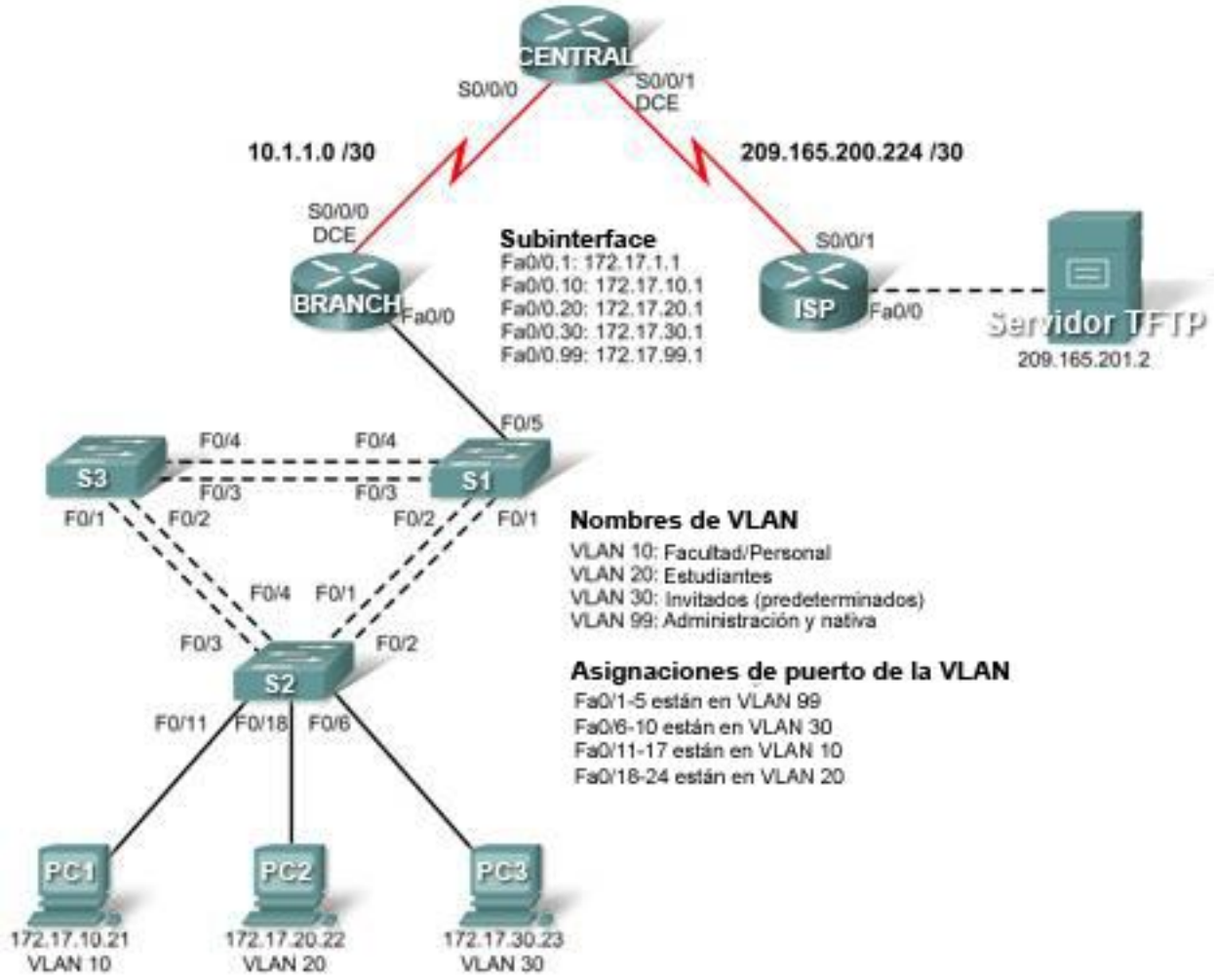


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	**S0/0/1**	209.165.200.225	255.255.255.252	No aplicable
	Fa0/0	209.165.201.1	255.255.255.252	No aplicable
CENTRAL	**S0/0/0**	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	209.165.200.226	255.255.255.252	No aplicable
BRANCH	**S0/0/0**	10.1.1.1	255.255.255.252	No aplicable
	Fa0/0.1	172.17.1.1	255.255.255.0	No aplicable
	Fa0/0.10	172.17.10.1	255.255.255.0	No aplicable
	Fa0/0.20	172.17.20.1	255.255.255.0	No aplicable
	Fa0/0.30	172.17.30.1	255.255.255.0	No aplicable
	Fa0/0.99	172.17.99.1	255.255.255.0	No aplicable
S1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.12	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.13	255.255.255.0	172.17.99.1
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**	172.17.30.23	255.255.255.0	172.17.30.1
Servidor Web	**NIC**	209.165.201.2	255.255.255.252	209.165.201.1

Objetivos de aprendizaje

- Configurar el enrutamiento estático y predeterminado
- Agregar y conectar el router BRANCH
- Agregar y conectar los switches
- Agregar y conectar las PC
- Realizar las configuraciones básicas del dispositivo
- Configurar el enrutamiento OSPF
- Configurar el STP
- Configurar el VTP
- Configurar las VLAN
- Verificar la conectividad de extremo a extremo

Introducción

Esta actividad abarca muchas de las aptitudes que adquirió en los primeros tres cursos de Exploration. Las aptitudes incluyen la creación de una red, la aplicación de un esquema de direccionamiento, la configuración del enrutamiento, las VLAN, el STP y el VTP y la prueba de la conectividad. Debe revisar esas aptitudes antes de proceder. Además, esta actividad le brinda una oportunidad de revisar los conceptos básicos del programa Packet Tracer Packet Tracer está integrado a todo este curso. Debe saber navegar el ámbito de Packet Tracer para completar este curso. Utilice los tutoriales si necesita una revisión de los fundamentos de Packet Tracer. Los tutoriales se encuentran en el menú **Ayuda** de Packet Tracer.

Nota: En esta actividad se evalúan más de 150 aspectos. Por lo tanto, es posible que no pueda ver el aumento del porcentaje de finalización cada vez que ingresa un comando. La contraseña EXEC del usuario es **cisco** y la contraseña de EXEC privilegiado es **class**.

Tarea 1: Configurar el enrutamiento estático y predeterminado

Paso 1. Configurar el enrutamiento estático desde el ISP a CENTRAL.

Utilice el diagrama de topología para configurar el ISP con rutas estáticas hacia todas las redes. Cada red se puede alcanzar a través de S0/0/1 desde el ISP. Utilice el parámetro de la interfaz de salida para configurar rutas estáticas hacia las siguientes redes:

- 10.1.1.0/30
- 172.17.1.0/24
- 172.17.10.0/24
- 172.17.20.0/24
- 172.17.30.0/24
- 172.17.99.0/24

Paso 2. Configurar el enrutamiento predeterminado desde CENTRAL al ISP.

Configure una ruta predeterminada en CENTRAL mediante el parámetro de la interfaz de salida para enviar todo el tráfico predeterminado al ISP.

Paso 3. Probar la conectividad al servidor Web.

Ahora CENTRAL debe poder hacer ping con éxito al servidor Web en 209.165.201.2.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 4%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Agregar y conectar el router BRANCH

Paso 1. Agregar el router BRANCH.

Haga clic en **Dispositivos personalizados** y agregue un router 1841 a la topología. Utilice la ficha **Configuración** para cambiar el Nombre de visualización y el Nombre del host a BRANCH. Los nombres de visualización distinguen mayúsculas de minúsculas

Paso 2. Conectar BRANCH a CENTRAL.

- Conecte BRANCH a CENTRAL
- Configure el enlace entre BRANCH y CENTRAL
- Utilice una frecuencia de reloj de **64 000** bps

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 8%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Agregar y conectar los switches

Consulte la topología para obtener información sobre ubicación, nombres de switches e interfaces.

Paso 1. Agregar los switches S1, S2 y S3 mediante el modelo 2960.

Paso 2. Conectar S1 a BRANCH.

Paso 3. Conectar S1 a S2.

Paso 4. Conectar S1 a S3.

Paso 5. Conectar S2 a S3.

Paso 6. Verificar los resultados.

Su porcentaje de finalización debe ser del 28%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Agregar y conectar las PC

Utilice las interfaces especificadas en el diagrama de topología y la tabla de direccionamiento.

Paso 1. Agregar las PC1, PC2 y PC3.

Paso 2. Conectar las PC1, PC2 y PC3 a S2.

Paso 3. Configurar las PC.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 41%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Realizar la configuración básica del dispositivo

Paso 1. Configurar los comandos básicos de BRANCH, S1, S2 y S3.

Los comandos básicos de configuración deben incluir nombre del host, contraseña EXEC, título, consola y líneas vty.

Paso 2. Configurar las subinterfaces de Fast Ethernet en BRANCH.

No olvide configurar la encapsulación 802.1q y las configuraciones de VLAN para cada una de las subinterfaces. El tercer octeto para cada dirección de subinterfaz corresponde al número de VLAN. Por ejemplo: la subinterfaz Fa0/030 utiliza la dirección IP 172.17.**30**.1 y pertenece a la VLAN 30. La VLAN 99 es la VLAN nativa

Paso 3. Configurar los switches.

- Configure la interfaz VLAN 99.
- Configure la gateway predeterminada.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 60%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Configurar el enrutamiento OSPF

Paso 1. Configurar OSPF en CENTRAL y propagar la ruta predeterminada.

- Configure OSPF mediante el ID de proceso 1.
- Utilice OSPF Área 0.
- Agregue sólo la red compartida con BRANCH.
- Propague la ruta predeterminada a vecinos OSPF.

Paso 2. Configurar OSPF en BRANCH.

- Configure OSPF mediante el ID de proceso 1.
- Utilice OSPF Área 0.
- Agregue todas las redes que enruta BRANCH.

Paso 3. Deshabilitar actualizaciones OSPF en las interfaces apropiadas de CENTRAL y BRANCH.

Deshabilite las actualizaciones OSPF en todas las interfaces LAN y en el ISP.

Paso 4. Probar la conectividad.

BRANCH debe poder hacer ping con éxito al servidor Web en 209.165.201.2.

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 69%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 7: Configurar el STP

Paso 1: Asegurarse de que S1 sea el puente raíz.

Establezca las prioridades en 4096.

Paso 2: Verificar que S1 sea el puente raíz.

Paso 3: Verificar los resultados.

Su porcentaje de finalización debe ser del 72%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 8: Configurar el VTP

Paso 1: Configurar el modo VTP en los tres switches.

Configure S1 como el servidor. Configure S2 y S3 como los clientes.

Paso 2: Configurar el nombre de dominio VTP en los tres switches.

Utilice **CCNA** como el nombre de dominio VTP.

Paso 3: Configurar la contraseña de dominio VTP en los tres switches.

Utilice **cisco** como la contraseña de dominio VTP.

Paso 4: Verificar los resultados.

Su porcentaje de finalización debe ser del 77%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 9: Configurar el enlace troncal

Paso 1: Configurar el enlace troncal en S1, S2 y S3.

Configure las interfaces apropiadas en el modo de enlace troncal y asigne VLAN 99 como la VLAN nativa.

Paso 2: Verificar los resultados.

Su porcentaje de finalización debe ser del 94%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 10: Configurar las VLAN

Paso 1: Configurar el S1 con las VLAN.

Los nombres de las VLAN distinguen mayúsculas de minúsculas. Agregar y nombrar las cuatro VLAN mediante las siguientes especificaciones:

- VLAN 10 – **Cuerpo docente/personal**
- VLAN 20 – **Estudiantes**
- VLAN 30 – **Guest (Predeterminado)**
- VLAN 99 – **Administración&Nativa**

Paso 2. Verificar que S2 y S3 hayan recibido las configuraciones de VLAN de S1.

Paso 3. Configurar los puertos conectados a las PC en S2 para su acceso y asignar a cada puerto la VLAN apropiada.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 11: Verificar la conectividad de extremo a extremo

Paso 1. Verificar que la PC1, PC2 y PC3 puedan hacer ping entre sí.

Paso 2. Verificar que la PC1, PC2 y PC3 puedan hacer ping al servidor Web.

Actividad de PT 2.1.7: Resolución de problemas de una interfaz serial

Diagrama de topología

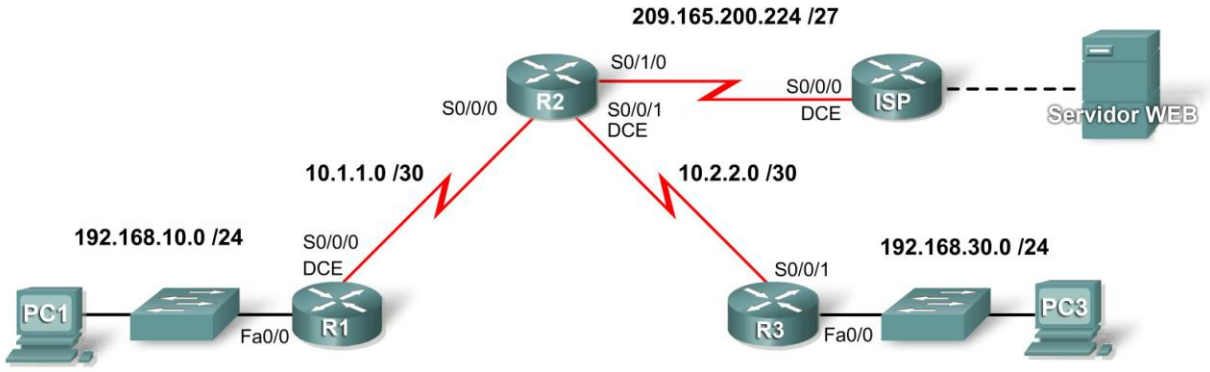


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.224
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	NIC	209.165.200.2	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0

Objetivos de aprendizaje

- Probar la conectividad
- Investigar problemas de conectividad mediante la recopilación de información
- Implementar la solución y probar la conectividad

Introducción

En esta actividad, sólo tiene acceso a la petición de entrada de comandos de PC1 y PC3. Para solucionar los problemas en los routers e implementar las soluciones, debe establecer una conexión Telnet de la PC1 o la PC3. Esta actividad se completa cuando alcanza el 100% y la PC1 puede hacer ping a la PC3.

Tarea 1: Probar la conectividad

Paso 1: Utilizar el ping para probar la conectividad de extremo a extremo.

Espere a que las luces de enlace en S1 y S3 cambien de ámbar a verde. Luego, desde la petición de entrada de comandos de PC1, haga ping a PC3. Este ping debe fallar.

Paso 2: Utilizar traceroute para detectar dónde falla la conectividad.

En la petición de entrada de comandos de PC1, utilice el comando **tracert** para determinar dónde falla la conexión.

```
Línea de comando 1.0 de la PC de Packet Tracer
PC>tracert 192.168.30.10
```

Utilice la combinación de teclas Ctrl-C para salir del comando **tracert**. ¿Cuál es el último router que responde a **tracert**? _____

Paso 3: Documentar los síntomas del problema.

_____

_____

Tarea 2: Reunir información acerca del problema

Paso 1: Acceder al último router que respondió al paquete traceroute.

Establezca una conexión Telnet al último router que respondió a **tracert**. Utilice **cisco** y **class** como contraseñas de Telnet y enable, respectivamente.

Paso 2: Utilizar los comandos de resolución de problemas para investigar por qué este router quizá no envía el rastreo al siguiente salto.

Utilice los siguientes comandos para aislar problemas específicos con la interfaz serial:

- **show ip interface brief**
- **show interfaces serial**
- **show controllers serial**

El comando **show ip interface brief** indica si una interfaz se configuró correctamente y si se puso en línea correctamente con el comando **no shutdown**.

El comando **show interface serial** brinda más información acerca de la interfaz que está fallando. Muestra uno de cinco posibles estados:

- Serial x is down, line protocol is down
- Serial x is up, line protocol is down
- Serial x is up, line protocol is up (looped)
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

El comando **show interface serial** también muestra qué encapsulación se está utilizando en la interfaz. Para esta actividad, todos los routers deben utilizar la encapsulación HDLC.

El comando **show controllers serial** indica el estado de los canales de la interfaz y si un cable está conectado a la interfaz o no.

Es probable que también deba verificar la configuración del router conectado para detectar el problema.

Paso 3: Documentar el problema y sugerir soluciones.

¿Cuáles son algunas posibles razones por las que puede fallar un enlace serial?

_____

_____

_____

Tarea 3: Implementar la solución y probar la conectividad

Paso 1: Realizar los cambios según las soluciones sugeridas en la Tarea 2.

Paso 2: Utilizar el ping para probar la conectividad de extremo a extremo.

En la línea de comandos del router o la PC1, utilice los comandos **ping** y **tracert** para probar la conectividad a la PC3.

Si los pings fallan, regrese a la Tarea 2 para continuar con la resolución de problemas. Es posible que en algún momento deba comenzar la resolución de problemas desde la PC3.

Paso 3. Verificar los resultados.

Haga clic en **Verificar resultados** y luego en la ficha **Pruebas de conectividad**. La Prueba de conectividad debe tener éxito ahora.

Paso 4. Resumir los resultados.

Problema 1:_____

Solución 1:_____

Problema 2:_____

Solución 2:_____

Problema 3:_____

Solución 3:_____

Actividad de PT 2.3.4: Configuración de encapsulaciones punto a punto

Diagrama de topología

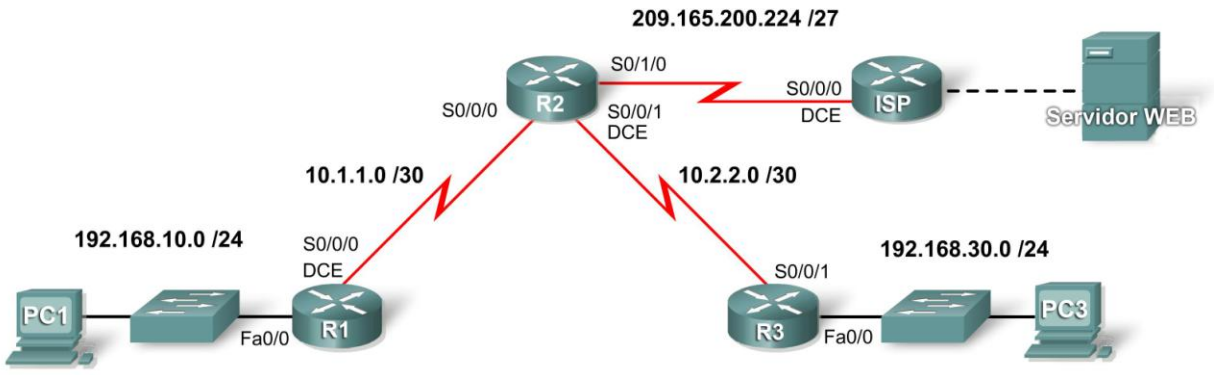


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/0**	192.168.10.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
R2	**S0/0/0**	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
	S0/1/0	209.165.200.225	255.255.255.252	No aplicable
R3	**Fa0/0**	192.168.30.1	255.255.255.0	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
ISP	**S0/0/0**	209.165.200.226	255.255.255.252	No aplicable
	Fa0/0	209.165.200.1	255.255.255.252	No aplicable
Servidor Web	**NIC**	209.165.200.2	255.255.255.252	209.165.200.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos de aprendizaje

- Revisar las configuraciones de enrutamiento
- Configurar PPP como el método de encapsulación
- Configurar HDLC como el método de encapsulación

Tarea 1: Revisar las configuraciones de enrutamiento.

Paso 1. Ver las configuraciones en ejecución en todos los routers.

Observe las configuraciones de enrutamiento, tanto las estáticas como las dinámicas. Al final del capítulo, configurará ambos tipos de enrutamiento en la actividad de Desafío de integración de aptitudes de Packet Tracer.

Paso 2. Probar la conectividad entre las PC y el servidor Web.

1. Abra una línea de comandos desde PC1.
2. Ejecute el comando **ping 209.165.200.2**.
3. Repita el mismo procedimiento con PC3.

Ambos comandos **ping** deben tener éxito. Recuerde esperar el tiempo suficiente para que el STP y el OSPF converjan.

Tarea 2: Configurar PPP como el método de encapsulación.

Paso 1. Configurar R1 para utilizar la encapsulación PPP con R2.

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation ppp
```

Paso 2. Configurar R2 para utilizar la encapsulación PPP con R1 y R3.

Paso 3. Configurar R3 para utilizar la encapsulación PPP con R2.

Paso 4. Probar la conectividad entre las PC y el servidor Web.

¿Por qué el OSPF debe converger después de que cambie la encapsulación?

_____

_____

_____

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 67%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar HDLC como el método de encapsulación

Paso 1. Configurar ISP para utilizar la encapsulación HDLC con R2.

```
ISP(config)#interface serial0/0/0
ISP(config-if)#encapsulation hdlc
ISP(config-if)#no shutdown
```

Paso 2. Configurar R2 para utilizar la encapsulación HDLC con el ISP.

```
R2(config)#interface serial0/1/0
R2(config-if)#encapsulation hdlc
R2(config-if)#no shutdown
```

Nota: Si bien Verificar resultados puede mostrar 100%, las Pruebas de conectividad fallarán a menos que configure el comando **no shutdown** en R2 y el ISP.

Paso 3. Probar la conectividad entre las PC y el servidor Web.

Utilice una PDU simple de Packet Tracer para verificar la conectividad. Esto debe tener éxito.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Actividad de PT 2.4.6: Configuración de autenticación PAP y CHAP

Diagrama de topología

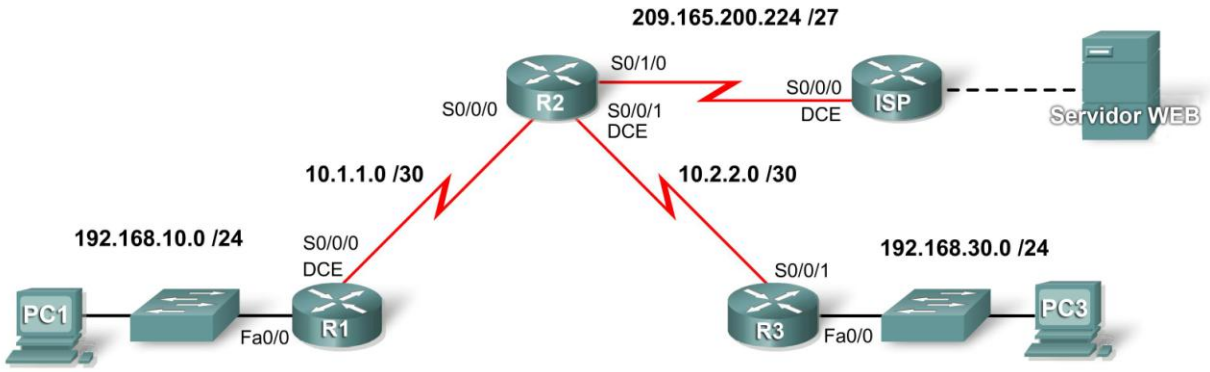


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	NIC	209.165.200.2	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0

Objetivos de aprendizaje

- Configurar el enrutamiento OSPF
- Configurar la autenticación PAP entre R1 y R2
- Configurar la autenticación CHAP entre R3 y R2

Introducción

La encapsulación PPP permite dos tipos diferentes de autenticación: Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación de intercambio de señales (CHAP). PAP utiliza una contraseña no cifrada, mientras que CHAP invoca un hash de una sola vía que brinda más seguridad que el PAP. En esta actividad, configurará tanto PAP como CHAP y además revisará la configuración de enrutamiento OSPF.

Tarea 1: Configurar el enrutamiento OSPF

Paso 1: Habilitar OSPF en R1.

Con un *process-ID* de **1**, utilice el comando **router ospf 1** para habilitar el enrutamiento OSPF.

Paso 2: Configurar sentencias de red en R1.

En el modo de configuración del router, agregue todas las redes conectadas al R1 mediante el comando **network**. El parámetro *area-id* de OSPF es **0** para todas las sentencias **network** en esta topología.

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

Paso 3: Configurar sentencias de red en R2 y R3.

Repetir los pasos 1 y 2 para los routers R2 y R3. Utilice la tabla de direccionamiento para determinar cuáles son las sentencias correctas. En el R2, *no* publique la red 209.165.202.224/30. Configurará una ruta predeterminada en el próximo paso.

Paso 4: Establecer y redistribuir la ruta predeterminada de OSPF.

- En el R2, cree una ruta estática predeterminada para el ISP con el comando **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- En la petición de entrada del router, ejecute el comando **default-information originate** para incluir la ruta estática en las actualizaciones de OSPF que se envían desde el R2.

Paso 5: Verificar la conectividad de extremo a extremo.

En este punto de su configuración, todos los dispositivos deben poder hacer ping a todas las ubicaciones.

Haga clic en **Verificar resultados** y a continuación haga clic en **Pruebas de conectividad**. El estado de ambas pruebas debe ser “Correcto”. Las tablas de enrutamiento para R1, R2 y R3 deben estar completas. El R1 y el R3 deben tener una ruta predeterminada, tal como se muestra en la siguiente tabla de enrutamiento para R1:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
<resultado omitido>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0
```

```
     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```

Paso 6: Verificar los resultados.

Su porcentaje de finalización debe ser del 40%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar la autenticación PAP

Paso 1: Configurar el R1 para que utilice la autenticación PAP con el R2.

- Con el R1 en el modo de configuración global, escriba el comando **username R2 password cisco123**. Este comando permite que el router remoto R2 se conecte al R1 cuando utiliza la contraseña **cisco 123**.
- Cambie a PPP el tipo de encapsulación de la interfaz s0/0/0 del R1 mediante el comando **encapsulation ppp**.
- Mientras se encuentre en la interfaz serial, configure la autenticación PAP con el comando **ppp authentication pap**.
- Configure el nombre de usuario y la contraseña que se enviarán al R2 con el comando **ppp pap sent-username R1 password cisco123**. Si bien Packet Tracer no califica el comando **ppp pap sent-username R1 password cisco123**, el comando es necesario para poder configurar la autenticación PAP con éxito.
- Regrese al modo exec privilegiado y utilice el comando **show ip interface brief** para observar que el enlace entre R1 y R2 se ha desactivado.

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    down
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Paso 2: Configurar el R2 para que utilice la autenticación PAP con el R1.

Repita el Paso 1 para el R2 mediante el enlace serial al R1.

Recuerde que el nombre utilizado en el comando **username** *name* **password** *password* siempre es el nombre del router remoto, pero en el comando **ppp pap sent-username** *name* **password** *password*, el nombre es el del router de origen.

Nota: Si bien Packet Tracer activará el enlace, en equipos reales es necesario ejecutar **shutdown** y luego **no shutdown** en la interfaz para obligar a PAP a que vuelva a autenticarse. También puede simplemente volver a cargar los routers.

Paso 3: Probar la conectividad entre la PC1 y el servidor Web.

Utilice el comando **show ip interface brief** para observar que el enlace entre R1 y R2 ahora está activado. El acceso al servidor Web desde R1 debe haberse restablecido. Pruébelo enviando un ping desde la PC1 al servidor Web.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Paso 4: Verificar los resultados.

Su porcentaje de finalización debe ser del 70%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar la autenticación CHAP

Paso 1: Configurar el R3 para que utilice la autenticación CHAP con el R2.

- En el modo de configuración global para R3, escriba **username R2 password cisco123**.
- En la interfaz s0/0/1, ejecute los comandos **encapsulation ppp** y **ppp authentication chap**, lo que habilitará la encapsulación PPP y la autenticación CHAP.
- Utilice el comando **show ip interface brief** para observar que el enlace entre R2 y R3 ahora está desactivado.

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

Paso 2: Configurar el R2 para que utilice la autenticación CHAP con el R3.

Repita el Paso 1 para el R2, pero cambie el nombre de usuario a R3, ya que el R3 es el router remoto.

Paso 3: Probar la conectividad entre la PC3 y el servidor Web.

Mediante el comando **show ip interface brief**, debe ver que el enlace entre R2 y R3 ahora está activado y la PC3 puede hacer ping al servidor Web.

Paso 4: Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Actividad 2.5.1: Configuración básica de PPP

Diagrama de topología

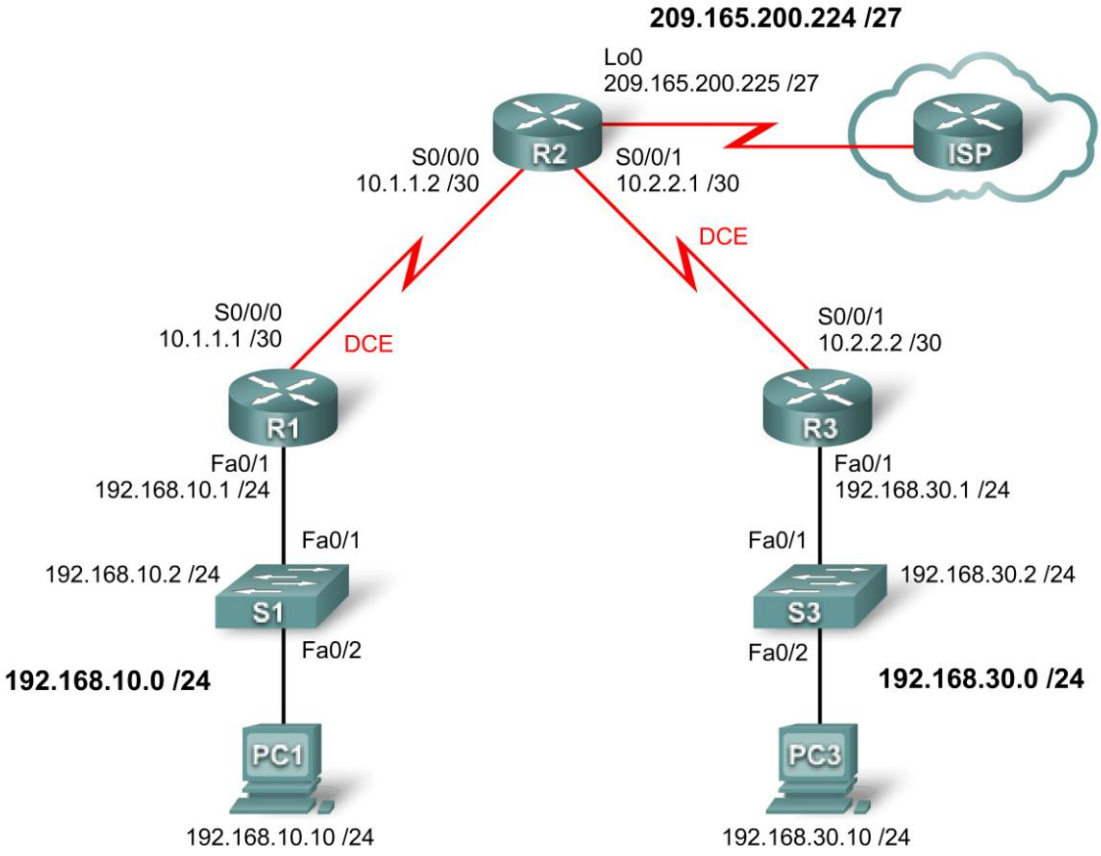


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/1**	192.168.10.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
R2	**Lo0**	209.165.200.225	255.255.255.224	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
R3	**Fa0/1**	192.168.30.1	255.255.255.0	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos de aprendizaje

- Configurar el enrutamiento OSPF en todos los routers
- Configurar la encapsulación PPP en todas las interfaces seriales
- Interrumpir intencionalmente y restablecer la encapsulación PPP
- Configurar la autenticación PPP, PAP y CHAP
- Interrumpir intencionalmente y restablecer la autenticación PPP, PAP y CHAP

Introducción

En esta actividad de laboratorio, aprenderá a configurar la encapsulación PPP en enlaces seriales utilizando la red que se muestra en el diagrama de topología. También aprenderá a restaurar los enlaces seriales a su encapsulación HDLC predeterminada. Finalmente, configurará la autenticación PPP PAP y la autenticación PPP CHAP.

Tarea 1: Configurar OSPF en los routers

Paso 1. Habilitar el enrutamiento OSPF en R1, R2 y R3.

Ejecute el comando **router ospf** con un ID de proceso de 1 para ingresar a la petición de entrada de la configuración del router. Para cada router, publique todas las redes conectadas.

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

R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.31 area 0
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.30.0 0.0.0.255 area 0
R3(config-router)#
```

Paso 2. Verificar que haya conectividad de red total.

Utilice los comandos **show ip route** y **ping** para verificar la conectividad.

```
R1#show ip route

<resultado omitido>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:02:22, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:00:08, Serial0/0/0
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.1.1.2, 00:02:22, Serial0/0/0

R1#ping 192.168.30.1

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R1#

R2#show ip route

<resultado omitido>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:02:31, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:20, Serial0/0/1
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, Loopback0

R2#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#

R3#show ip route

<resultado omitido>

     10.0.0.0/30 is subnetted, 2 subnets
O       10.1.1.0 [110/128] via 10.2.2.1, 00:00:34, Serial0/0/1
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/129] via 10.2.2.1, 00:00:34, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.2.2.1, 00:00:34, Serial0/0/1

R3#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R3#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R3#
```

Tarea 2: Configurar la encapsulación PPP en interfaces seriales

Paso 1. Utilizar el comando show interface para verificar si HDLC es la encapsulación serial predeterminada.

La encapsulación serial predeterminada en los routers Cisco es HDLC. Utilice el comando **show interface** en cualquiera de las interfaces seriales para visualizar la encapsulación actual.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<resultado omitido>
```

Si verifica todas las interfaces seriales activas, verá que la encapsulación se establece en HDLC.

Paso 2. Cambiar la encapsulación de las interfaces seriales de HDLC a PPP.

Cambie el tipo de encapsulación en el enlace entre R1 y R2, y observe los efectos.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#

R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#
```

¿Qué sucede cuando un extremo del enlace serial se encapsula con PPP y el otro extremo del enlace se encapsula con HDLC?

¿Qué sucede cuando la encapsulación PPP se configura en cada extremo del enlace serial?

Paso 3. Cambiar la encapsulación de HDLC a PPP en ambos extremos del enlace serial entre R2 y R3.

```
R2(config)#interface serial0/0/1
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
```

```
 state to down
R3(config)#interface serial 0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
```

¿Cuándo se activa el protocolo de línea del enlace serial y se restablece la adyacencia OSPF?

Paso 4. Verificar que PPP sea ahora la encapsulación de las interfaces seriales.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<resultado omitido>

R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<resultado omitido>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<resultado omitido>
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<resultado omitido>
```

Tarea 3: Interrumpir y restablecer la encapsulación PPP

Paso 1. Restablecer las dos interfaces seriales en R2 a su encapsulación HDLC predeterminada.

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
```

¿Por qué es útil interrumpir intencionalmente una configuración?

_____

_____

¿Por qué ambas interfaces se desactivan, luego se activan y finalmente vuelven a desactivarse?

_____

_____

¿Puede pensar en otra manera de cambiar la encapsulación de una interfaz serial de PPP a la encapsulación HDLC predeterminada que no sea la utilización del comando encapsulation hdlc? (Ayuda: está relacionada con el comando **no**).

_____

_____

_____

_____

_____

Paso 2. Restablecer las dos interfaces seriales en R2 a la encapsulación PPP.

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

Tarea 4: Configurar la autenticación PPP

Paso 1. Configurar la autenticación PPP PAP en el enlace serial entre R1 y R2.

```
R1(config)#username R1 password cisco
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#ppp pap sent-username R2 password cisco
```

¿Qué sucede cuando la autenticación PPP PAP sólo se configura en un extremo del enlace serial?

_____

_____

```
R2(config)#username R2 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R1 password cisco
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
```

¿Qué sucede cuando la autenticación PPP PAP se configura en ambos extremos del enlace serial?

_____

Paso 2. Configurar la autenticación PPP CHAP en el enlace serial entre R2 y R3.

En la autenticación PAP, la contraseña no está encriptada. Si bien es mejor que no tener ningún tipo de autenticación, es mucho más preferible encriptar la contraseña que se envía a través del enlace. CHAP encripta la contraseña.

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
R2(config-if)#
R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

¿Observe que el protocolo de línea en la interfaz serial 0/0/1 cambia su estado a UP incluso antes de que se configure la interfaz para la autenticación CHAP. Puede imaginar por qué sucede esto?

_____

_____

Tarea 5: Interrumpir intencionalmente y restablecer la autenticación PPP CHAP

Paso1. Interrumpir la autenticación PPP CHAP.

En el enlace serial entre R2 y R3, cambie el protocolo de autenticación en la interfaz serial 0/0/1 a PAP.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#^Z
R2#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

¿El cambio de protocolo de autenticación a PAP en la interfaz serial 0/0/1 produce la interrupción de la autenticación entre R2 y R3?

_____

Paso 2. Restablecer la autenticación PPP CHAP en el enlace serial.

Observe que no es necesario recargar el router para que este cambio surta efecto.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

Paso 3. Interrumpir intencionalmente la autenticación PPP CHAP mediante el cambio de la contraseña del R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password ciisco
R3(config)#^Z
R3#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
```

¿Cuál es el estado del protocolo de línea en la serial 0/0/1 después de la recarga?

_____

Paso 4. Restablecer la autenticación PPP CHAP mediante el cambio de la contraseña del R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

Observe que el enlace se activó nuevamente. Pruebe la conectividad haciendo ping desde la PC1 a la PC3.

Actividad 2.5.2: Desafío de configuración de PPP

Topología

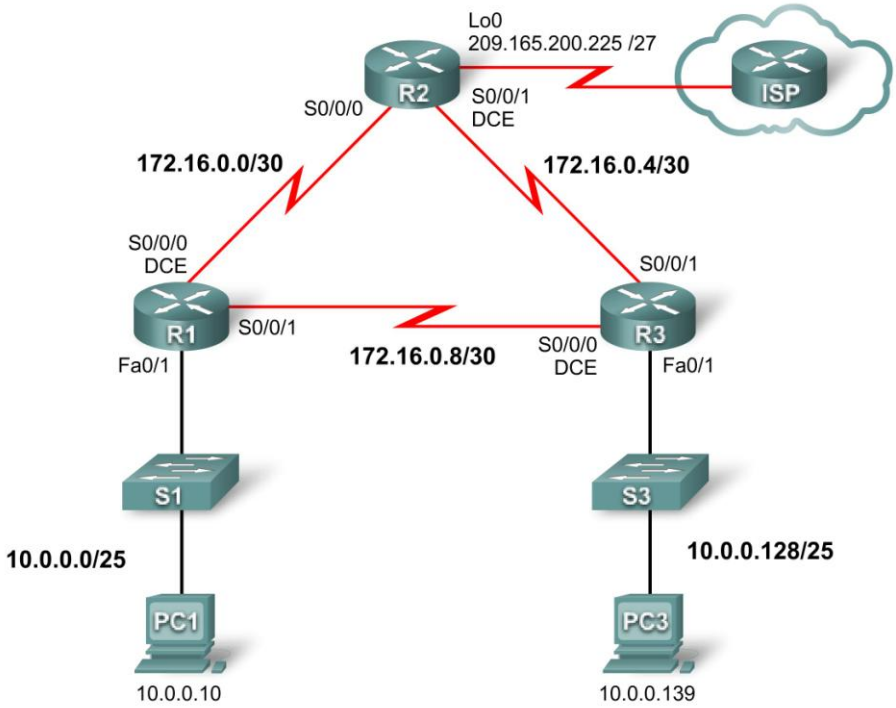


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/1**	10.0.0.1	255.255.255.128	No aplicable
	S0/0/0	172.16.0.1	255.255.255.252	No aplicable
	S0/0/1	172.16.0.9	255.255.255.252	No aplicable
R2	**Lo0**	209.165.200.161	255.255.255.224	No aplicable
	S0/0/0	172.16.0.2	255.255.255.252	No aplicable
	S0/0/1	172.16.0.5	255.255.255.252	No aplicable
R3	**Fa0/1**	10.0.0.129	255.255.255.128	No aplicable
	S0/0/0	172.16.0.10	255.255.255.252	No aplicable
	S0/0/1	172.16.0.6	255.255.255.252	No aplicable
PC1	**NIC**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**NIC**	10.0.0.139	255.255.255.128	10.0.0.129

Objetivos de aprendizaje

- Configurar y activar interfaces
- Configurar el enrutamiento OSPF en todos los routers
- Configurar la encapsulación PPP en todas las interfaces seriales
- Configurar la autenticación PPP CHAP

Introducción

En esta actividad, configurará la encapsulación PPP en enlaces seriales a través de la red que se muestra en el diagrama de topología. Además, configurará la autenticación PPP CHAP. Si necesita ayuda, consulte la práctica de laboratorio o actividad Configuración básica de PPP, pero trate de hacer cuanto más pueda sin recurrir a la ayuda.

Tarea 1: Configurar y activar las direcciones serial y Ethernet

Paso 1. Configurar las interfaces de R1, R2 y R3.

El esquema de direccionamiento figura en la topología y en la tabla de direccionamiento. Se proporcionan algunas direcciones de interfaces pero para algunas interfaces sólo se proporciona la red. Cuando sólo tenga la dirección de red, puede utilizar cualquier dirección válida de la red especificada para poder calificarla correctamente en el Packet Tracer.

Configure las interfaces para R1, R2 y R3 según la topología. En los lados DCE de los enlaces seriales, la frecuencia de reloj es de 64 000 bits.

Paso 2. Verificar el direccionamiento IP y las interfaces.

Verifique que todas las interfaces estén activadas tanto en la capa física como en la capa de enlace de datos. Los routers conectados directamente deben poder hacer ping entre sí.

Paso 3. Configurar las interfaces Ethernet de PC1 y PC3.

Paso 4. Probar la conectividad entre las PC.

¿Deben las PC poder hacer ping entre sí en este punto? ¿Pueden hacer ping a sus gateways predeterminadas?

Tarea 2: Configurar OSPF en los routers

Paso 1. Habilitar el enrutamiento OSPF en los routers.

Cuando configure el enrutamiento OSPF, utilice un area-id de 1.

Paso 2. Verificar que haya conectividad de red total.

Todos los routers deben tener rutas hacia todas las redes y deben ahora poder hacer ping a cualquier dispositivo.

Tarea 3: Configurar la encapsulación PPP en interfaces seriales

Paso 1. Configurar PPP en las interfaces seriales de los tres routers.

Actualmente, la encapsulación está establecida en HDLC en todos los enlaces seriales. Para poder configurar la autenticación más adelante, la encapsulación debe establecerse en PPP.

Paso 2. Verificar que todas las interfaces seriales utilicen la encapsulación PPP.

Si se produce una falta de concordancia entre las encapsulaciones de las interfaces seriales conectadas, el enlace se desactivará. Asegúrese de que todas las interfaces estén establecidas en encapsulación PPP.

Tarea 4: Configurar la autenticación PPP CHAP

La contraseña para la autenticación CHAP es cisco.

Paso 1. Configurar la autenticación PPP CHAP en todos los enlaces seriales.

Paso 2. Verificar la autenticación PPP CHAP en todos los enlaces seriales.

¿Pueden todos los routers comunicarse entre sí? ¿Puede la PC1 hacer ping a la PC3?

Actividad 2.5.3: Resolución de problemas de la configuración de PPP

Diagrama de topología

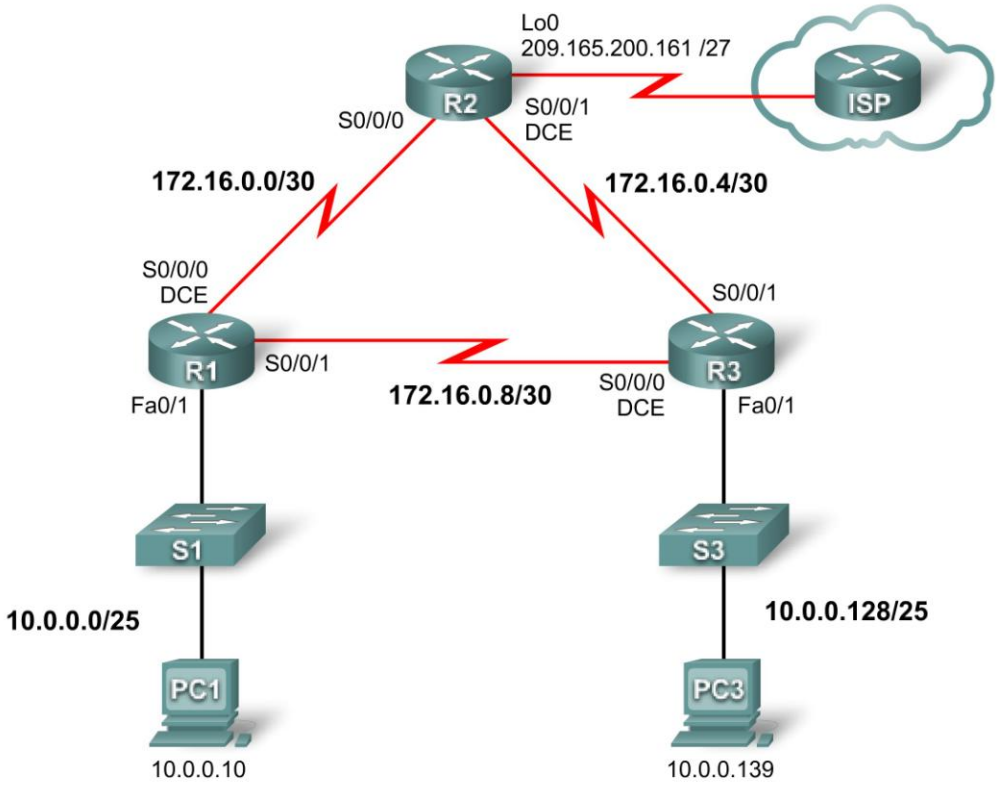


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/1**	10.0.0.1	255.255.255.128	No aplicable
	S0/0/0	172.16.0.1	255.255.255.252	No aplicable
	S0/0/1	172.16.0.9	255.255.255.252	No aplicable
R2	**Lo0**	209.165.200.161	255.255.255.224	No aplicable
	S0/0/0	172.16.0.2	255.255.255.252	No aplicable
	S0/0/1	172.16.0.5	255.255.255.252	No aplicable
R3	**Fa0/1**	10.0.0.129	255.255.255.128	No aplicable
	S0/0/0	172.16.0.10	255.255.255.252	No aplicable
	S0/0/1	172.16.0.6	255.255.255.252	No aplicable
PC1	**NIC**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**NIC**	10.0.0.139	255.255.255.128	10.0.0.129

Objetivos de aprendizaje

- Detectar y corregir errores de red
- Documentar la red corregida

Escenario

Un ingeniero de redes inexperto configuró los routers de su empresa. Diversos errores en la configuración produjeron problemas de conectividad. Su jefe le pidió que resuelva y corrija los errores de configuración y que documente su trabajo. Según sus conocimientos de PPP y de métodos de prueba estándar, detecte y corrija los errores. Asegúrese de que todos los enlaces seriales utilicen la autenticación PPP CHAP y de que todas las redes sean alcanzables.

Tarea 1: Detectar y corregir errores de red

- Utilice **64 000** para todas las frecuencias de reloj.
- Utilice **cisco** para todas las contraseñas CHAP.

Tarea 2: Documentar la red corregida

Actividad del PT 2.6.1: Desafío de integración de aptitudes del Packet Tracer

Diagrama de topología

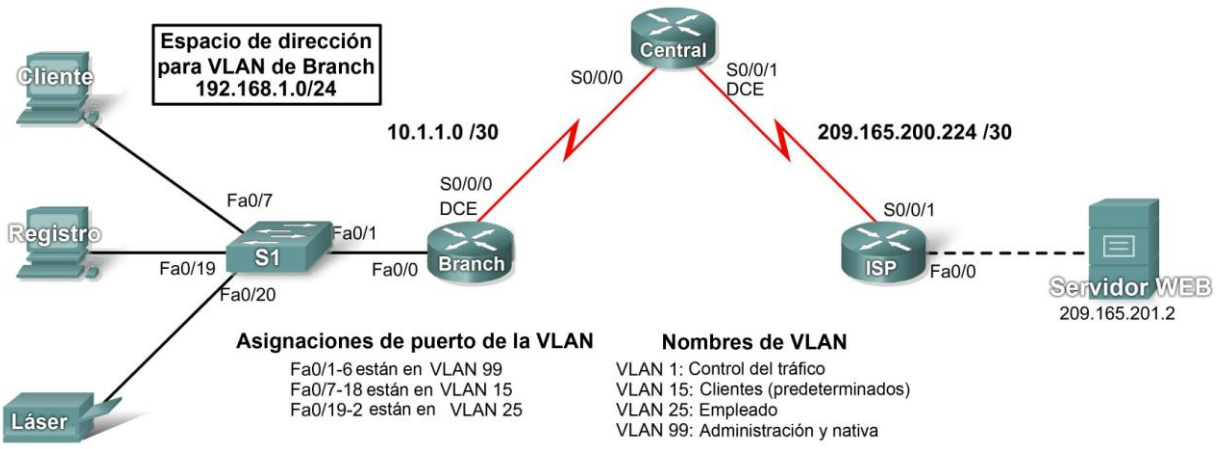


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
CENTRAL	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	209.165.200.226	255.255.255.252	No aplicable
ISP	S0/0/1	209.165.200.225	255.255.255.252	No aplicable
	Fa0/0	209.165.201.1	255.255.255.252	No aplicable
BRANCH	Fa0/0.1			No aplicable
	Fa0/0.15			No aplicable
	Fa0/0.25			No aplicable
	Fa0/0.99			No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
S1	VLAN99			
Cliente	NIC			
Registro	NIC			
Láser	NIC			
Servidor Web	NIC	209.165.201.2	255.255.255.252	209.165.201.1

Objetivos de aprendizaje

- Configurar el enrutamiento estático y predeterminado
- Agregar y conectar un router
- Diseñar y documentar un esquema de direccionamiento
- Agregar y conectar dispositivos en un espacio de dirección
- Configurar parámetros básicos de dispositivos
- Configurar la encapsulación PPP con CHAP
- Configurar el enrutamiento OSPF
- Configurar las VLAN
- Verificar la conectividad

Tarea 1: Configurar el enrutamiento estático y predeterminado

Paso 1. Configurar el enrutamiento estático desde el ISP a CENTRAL.

Utilice las contraseñas **cisco** y **class** para acceder a los modos EXEC de la CLI para los routers. Configure dos rutas estáticas en el ISP mediante el argumento de interfaz de salida a las siguientes redes:

- 10.1.1.0/30
- 192.168.1.0/24

Paso 2. Configurar el enrutamiento predeterminado desde CENTRAL al ISP.

Configure una ruta predeterminada en CENTRAL mediante el argumento de la interfaz de salida para enviar todo el tráfico predeterminado al ISP.

Paso 3. Probar la conectividad al servidor Web.

CENTRAL debe poder hacer ping con éxito al servidor Web en 209.165.201.2.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 4%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Agregar y conectar un router

Paso 1. Agregar el router BRANCH.

Haga clic en Dispositivos personalizados y agregue un router 1841 a la topología. Utilice la ficha Configuración para cambiar el Nombre de visualización a BRANCH. Los nombres de visualización distinguen mayúsculas de minúsculas. No cambie el nombre de host aún.

Paso 2. Conectar BRANCH a CENTRAL.

Elija el cable correcto y conecte BRANCH a CENTRAL según las interfaces que se muestran en la topología.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 9%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado. Si cambió el nombre de host en el Paso 2, su porcentaje será mayor.

Tarea 3: Diseño y documentación de un esquema de direccionamiento

Paso 1. Diseñar un esquema de direccionamiento.

Utilice la topología y los siguientes requisitos para diseñar un esquema de direccionamiento:

- Se proporciona el direccionamiento para todos los enlaces WAN.
- Para las VLAN conectadas a BRANCH, utilice el espacio de dirección 192.168.1.0/24. Comience con el mayor requisito de host y asigne las subredes en el siguiente orden para todas las VLAN.
    - VLAN 15 necesita espacio para 100 hosts _____
    - VLAN 25 necesita espacio para 50 hosts _____
    - VLAN 1 necesita espacio para 20 hosts _____
    - VLAN 99 necesita espacio para 20 hosts _____

Paso 2. Documentar el esquema de direccionamiento.

- Complete la tabla de direccionamiento mediante las siguientes pautas. Agregará los dispositivos restantes en la próxima tarea.
    - Asigne la primera dirección en cada VLAN a la subinterfaz de BRANCH correspondiente. Los números de subinterfaces coinciden con los números de VLAN.
    - Asigne la segunda dirección en VLAN 99 a S1.
    - Asigne la segunda dirección en VLAN 15 a la PC del cliente.
    - Asigne la segunda dirección en VLAN 25 a la PC de registro.
    - Asigne la última dirección en VLAN 25 a la impresora láser.
- Asegúrese de registrar la máscara de subred y la gateway predeterminada apropiadas para cada dirección.

Tarea 4: Agregar y conectar los dispositivos en el espacio de dirección

Paso 1. Agregar S1, PC del cliente, PC de registro e impresora láser al espacio de dirección 192.168.1.0/24.

- S1 es un switch 2960. Agréguelo a la topología y cambie el nombre de visualización a S1. Los nombres de visualización distinguen mayúsculas de minúsculas. No cambie el nombre de host aún.
- Las PC y la impresora se enumeran en Dispositivos finales. Agregue dos PC y una impresora. Cambie los nombres de visualización de las PC y la impresora según la topología.

Paso 2. Conectar S1 a BRANCH.

Elija el cable correcto y conecte S1 a BRANCH según las interfaces que se muestran en la topología.

Paso 3. Conectar la PC del cliente, la PC de registro y la impresora láser a S1.

Elija el cable correcto y conecte las PC y la impresora a S1 según las interfaces que se muestran en la topología.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 22%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado. Si cambió el nombre de host de S1 en el Paso 1, su porcentaje será mayor.

Tarea 5: Configurar los parámetros básicos de dispositivos

Paso 1. Configurar BRANCH y S1.

Mediante su documentación, establezca la configuración básica para BRANCH y S1, incluyendo el direccionamiento. Utilice **cisco** como contraseña de línea y **class** como la contraseña secreta. Utilice 64 000 como frecuencia de reloj. Los aspectos de la configuración básica que se califican incluyen:

- Los nombres de host, que distinguen mayúsculas de minúsculas.
- La dirección y la activación de la interfaz. Establezca la frecuencia de reloj en 64 000 bps.
- Para la interfaz Fa0/0.99, configure la VLAN 99 como la VLAN nativa.
- Creación de la interfaz VLAN 99 y direccionamiento en S1. La activación de la VLAN 99 se realiza después de que se haya configurado el enlace troncal más adelante en la actividad.

Paso 2. Configurar los dispositivos restantes.

Mediante su documentación, configure las PC y la impresora con la dirección correcta.

Paso 3. Probar la conectividad entre BRANCH y CENTRAL.

Ahora CENTRAL debe poder hacer ping con éxito a BRANCH. S1 no puede hacer ping hasta que se haya configurado el enlace troncal.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 63%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Configurar la encapsulación PPP con autenticación CHAP

Paso 1. Configurar CENTRAL para que utilice PPP con CHAP para el enlace a BRANCH.

La contraseña para la autenticación CHAP es **cisco123**. El enlace se desactiva.

Paso 2. Configurar BRANCH para que utilice PPP con CHAP para el enlace a CENTRAL.

La contraseña para la autenticación CHAP es **cisco123**. El enlace se activa nuevamente.

Paso 3. Probar la conectividad entre BRANCH y CENTRAL.

Es posible que Packet Tracer demore un poco más que el equipo real para activar nuevamente las interfaces. Una vez que las interfaces se activen, CENTRAL debe poder hacer ping con éxito a BRANCH.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 71%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 7: Configurar el enrutamiento OSPF

Paso 1. Configurar OSPF en CENTRAL.

- Configure OSPF mediante el ID de proceso 1.
- Agregue sólo la red compartida con BRANCH.
- Propague la ruta predeterminada a vecinos OSPF.
- Deshabilite las actualizaciones de OSPF para el ISP.

Paso 2. Configurar OSPF en BRANCH.

- Configure OSPF mediante el ID de proceso 1.
- Agregue todas las redes activas que enruta BRANCH.
- Deshabilite las actualizaciones de OSPF para las VLAN.

Paso 3. Probar la conectividad al servidor Web.

BRANCH debe ahora poder hacer ping con éxito al servidor Web en 209.165.201.2.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 86%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 8: Configurar las VLAN

Paso 1. Agregar las VLAN a S1.

Los nombres de las VLAN distinguen mayúsculas de minúsculas. Agregar y nombrar las cuatro VLAN mediante las siguientes especificaciones:

- VLAN 15; el nombre es **Clientes (Predeterminado)**
- VLAN 25; el nombre es **Empleado**
- VLAN 99; el nombre es **Administración y Nativa**

Paso 2. Asignar puertos a las VLAN apropiadas y activar la interfaz VLAN 99.

- Mediante las Asignaciones de puertos VLAN que se muestran en el diagrama de topología, configure los puertos conectados a los dispositivos finales y asigne cada uno de éstos a la VLAN correspondiente.
- Habilite el enlace troncal en el puerto Fa0/1 y configúrelo para que utilice la VLAN 99 como la VLAN nativa.
- Si es necesario, active la interfaz VLAN 99. Ya debe estar activada.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 9: Verificar la conectividad

Paso 1. Verificar que la PC del cliente, la PC de registro y la impresora láser puedan hacer ping entre sí.

Paso 2. Verificar que la PC del cliente, la PC de registro y la impresora láser puedan hacer ping al servidor Web.

Actividad de PT 3.2.2: Configuración básica de Frame Relay con mapas estáticos

Diagrama de topología

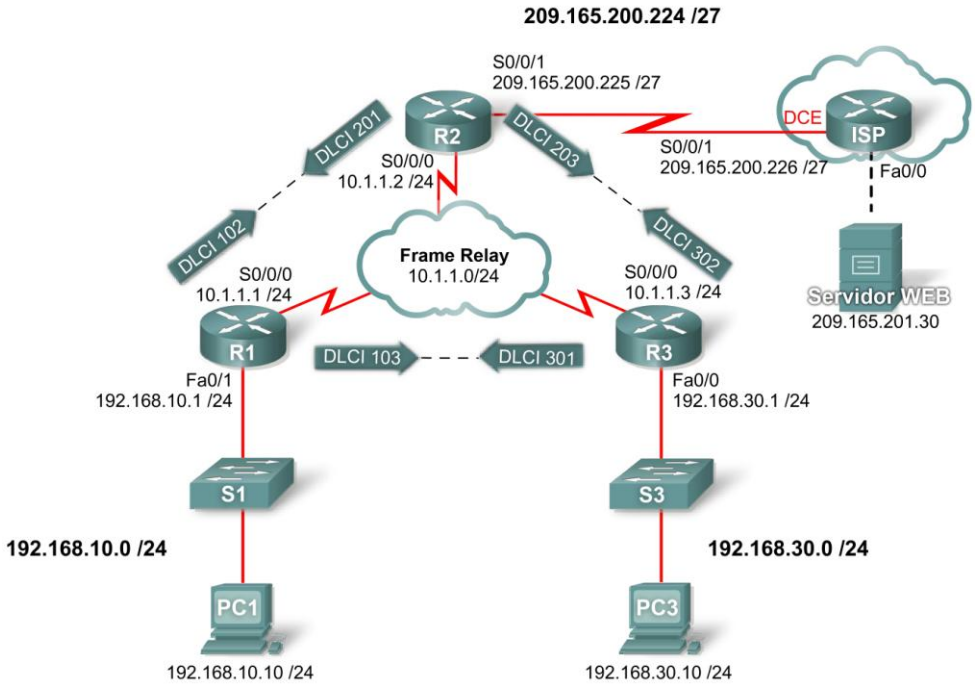


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/0**	192.168.10.1	255.255.255.0
	S0/0/1	10.10.10.1	255.255.255.0
R2	**S0/0/0**	10.10.10.2	255.255.255.0
	S0/0/1	209.165.200.225	255.255.255.224
R3	**Fa0/0**	192.168.30.1	255.255.255.0
	S0/0/0	10.10.10.3	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.224

Objetivos de aprendizaje

- Configurar Frame Relay
- Configurar mapas estáticos de Frame Relay
- Configurar Frame Relay tipo LMI

Introducción

En esta actividad, configurará Frame Relay en las interfaces seriales 0/0/0 de los routers R1, R2 y R3. Además, configurará dos mapas estáticos de Frame Relay en cada router para alcanzar los otros dos routers. Si bien el tipo LMI se detecta automáticamente en los routers, asignará el tipo de manera estática mediante la configuración manual de la LMI.

Los routers R1, R2 y R3 se configuraron previamente con nombres de host y direcciones IP en todas las interfaces. Las interfaces Fast Ethernet de los routers R1 y R3 están activas, y la interfaz S0/0/1 del R2 está activa.

Tarea 1: Configurar Frame Relay

Paso 1. Configurar la encapsulación Frame Relay en la interfaz serial 0/0/0 de R1.

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
```

Paso 2. Configurar la encapsulación Frame Relay en las interfaces seriales 0/0/0 de R2 y R3.

Paso 3. Probar la conectividad.

Desde la línea de comandos de la PC1, verifique la conectividad al host de la PC3, ubicado en 192.168.30.10, mediante el comando **ping**.

El ping desde la PC1 a la PC3 debe fallar, ya que el router R1 no tiene información acerca de dónde se encuentra la red 192.168.30.0. El R1 debe configurarse con un mapa de Frame Relay para que pueda encontrar el destino del siguiente salto y así alcanzar dicha red.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 40%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configuración de mapas estáticos de Frame Relay

Paso 1. Configurar mapas estáticos en R1, R2 y R3.

Cada router necesita dos mapas estáticos para poder alcanzar a los demás routers. Los DLCI para alcanzar a estos routers son los siguientes:

Router R1:

- Para alcanzar al router R2, utilice DLCI 102 ubicado en la dirección IP 10.10.10.2.
- Para alcanzar al router R3, utilice DLCI 103 ubicado en la dirección IP 10.10.10.3.

Router R2:

- Para alcanzar al router R1, utilice DLCI 201 ubicado en la dirección IP 10.10.10.1.
- Para alcanzar al router R3, utilice DLCI 203 ubicado en la dirección IP 10.10.10.3.

Router R3:

- Para alcanzar al router R1, utilice DLCI 301 ubicado en la dirección IP 10.10.10.1.
- Para alcanzar al router R3, utilice DLCI 302 ubicado en la dirección IP 10.10.10.2.

Los routers también deben admitir RIP, por lo que se requiere la palabra clave **broadcast**.

En el router R1, configure los mapas estáticos de Frame Relay de la siguiente manera:

```
R1(config-if)#frame-relay map ip 10.10.10.2 102 broadcast
R1(config-if)#frame-relay map ip 10.10.10.3 103 broadcast
```

Configure los routers R2 y R3 mediante la información proporcionada anteriormente.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 80%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar Frame Relay tipo LMI

La nube Frame Relay contiene switches que utilizan ANSI como el tipo LMI. Por lo tanto, todos los enlaces Frame Relay deben configurarse manualmente para que utilicen ANSI.

Paso 1. Configurar ANSI como el tipo LMI en R1, R2 y R3.

Ingrese el siguiente comando en la interfaz serial para cada router.

```
R1(config-if)#interface s0/0/0
R1(config-if)#frame-relay lmi-type ansi
```

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Paso 3. Probar la conectividad.

Es posible completar la actividad en un 100% y, sin embargo, no tener conectividad. La PC1 y la PC3 deben ahora poder hacer ping con éxito entre sí y al servidor Web. De no ser así, asegúrese de haber ingresado todos los comandos exactamente como se especificó en los pasos anteriores.

Actividad de PT 3.6.1: Desafío de integración de aptitudes de Packet Tracer

Diagrama de topología

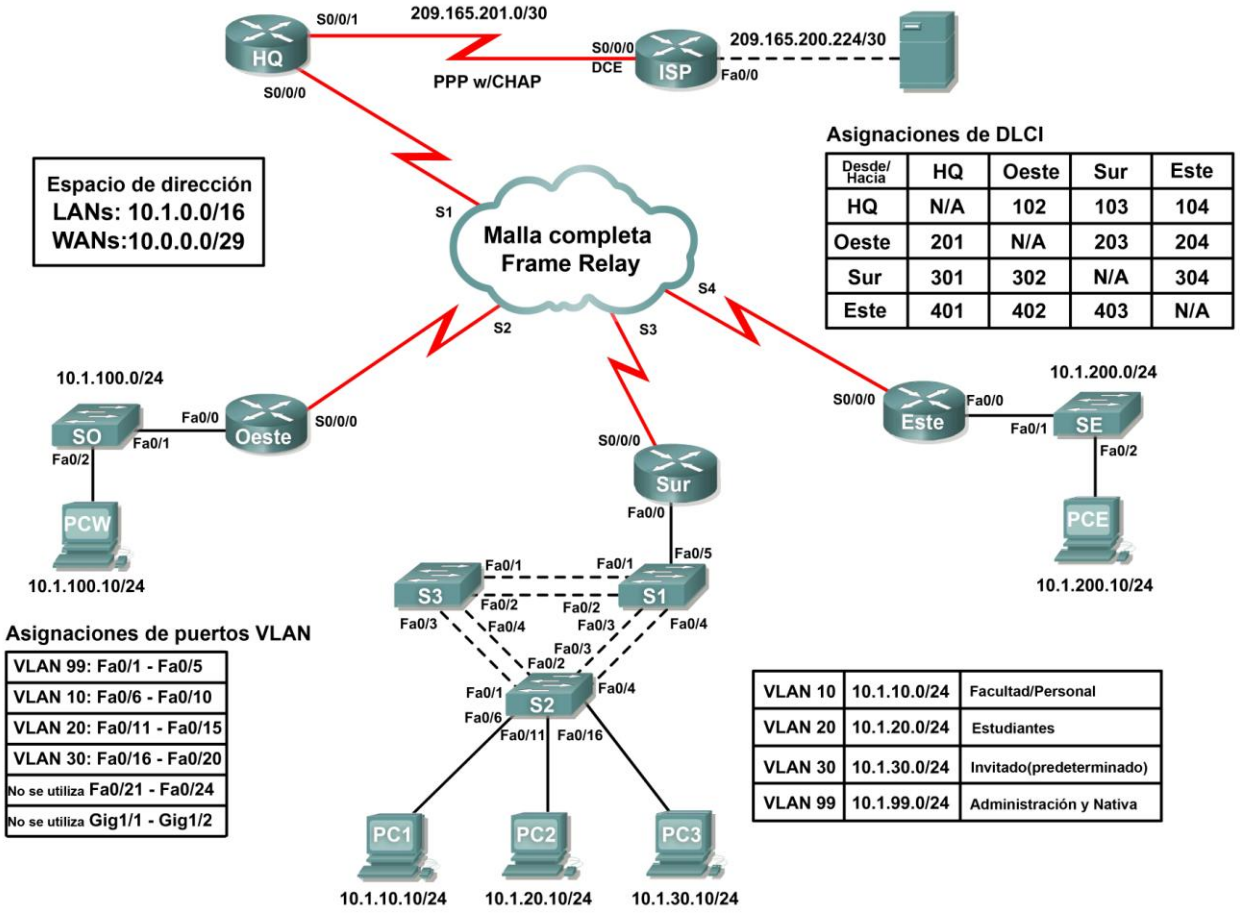


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
HQ	**S0/0/1**	209.165.201.2	255.255.255.252
	S0/0/0	10.0.0.1	255.255.255.248
WEST	**S0/0/0**	10.0.0.2	255.255.255.248
	Fa0/0	10.1.100.1	255.255.255.0
SOUTH	**S0/0/0**	10.0.0.3	255.255.255.248
	Fa0/0.10	10.1.10.1	255.255.255.0
	Fa0/0.20	10.1.20.1	255.255.255.0
	Fa0/0.30	10.1.30.1	255.255.255.0
	Fa0/0.99	10.1.99.1	255.255.255.0
EAST	**S0/0/0**	10.0.0.4	255.255.255.248
	Fa0/0	10.1.200.1	255.255.255.0
ISP	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Servidor Web	**NIC**	209.165.200.226	255.255.255.252
S1	**VLAN99**	10.1.99.11	255.255.255.0
S2	**VLAN99**	10.1.99.12	255.255.255.0
S3	**VLAN99**	10.1.99.13	255.255.255.0

Objetivos de aprendizaje

- Configurar PPP con CHAP
- Configurar Frame Relay con malla completa
- Configurar el enrutamiento estático y predeterminado
- Configurar y probar el enrutamiento entre las VLAN
- Configurar VTP y el enlace troncal en los switches
- Configurar las VLAN en un switch
- Configurar y verificar la interfaz VLAN 99
- Configurar un switch como raíz para todos los spanning tree
- Asignar puertos a las VLAN
- Probar la conectividad de extremo a extremo

Introducción

Esta actividad le permite practicar diversas aptitudes, incluso la configuración de Frame Relay, PPP con CHAP, enrutamiento estático y predeterminado, VTP y VLAN. Debido a que esta actividad contiene casi 150 componentes que se califican, es posible que no vea que el porcentaje de finalización aumenta cada vez que configura un comando con calificación. Recuerde que puede hacer clic en **Verificar resultados** y en **Puntos de evaluación** para ver si ingresó correctamente un comando con calificación.

Tarea 1: Configurar PPP con CHAP entre dispositivos

Paso 1. Configurar y activar serial 0/0/1 en HQ.

Paso 2. Configurar la encapsulación PPP en HQ para el enlace compartido con el ISP.

Paso 3. Configurar la autenticación CHAP en HQ.

Utilice **cisco** como contraseña.

Paso 4. Verificar la conectividad entre HQ y el ISP.

El enlace entre el HQ y el ISP debe estar activado ahora y debe poder hacer ping al ISP. Sin embargo, es posible que el enlace necesite unos minutos en Packet Tracer antes de activarse. Para acelerar el proceso, cambie entre el modo Simulación y Tiempo real tres o cuatro veces.

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 4%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar Frame Relay con malla completa

El diagrama de topología anterior y la tabla que aparece a continuación muestran las asignaciones DLCI que se utilizan en esta configuración de Frame Relay con malla completa. Lea la tabla de izquierda a derecha. Por ejemplo: los mapeos DLCI que configurará en HQ son: 102 a WEST, 103 a SOUTH y 104 a EAST.

	Mapeos DLCI			
Desde/Hacia	**HQ**	**WEST**	**SOUTH**	**EAST**
HQ	No aplicable	102	103	104
WEST	201	No aplicable	203	204
SOUTH	301	302	No aplicable	304
EAST	401	402	403	No aplicable

Nota: HQ, WEST y SOUTH utilizan la encapsulación Frame Relay predeterminada **cisco**. Sin embargo, EAST utiliza el tipo de encapsulación IETF.

Paso 1. Configurar y activar la interfaz serial 0/0/0 en HQ.

Configure la interfaz con la siguiente información:

- Dirección IP
- Encapsulación Frame Relay
- Mapeos hacia WEST, SOUTH y EAST (EAST utiliza encapsulación IETF)
- El tipo de LMI es ANSI

Paso 2. Configurar y activar la interfaz serial 0/0/0 en WEST.

Configure la interfaz con la siguiente información:

- Dirección IP
- Encapsulación Frame Relay
- Mapeos hacia HQ, SOUTH y EAST (EAST utiliza encapsulación IETF)
- El tipo de LMI es ANSI

Paso 3. Configurar y activar la interfaz serial 0/0/0 en SOUTH.

Configure la interfaz con la siguiente información:

- Dirección IP
- Encapsulación Frame Relay
- Mapeos hacia HQ, WEST y EAST (EAST utiliza encapsulación IETF)
- El tipo de LMI es ANSI

Paso 4. Configurar y activar la interfaz Serial 0/0/0 en EAST.

Configure la interfaz con la siguiente información:

- Dirección IP
- Encapsulación Frame Relay con IETF
- Mapeos hacia HQ, WEST y SOUTH
- El tipo de LMI es ANSI

Nota: Packet Tracer no califica sus sentencias de mapa. Sin embargo, debe configurar los comandos de todos modos. Ahora debe tener conectividad total entre los routers Frame Relay.

Paso 5. Verificar la conectividad entre los routers Frame Relay.

El mapa en HQ debe verse como el que aparece a continuación. Asegúrese de que todos los routers tengan mapas completos.

```
Serial0/0/0 (up): ip 10.0.0.2 dlci 102, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.3 dlci 103, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.4 dlci 104, static, broadcast, IETF, status
defined, active
```

Verifique que HQ, WEST, SOUTH y EAST ahora puedan hacer ping entre sí.

Paso 6. Verificar los resultados.

Su porcentaje de finalización debe ser del 28%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar el enrutamiento estático y predeterminado

No se utiliza ningún protocolo de enrutamiento en esta topología. Todo el enrutamiento se realiza a través del enrutamiento estático y predeterminado.

Paso 1. Configurar rutas estáticas y predeterminadas en HQ.

- HQ necesita seis rutas estáticas a las seis LAN remotas en la topología. Utilice el argumento *ip-del-siguiente-salto* en la configuración de las rutas estáticas.
- Además, HQ necesita una ruta predeterminada. Use el argumento de *interfaz de salida* en la configuración de la ruta predeterminada.

Paso 2. Configurar rutas estáticas y predeterminadas en WEST.

- WEST necesita cinco rutas estáticas a las cinco LAN remotas en la topología. Utilice el argumento *ip-del-siguiente-salto* en la configuración de las rutas estáticas.
- Además, WEST necesita una ruta predeterminada. Utilice el argumento *ip-del-siguiente-salto* en la configuración de la ruta predeterminada.

Paso 3. Configurar rutas estáticas y predeterminadas en SOUTH.

- SOUTH necesita dos rutas estáticas a las dos LAN remotas en la topología. Utilice el argumento *ip-del-siguiente-salto* en la configuración de las rutas estáticas.
- SOUTH necesita una ruta predeterminada. Utilice el argumento *ip-del-siguiente-salto* en la configuración de la ruta predeterminada.

Paso 4. Configurar rutas estáticas y predeterminadas en EAST.

- EAST necesita cinco rutas estáticas a las cinco LAN remotas en la topología. Utilice el argumento *ip-del-siguiente-salto* en la configuración de las rutas estáticas.
- EAST necesita una ruta predeterminada. Utilice el argumento *ip-del-siguiente-salto* en la configuración de la ruta predeterminada.

Paso 5. Verificar la conectividad desde las LAN EAST y WEST hacia el servidor Web.

- Todos los routers deben ahora poder hacer ping al servidor Web.
- La PC WEST (PCW) y la PC EAST (PCE) deben ahora poder hacer ping entre sí y al servidor Web.

Paso 6. Verificar los resultados.

Su porcentaje de finalización debe ser del 43%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar y probar el enrutamiento entre las VLAN

Paso 1. Configurar el enrutamiento entre las VLAN en SOUTH.

Utilizando la tabla de direccionamiento, active Fast Ethernet 0/0 en SOUTH y configure el enrutamiento entre las VLAN. El número de subinterfaz corresponde al número de VLAN. La VLAN 99 es la VLAN nativa.

Paso 2. Probar el enrutamiento entre las VLAN en SOUTH.

HQ, WEST y EAST deben ahora poder hacer ping a cada una de las subinterfaces de SOUTH.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 56%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado. Los routers están ahora completamente configurados.

Tarea 5: Configurar VTP y el enlace troncal en los switches

Paso 1. Configurar los valores VTP en S1, S2 y S3.

- S1 es el servidor. S2 y S3 son los clientes.
- El nombre de dominio es **CCNA**.
- La contraseña es **cisco**.

Paso 2. Configurar el enlace troncal en S1, S2 y S3.

Los puertos del enlace troncal para S1, S2 y S3 son todos puertos conectados a otro switch o router. Establezca todos los puertos del enlace troncal en el modo de enlace troncal y asigne la VLAN 99 como la VLAN nativa.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 81%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Configurar las VLAN en el switch

Paso 1. Crear y nombrar las VLAN.

Cree y nombre las siguientes VLAN sólo en S1:

- VLAN 10, nombre = **Cuerpo docente/Personal**
- VLAN 20, nombre = **Estudiantes**
- VLAN 30, nombre = **Guest (Predeterminado)**
- VLAN 99, nombre = **Administración y Nativa**

Paso 2. Verificar que las VLAN se hayan enviado a S2 y S3.

¿Qué comando muestra el siguiente resultado? _____

```
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF5 0x50 0x30 0xB6 0x91 0x74 0x95 0xD9
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:30
```

¿Qué comando muestra el siguiente resultado? _____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
```

```
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
10   Faculty/Staff                  active
20   Students                       active
30   Guest(Default)                 active
99   Management&Native              active
<resultado omitido>
```

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 84%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 7: Configurar y verificar VLAN 99

Paso 1. En S1, S2 y S3, completar los siguientes pasos:

- Configurar y activar VLAN 99
- Configure la gateway predeterminada
- Verificar que S1, S2 y S3 puedan ahora hacer ping a SOUTH en 10.1.99.1

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 92%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 8: Configurar S1 como raíz para todos los spanning tree

Paso 1. Configurar S1 como el puente raíz para todos los spanning tree, incluidas las VLAN 1, 10, 20, 30 y 99.

Observe que S3 fue preponderante y actualmente es el puente raíz para todos los spanning tree. Establezca la prioridad en 4096 en S1 para todos los spanning tree.

Paso 2. Verificar que S1 sea ahora la raíz para todos los spanning tree.

A continuación se muestran sólo los resultados para VLAN 1. Sin embargo, S1 debería ser la raíz para todos los spanning tree. ¿Qué comando muestra el siguiente resultado?

_____

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     00D0.BC79.4B57
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     00D0.BC79.4B57
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

```
Fa0/5            Desg FWD 19        128.3    Shr
<resultado omitido>
```

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 96%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 9: Asignar puertos a las VLAN

Paso 1. Asignar puertos en S2 a las VLAN.

Packet Tracer sólo califica los puertos que están conectados a la PC1, PC2 y PC3.

- Configure el puerto para el modo de acceso
- Asigne el puerto a su VLAN

Las asignaciones de puertos de VLAN son las siguientes:

- VLAN 99: Fa0/1 – Fa0/5
- VLAN 10: Fa0/6 – Fa0/10
- VLAN 20: Fa0/11 – Fa0/15
- VLAN 30: Fa0/16 – Fa0/20
- No se utiliza: Fa0/21 – Fa0/24; Gig1/1; Gig1/2

Los puertos que no se utilizan deben cerrarse por seguridad.

Paso 2. Verificar las asignaciones de puertos de VLAN.

¿Qué comando se utilizó para obtener el siguiente resultado que muestran las asignaciones de VLAN?

_____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
10   Faculty/Staff                     active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
20   Students                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
30   Guest(Default)                    active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 10: Probar la conectividad de extremo a extremo

Si bien es posible que Packet Tracer necesite un tiempo para converger, eventualmente los pings desde PC1, PC2 y PC3 tendrán éxito. Pruebe la conectividad hacia PCW, PCE y el servidor Web. De ser necesario, cambie entre los modos Simulación y Tiempo real para acelerar la convergencia.

Actividad de PT 4.3.2: Configuración de la autenticación de OSPF

Diagrama de topología

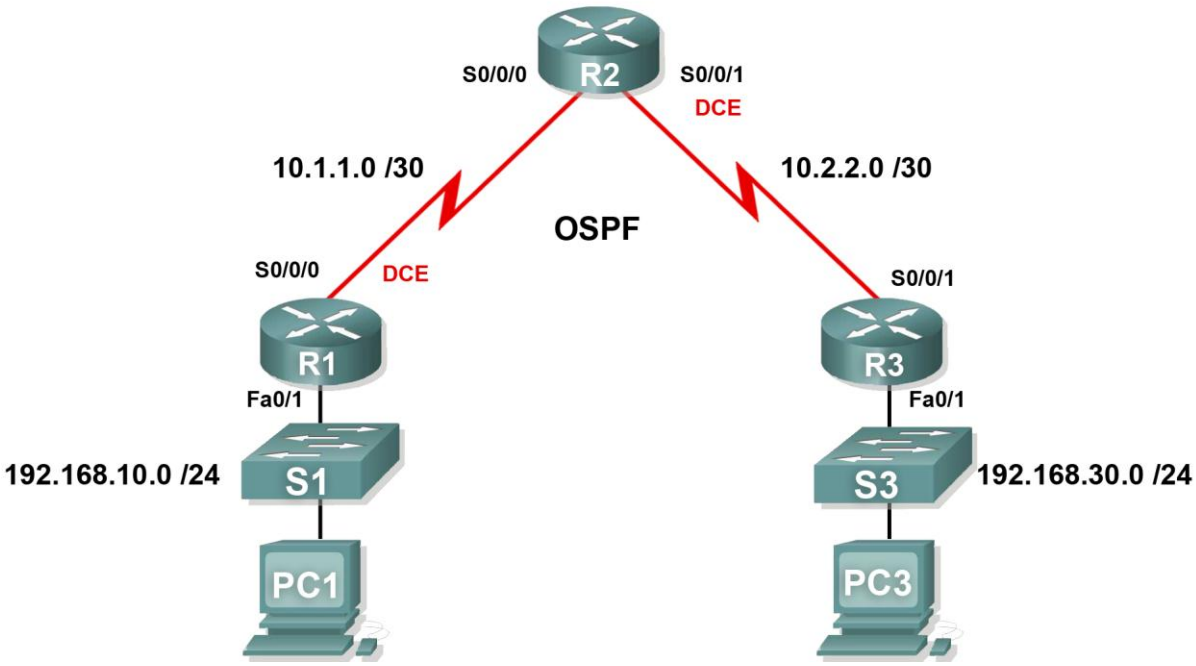


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0

Objetivos de aprendizaje

- Configurar la autenticación simple de OSPF
- Configurar la autenticación MD5 de OSPF
- Probar la conectividad

Introducción

Esta actividad abarca la autenticación simple de OSPF y la autenticación MD5 (message digest 5) de OSPF. Puede habilitar la autenticación de OSPF para intercambiar información de actualización de enrutamiento de manera segura. Con la autenticación simple, la contraseña se envía en texto no cifrado a través de la red. La autenticación simple se utiliza cuando los dispositivos dentro de un área no admiten la autenticación MD5, que es más segura. Con la autenticación MD5, la contraseña se envía a través de la red. Se considera que MD5 es el modo de autenticación de OSPF más seguro. Cuando configure la autenticación, debe configurar un área completa con el mismo tipo de autenticación. En esta actividad, configurará la autenticación simple entre R1 y R2 y la autenticación MD5 entre R2 y R3.

Tarea 1: Configurar la autenticación simple de OSPF

Paso 1. Configurar R1 con autenticación simple de OSPF.

Para habilitar la autenticación simple en R1, ingrese al modo de configuración del router mediante el comando **router ospf 1** en la petición de entrada de configuración global. A continuación, ejecute el comando **area 0 authentication** para habilitar la autenticación.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

Finalmente, aparece un mensaje de consola que indica que la adyacencia con R2 está desactivada. R1 pierde todas las rutas OSPF de su tabla de enrutamiento hasta que pueda autenticar las rutas con R2. Si bien todavía no configuró una contraseña, R1 requiere que cualquier vecino utilice autenticación en los mensajes y las actualizaciones de enrutamiento de OSPF.

El comando **area 0 authentication** permite la autenticación para todas las interfaces en el área 0. La utilización de este comando solamente funciona para R1, ya que no tiene que admitir ningún otro tipo de autenticación.

Para configurar R1 con una contraseña de autenticación simple, ingrese al modo de configuración de la interfaz para el enlace que conecta a R2. A continuación, ejecute el comando **ip ospf authentication-key cisco 123**. Este comando establece la contraseña de autenticación como **cisco 123**.

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

Paso 2. Configurar R2 con autenticación simple de OSPF.

Ya configuró la autenticación en R1 para toda el área. Debido a que R2 admite tanto la autenticación simple como la MD5, los comandos se ingresan a nivel de la interfaz.

Ingrese al modo de configuración de la interfaz para S0/0/0. Especifique que utiliza la autenticación simple con el comando **ip ospf authentication**. A continuación, ejecute el comando **ip ospf authentication-key cisco 123** para establecer la contraseña de autenticación como **cisco 123**.

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

Una vez que haya completado estas tareas de configuración, debe ver finalmente un mensaje de consola que indica que se restableció la adyacencia entre R1y R2. Las rutas OSPF se reinstalaron en la tabla de enrutamiento.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 50%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar la autenticación MD5 de OSPF

Paso 1. Configurar R3 con autenticación MD5 de OSPF.

Para habilitar la autenticación MD5 en R3, ingrese al modo de configuración del router mediante el comando **router ospf 1** en la petición de entrada de configuración global. A continuación, ejecute el comando **area 0 authentication message-digest** para habilitar la autenticación.

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

Finalmente, aparece un mensaje de consola que indica que la adyacencia con R2 está desactivada. R3 pierde todas las rutas OSPF de su tabla de enrutamiento hasta que pueda autenticar las rutas con R2.

Para configurar R3 con una contraseña de autenticación MD5, ingrese al modo de configuración de interfaz para el enlace que conecta a R2. A continuación, ejecute el comando **ip ospf message-digest-key 1 md5 cisco123**. Este comando establece la contraseña de autenticación de OSPF como **cisco 123**, protegida con el algoritmo MD5.

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

Paso 2. Configurar R2 con autenticación MD5 de OSPF.

En R2, ingrese al modo de configuración de la interfaz para el enlace que conecta a R3. Ejecute el comando **ip ospf authentication message-digest** para habilitar la autenticación MD5. Este comando es necesario en R2 porque este router utiliza dos tipos de autenticación.

A continuación, ejecute el comando **ip ospf message-digest-key 1 md5 cisco123** para configurar la contraseña de autenticación.

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

Una vez que haya ingresado este comando, espere un momento para que los routers converjan. Aparece un mensaje de consola tanto en R2 como en R3 que indica que se restableció la adyacencia vecina. Puede confirmar que R2 reinstaló las rutas OSPF y que R2 tiene a R3 como vecino OSPF.

```
R2#show ip route
<resultado omitido>

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1
```

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.1      1   FULL/-          00:00:32    10.1.1.1        Serial0/0/0
192.168.30.1      1   FULL/-          00:00:37    10.2.2.2        Serial0/0/1
```

Paso 3. Verificar los resultados.

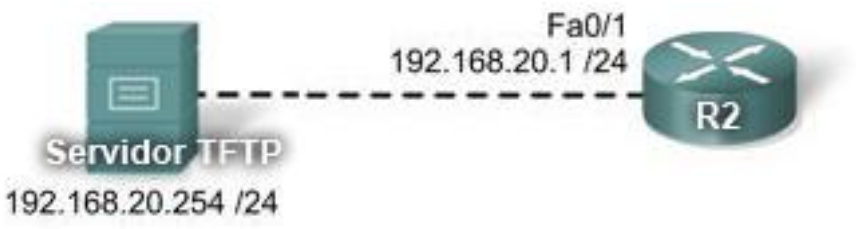
Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Probar la conectividad

La autenticación debe ahora estar configurada correctamente en los tres routers; de esta manera, la PC1 no debe tener problemas en hacer ping a la PC3. Haga clic en **Verificar resultados** y después en **Pruebas de conectividad** para ver si tiene éxito.

Actividad de PT 4.5.4: Uso de un servidor TFTP para actualizar una imagen IOS de Cisco

Diagrama de topología



Objetivos de aprendizaje

- Verificar la imagen IOS de Cisco actual
- Configurar el acceso al servidor TFTP
- Cargar una nueva imagen IOS de Cisco
- Configurar el comando **boot system**
- Probar la nueva imagen IOS de Cisco

Introducción

En esta actividad, configurará el acceso a un servidor TFTP y cargará una imagen IOS de Cisco más nueva y avanzada. Si bien Packet Tracer simula la actualización de la imagen IOS de Cisco en un router, no simula la realización de una copia de respaldo de una imagen IOS de Cisco en el servidor TFTP. Además, si bien la imagen a la que se actualiza es más avanzada, esta simulación del Packet Tracer no reflejará la actualización mediante la habilitación de comandos más avanzados. El mismo conjunto de comandos del Packet Tracer seguirá en funcionamiento.

Tarea 1: Verificar la imagen IOS de Cisco actual

Paso 1. Utilizar el comando show version para verificar la imagen que está cargada actualmente en la RAM.

```
R2#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7,
RELEASE SOFTWARE (fc2)
Soporte técnico: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
<resultado omitido>
```

La imagen cargada actualmente en la RAM no admite SSH ni muchas otras funciones avanzadas.

Paso 2. Utilizar el comando show flash para verificar cualquier imagen disponible actualmente en la memoria flash.

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

Sólo una imagen IOS de Cisco está disponible. Antes de que pueda utilizar SSH y las funciones de seguridad adicionales, debe actualizar la imagen con una versión más avanzada.

Tarea 2: Configurar el acceso al servidor TFTP

R2 necesita establecer una conexión a un servidor TFTP que tiene la imagen IOS de Cisco que necesita.

Paso 1. Conectar R2 y el servidor TFTP.

Consulte el diagrama de topología para determinar la interfaz correcta.

Paso 2. Configurar R2 con una dirección IP.

Consulte el diagrama de topología para determinar el direccionamiento IP correcto.

Paso 3. Configurar el servidor TFTP con direccionamiento IP y una gateway predeterminada.

Consulte el diagrama de topología para determinar el direccionamiento IP correcto.

Paso 4. Probar la conectividad.

R2 debe poder hacer ping con éxito al servidor TFPT. De no ser así, verifique el cableado y el direccionamiento.

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 80%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Cargar una nueva imagen IOS de Cisco

Paso 1. Consultar el servidor TFTP para observar las imágenes IOS de Cisco.

Haga clic en Servidor TFTP y a continuación, en la ficha **Configuración**. Observe que hay varias imágenes disponibles. Cargará la imagen c1841-ipbasek9-mz.124-12.bin en R2.

Paso 2. Cargar la imagen c1841-ipbasek9-mz.124-12.bin en R2.

- En R2, comience el proceso de carga con el comando **copy tftp flash**.
- Ingrese la dirección IP del servidor TFTP.
- Ingrese el nombre de archivo completo para la imagen IOS de Cisco.

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254
Source filename []? c1841-ipbasek9-mz.124-12.bin
Destination filename [c1841-ipbasek9-mz.124-12.bin]? Enter
Accessing tftp://192.168.20.254/c1841-ipbasek9-mz.124-12.bin...
```

```
Loading c1841-ipbasek9-mz.124-12.bin from 192.168.20.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
[OK - 16599160 bytes]

16599160 bytes copied in 13.047 secs (284682 bytes/sec)
R2#
```

Paso 3. Verificar que la nueva imagen se encuentre ahora en la memoria flash.

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
  2   16599160 c1841-ipbasek9-mz.124-12.bin
[30431192 bytes used, 2082856 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)

R2#
```

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 90%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar el comando boot system

De manera predeterminada, la secuencia de arranque del router carga la primera imagen IOS de Cisco que aparece en la memoria flash. Una manera de asegurarse de que el router cargue la nueva imagen es configurar el comando **boot system flash**. En R2, ingrese el siguiente comando:

```
R2(config)#boot system flash c1841-ipbasek9-mz.124-12.bin
```

Este comando es ahora parte de la configuración en ejecución. No obstante, la configuración en ejecución también debe guardarse en NVRAM. De no ser así, la configuración se sobrescribe la próxima vez que recargue el router.

```
R2(config)#end
R2#copy running-config startup-config
```

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Probar la nueva imagen

Vuelva a cargar R2 y espere a que se reinicie. Cuando el router se vuelva a cargar, verifique que la nueva imagen esté en la RMA con el comando **show version**.

```
R2#reload
Proceed with reload? [confirm][Intro]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
<resultado omitido>
```

```
R2>show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbasek9-mz.124-12.bin"
<resultado omitido>
```

Actividad de PT 4.7.1: Desafío de integración de aptitudes del Packet Tracer

Diagrama de topología

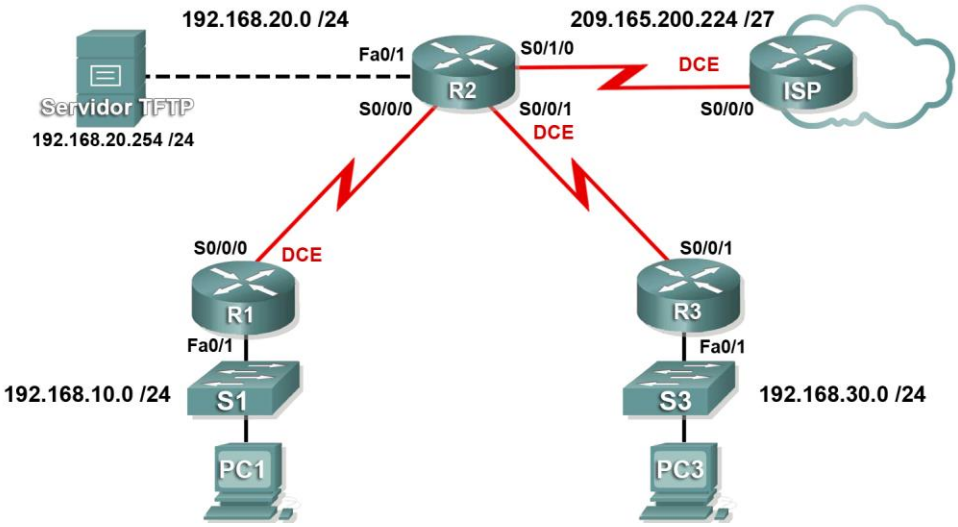


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
ISP	**S0/0/0**	209.165.200.226	255.255.255.252
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255255.255.252
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
Servidor TFTP	**NIC**	192.168.20.254	255.255.255.255

Objetivos de aprendizaje

- Configurar el enrutamiento
- Configurar la autenticación de OSPF
- Actualizar la imagen IOS de Cisco

Introducción

Esta actividad es una revisión acumulativa del capítulo que abarca el enrutamiento y autenticación de OSPF y la actualización de la imagen IOS de Cisco.

Tarea 1: Configurar el enrutamiento

Paso 1. Configurar una ruta predeterminada al ISP.

En R2, utilice el argumento de interfaz de salida para configurar una ruta predeterminada al ISP.

Paso 2. Configurar el enrutamiento OSPF entre R1, R2 y R3.

Configure el enrutamiento OSPF en los tres routers. Utilice el ID de proceso 1. Deshabilite las actualizaciones de OSPF en las interfaces correspondientes.

Paso 3. Propagar la ruta predeterminada.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 59%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar la autenticación de OSPF

Paso 1. Configurar la autenticación MD5 entre R1, R2 y R3.

Configure la autenticación MD5 de OSPF entre R1, R2 y R3 utilizando **1** como el valor clave y **cisco123** como la contraseña.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 91%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Actualizar la imagen IOS de Cisco

Paso 1. Copiar una imagen más nueva desde el servidor TFTP en la memoria flash de R2.

Busque en la ficha Configuración para que el servidor TFTP pueda determinar el nombre de la imagen IOS de Cisco más nueva. A continuación, copie la imagen más nueva en la memoria flash de R2.

Paso 2. Configurar R2 para que se inicie con la nueva imagen.

Paso 3. Guardar la configuración y recargar.

Verifique que la nueva imagen esté cargada en la RAM.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Actividad de PT 5.2.8: Configuración de las ACL estándar

Diagrama de topología

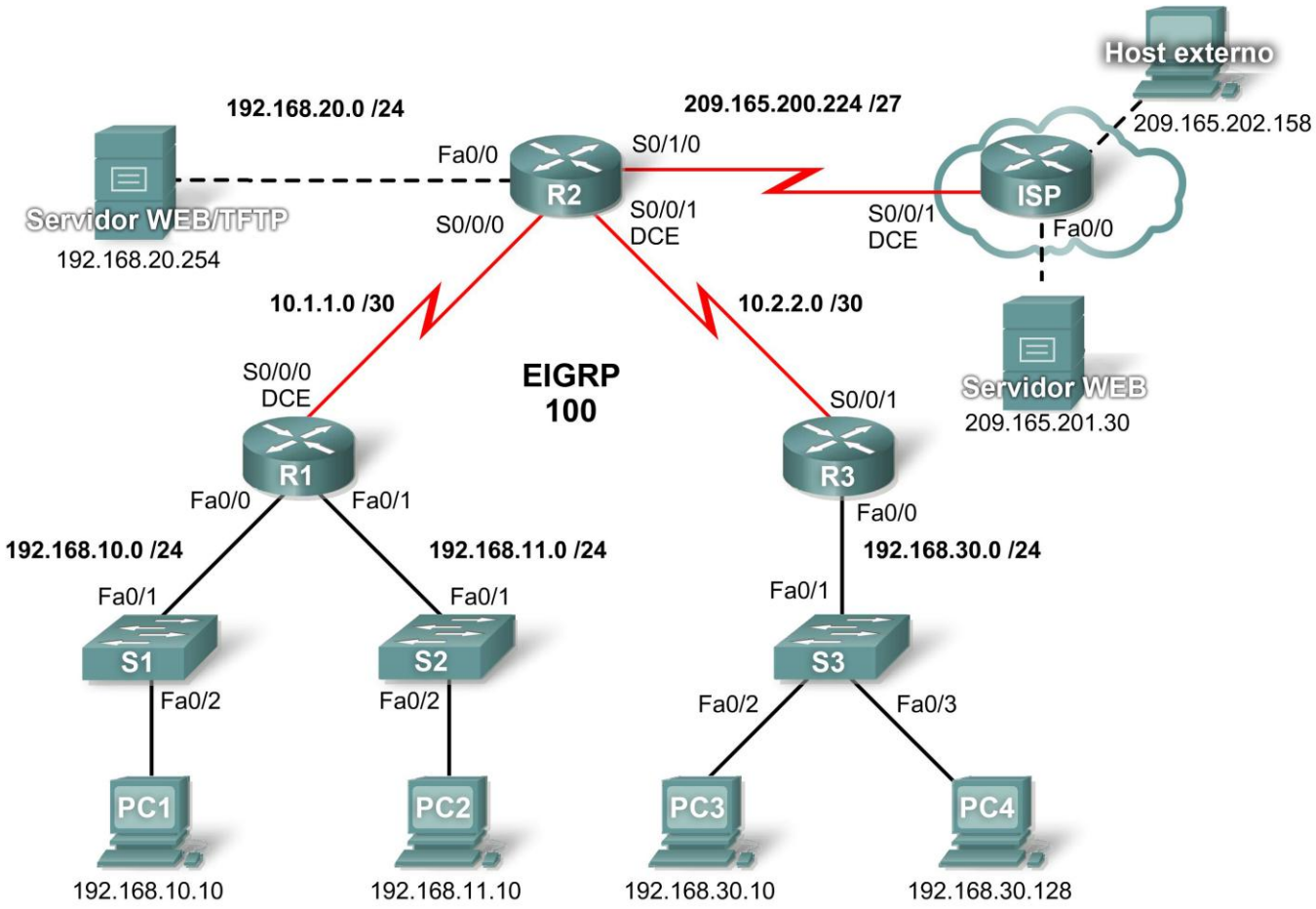


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**NIC**	192.168.10.10	255.255.255.0
PC2	**NIC**	192.168.11.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
PC4	**NIC**	192.168.30.128	255.255.255.0
Servidor TFTP/WEB	**NIC**	192.168.20.254	255.255.255.0
Servidor WEB	**NIC**	209.165.201.30	255.255.255.224
Host externo	**NIC**	209.165.202.158	255.255.255.224

Objetivos de aprendizaje

- Investigar la configuración actual de la red.
- Evaluar una política de red y planificar una implementación de ACL.
- Configurar ACL estándar y numeradas.
- Configurar ACL estándar y nombradas.

Introducción

Las ACL estándar son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, lo que incluye direcciones IP y enrutamiento EIGRP. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiada es **class**.

Tarea 1: Investigar la configuración actual de la red

Paso 1. Visualizar la configuración en ejecución en los routers.

Visualice la configuración en ejecución en los tres routers mediante el comando **show running-config** mientras esté en el modo EXEC privilegiado. Observe que las interfaces y el enrutamiento están totalmente configurados. Compare las configuraciones de la dirección IP con la tabla de direccionamiento que se muestra más arriba. En este momento, no debe haber ninguna ACL configurada en los routers.

El router ISP no requiere ninguna configuración durante este ejercicio. Supongamos que el router ISP no está bajo su administración y el administrador del ISP se ocupa de su configuración y mantenimiento.

Paso 2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Si no prueba la conectividad en su red antes de aplicar una ACL, probablemente la resolución de problemas sea más difícil.

Un paso útil en la prueba de conectividad es visualizar las tablas de enrutamiento en cada dispositivo para asegurarse de que cada red figure en éstas. En R1, R2 y R3 ejecute el comando **show ip route**. Debe ver que cada dispositivo tiene rutas conectadas para redes conectadas y rutas dinámicas a todas las demás redes remotas. Todos los dispositivos pueden acceder a todas las demás ubicaciones.

Aunque la tabla de enrutamiento puede ser útil para evaluar el estado de la red, la conectividad aún debe probarse al hacer **ping**. Realice las siguientes pruebas:

- Desde la PC1, haga ping a la PC2.
- Desde la PC2, haga ping al host externo.
- Desde la PC4, haga ping al servidor Web/TFTP.

Cada una de estas pruebas de conectividad debe tener éxito.

Tarea 2: Evaluar una política de red y planificar una implementación de ACL

Paso 1. Evaluar la política para las LAN del R1.

- La red 192.168.10.0/24 puede acceder a todas las ubicaciones, excepto a la red 192.168.11.0/24.
- La red 192.168.11.0/24 puede acceder a todos los demás destinos, excepto a cualquier red conectada al ISP.

Paso 2. Planificar la implementación de ACL para las LAN del R1.

- Dos ACL implementan completamente la política de seguridad para las LAN del R1.
- La primera ACL en el R1 deniega el tráfico desde la red 192.168.10.0/24 a la red 192.168.11.0/24 pero acepta el resto del tráfico.
- Esta primera ACL, aplicada en dirección de salida en la interfaz Fa0/1, monitorea el tráfico que se envía a la red 192.168.11.0.
- La segunda ACL en el R2 deniega el acceso de la red 192.168.11.0/24 al ISP pero acepta el resto del tráfico.
- El trafico saliente desde la interfaz S0/1/0 está controlado.
- Coloque las sentencias ACL en orden, desde la más específica a la menos específica. Se deniega el acceso del tráfico de la red a otra red antes de permitir el acceso del resto del tráfico.

Paso 3. Evaluar la política para la LAN del R3.

- La red 192.168.30.0/10 puede acceder a todos los destinos.
- El host 192.168.30.128 no tiene permitido el acceso fuera de la LAN.

Paso 4. Planificar la implementación de ACL para la LAN del R3.

- Una ACL implementa completamente la política de seguridad para la LAN del R3.
- La ACL se coloca en el R3 y deniega el acceso del host 192.168.30.128 fuera de la LAN pero permite el tráfico desde el resto de los hosts en la LAN.
- Al aplicar una ACL entrante en la interfaz Fa0/0, esta ACL monitoreará todo el tráfico que intente salir de la red 192.168.30.0/10.
- Coloque las sentencias ACL en orden, desde la más específica a la menos específica. Se deniega el acceso al host 192.168.30.128 antes de permitir el acceso al resto del tráfico.

Tarea 3: Configurar ACL estándar y numeradas

Paso 1. Determinar la máscara wildcard.

La máscara wildcard en una sentencia ACL determina cuánto se debe verificar en una dirección IP de origen o destino. Un bit 0 implica hacer coincidir ese valor en la dirección, mientras que un bit 1 ignora ese valor en la dirección. Recuerde que las ACL estándar sólo pueden verificar direcciones de origen.

- Debido a que la ACL en el R1 deniega todo el tráfico de la red 192.168.10.0/24, se rechazará toda dirección IP de origen que comience con 192.168.10. Dado que el último octeto de la dirección IP puede ignorarse, la máscara wildcard correcta es 0.0.0.255. Cada octeto en esta máscara puede interpretarse como “verificar, verificar, verificar, ignorar”.
- La ACL en el R2 también deniega el tráfico de la red 192.168.11.0/24. Puede aplicarse la misma máscara wildcard, 0.0.0.255.

Paso 2. Determinar las sentencias.

- Las ACL se configuran en el modo de configuración global.
- Para las ACL estándar, use un número entre 1 y 99. El número **10** se usa para esta lista en el R1 para ayudar a recordar que esta ACL monitorea la red 192.168.**10**.0.
- En el R2, la lista de acceso **11 denegará** el tráfico de la red 192.168.**11**.0 a cualquier red del ISP; por lo tanto, la opción **deny** está configurada con la red **192.168.11.0** y la máscara wildcard **0.0.0.255**.
- Debe permitirse el resto del tráfico con la opción **permit,** debido a la sentencia implícita “deny any” al final de las ACL. La opción **any** especifica a todo host de origen.

Configure lo siguiente en R1:

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Nota: Packet Tracer no calificará una configuración de ACL hasta tanto se ingresen todas las sentencias en el orden correcto.

Ahora cree una ACL en el R2 para denegar la red 192.168.11.0 y permitir las demás redes. Para esta ACL, use el número **11**. Configure lo siguiente en R2:

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Paso 3. Aplicar las sentencias a las interfaces.

En R1, ingrese al modo de configuración para la interfaz Fa0/1.

Ejecute el comando **ip access-group 10 out** para aplicar la ACL estándar saliente en la interfaz.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

En R2, ingrese al modo de configuración para la interfaz S0/1/0.

Ejecute el comando **ip access-group 11 out** para aplicar la ACL estándar saliente en la interfaz.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Paso 4. Verificar y probar las ACL.

Con las ACL configuradas y aplicadas, la PC1 (192.168.10.10) no debe poder hacer ping a la PC2 (192.168.11.10), ya que la ACL 10 se aplica con dirección de salida en la Fa0/1 en R1.

La PC2 (192.168.11.10) no debe poder hacer ping al servidor Web (209.165.201.30) ni al host externo (209.165.202.158), pero sí debe poder hacer ping a cualquier otra ubicación, ya que la ACL 11 se aplica en dirección de salida en la S0/1/0 en R2. Sin embargo, la PC2 no puede hacer ping a la PC1 porque la ACL 10 en R1 impide la respuesta de eco de la PC1 a la PC2.

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 67%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar ACL estándar y nombradas

Paso 1. Determinar la máscara wildcard.

- La política de acceso para R3 indica que el host en 192.168.30.128 no debe tener permitido ningún acceso fuera de la LAN local. El resto de los hosts de la red 192.168.30.0 debe tener permitido el acceso a las demás ubicaciones.
- Para verificar un único host, debe verificarse la dirección IP completa mediante la palabra clave **host**.
- Se permiten todos los paquetes que no coinciden con la sentencia host.

Paso 2. Determinar las sentencias.

- En R3, entre al modo de configuración global.
- Cree una ACL nombrada con la denominación NO_ACCESS mediante el comando **ip access-list standard NO_ACCESS**. Ingresará al modo de configuración de ACL. Todas las sentencias permit y deny se configuran desde este modo de configuración.
- Deniegue el tráfico desde el host 192.168.30.128 con la opción **host**.
- Permita todo el tráfico restante con **permit any**.

Configure la siguiente ACL nombrada en R3:

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Paso 3. Aplicar las sentencias a la interfaz correcta.

En R3, ingrese al modo de configuración para la interfaz Fa0/0.

Ejecute el comando **ip access-group NO_ACCESS in** para aplicar la ACL nombrada entrante en la interfaz. Este comando hace que todo el tráfico que ingresa a la interfaz Fa0/0 desde la LAN 192.168.30.0/24 se compare con la ACL.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```

Paso 4. Verificar y probar las ACL.

Haga clic en **Verificar resultados** y luego en **Pruebas de conectividad**. Las siguientes pruebas deben fallar:

- PC1 a PC2
- PC2 al host externo
- PC2 al servidor Web
- Todos los pings desde PC4 y hacia ésta, excepto entre PC3 y PC4

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para observar qué componentes requeridos aún no se han completado.

Actividad de PT 5.3.4: Configuración de las ACL extendidas

Diagrama de topología

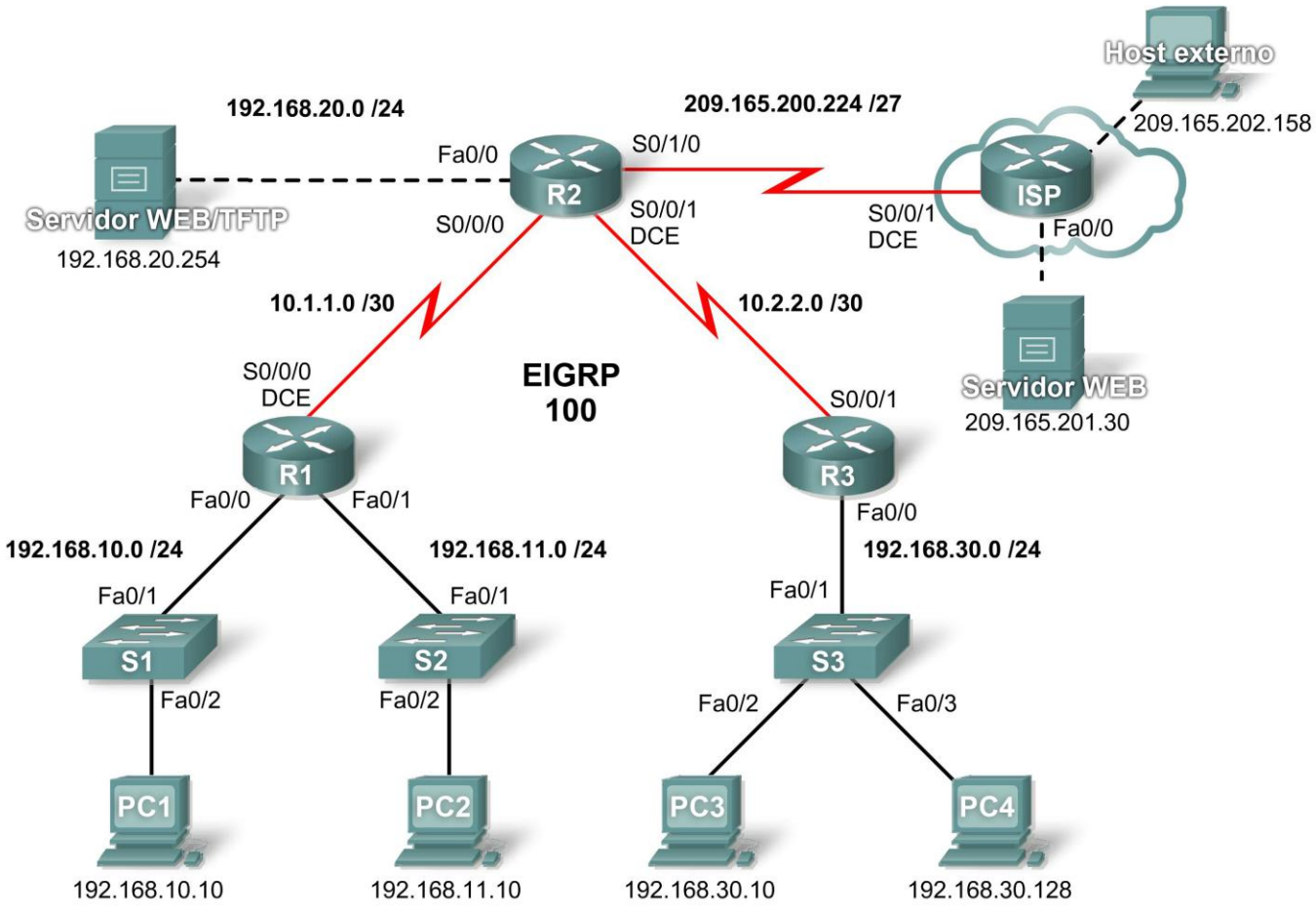


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**NIC**	192.168.10.10	255.255.255.0
PC2	**NIC**	192.168.11.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
PC4	**NIC**	192.168.30.128	255.255.255.0
Servidor TFTP/WEB	**NIC**	192.168.20.254	255.255.255.0
Servidor WEB	**NIC**	209.165.201.30	255.255.255.224
Host externo	**NIC**	209.165.202.158	255.255.255.224

Objetivos de aprendizaje

- Investigar la configuración actual de la red.
- Evaluar una política de red y planificar una implementación de ACL.
- Configurar ACL extendidas y numeradas.
- Configurar ACL extendidas y nombradas.

Introducción

Las ACL extendidas son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen o destino y los protocolos o puertos. Las ACL extendidas proporcionan mayor flexibilidad y especificidad que las ACL estándar. Esta actividad se concentra en definir criterios de filtrado, configurar ACL extendidas, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, lo que incluye direcciones IP y enrutamiento EIGRP. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiada es **class**.

Tarea 1: Investigar la configuración actual de la red

Paso 1. Visualizar la configuración en ejecución en los routers.

Visualice la configuración en ejecución en los tres routers mediante el comando **show running-config** mientras esté en el modo EXEC privilegiado. Observe que las interfaces y el enrutamiento están totalmente configurados. Compare las configuraciones de la dirección IP con la tabla de direccionamiento que se muestra más arriba. En este momento, no debe haber ninguna ACL configurada en los routers.

El router ISP no requiere ninguna configuración durante este ejercicio. Se supone que el router ISP no está bajo su administración y el administrador del ISP se ocupa de su configuración y mantenimiento.

Paso 2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Si no prueba la conectividad en su red antes de aplicar una ACL, la resolución de problemas será muy difícil.

A fin de asegurar la conectividad a lo largo de toda la red, utilice los comandos **ping** y **tracert** entre diferentes dispositivos de red para verificar las conexiones.

Tarea 2: Evaluar una política de red y planificar una implementación de ACL

Paso 1. Evaluar la política para las LAN del R1.

- Para la red 192.168.10.0/24, bloquee el acceso Telnet a todas las ubicaciones y el acceso TFTP al servidor Web/TFTP corporativo en 192.168.20.254. Se permite todo el acceso restante.
- Para la red 192.168.11.0/24, permita el acceso TFTP y el acceso Web al servidor Web/TFTP corporativo en 192.168.20.254. Bloquee el resto del tráfico de la red 192.168.11.0/24 a la red 192.168.20.0/24. Se permite todo el acceso restante.

Paso 2. Planificar la implementación de ACL para las LAN del R1.

- Dos ACL implementan completamente la política de seguridad para las LAN del R1.
- La primera ACL mantiene la primera parte de la política, se configura en R1 y se aplica con dirección de entrada a la interfaz Fast Ethernet 0/0.
- La segunda ACL mantiene la segunda parte de la política, se configura en R1 y se aplica con dirección de entrada a la interfaz Fast Ethernet 0/1.

Paso 3. Evaluar la política para la LAN del R3.

- Todas las direcciones IP de la red 192.168.30.0/24 tienen bloqueado el acceso a todas las direcciones IP de la red 192.168.20.0/24.
- La primera mitad de 192.168.30.0/24 puede acceder a todos los demás destinos.
- La segunda mitad de 192.168.30.0/24 puede acceder a las redes 192.168.10.0/24 y 192.168.11.0/24.
- La segunda mitad de 192.168.30.0/24 tiene permitido el acceso Web e ICMP a todos los demás destinos.
- El resto del acceso está implícitamente denegado.

Paso 4. Planificar la implementación de ACL para la LAN del R3.

Este paso requiere una ACL configurada en R3 y aplicada con dirección de entrada a la interfaz Fast Ethernet 0/0.

Paso 5. Evaluar la política para el tráfico proveniente de Internet a través del ISP.

- Los hosts externos pueden establecer una sesión de Web con el servidor Web interno únicamente en el puerto 80.
- Sólo se permiten las sesiones TCP establecidas.
- A través del R2 sólo se permiten respuestas de ping.

Paso 6. Planificar las implementaciones de ACL para el tráfico proveniente de Internet a través del ISP.

Este paso requiere una ACL configurada en R2 y aplicada con dirección de entrada a la interfaz Serial 0/1/0.

Tarea 3: Configurar ACL extendidas y numeradas

Paso 1. Determinar las máscaras wildcard.

Se necesitan dos ACL para implementar la política de control de acceso en R1. Ambas ACL se diseñarán para denegar una red de clase C completa. Se configurará una máscara wildcard que coincida con todos los hosts en cada una de estas redes de clase C.

Por ejemplo: para que la subred completa de 192.168.10.0/24 coincida, la máscara wildcard es 0.0.0.255. Esto puede interpretarse como “verificar, verificar, verificar, ignorar” y, básicamente, coincide con la red 192.168.10.0/24 completa.

Paso 2. Configurar la primera ACL extendida para R1.

Desde el modo de configuración global, configure la primera ACL con el número 110. En primer lugar, se debe bloquear Telnet a cualquier ubicación para todas las direcciones IP en la red 192.168.10.0/24.

Al escribir la sentencia, asegúrese de estar actualmente en el modo de configuración global.

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

A continuación, bloquee todas las direcciones IP en la red 192.168.10.0/24 del acceso TFTP al host en 192.168.20.254.

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Por último, permita el resto del tráfico.

```
R1(config)#access-list 110 permit ip any any
```

Paso 3. Configurar la segunda ACL extendida para R1.

Configure la segunda ACL con el número 111. Permita WWW al host en 192.168.20.254 para cualquier dirección IP en la red 192.168.11.0/24.

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

A continuación, permita TFTP al host en 192.168.20.254 para cualquier dirección IP en la red 192.168.11.0/24.

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Bloquee el resto del tráfico de la red 192.168.11.0/24 a la red 192.168.20.0/24.

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

Por último, permita cualquier otro tráfico. Esta sentencia garantiza que no se bloquee el tráfico proveniente de otras redes.

```
R1(config)#access-list 111 permit ip any any
```

Paso 4. Verificar las configuraciones de ACL.

Confirme sus configuraciones en R1 mediante el comando **show access-lists**. Los resultados serán similares a los siguientes:

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

Paso 5. Aplicar las sentencias a las interfaces.

Para aplicar una ACL a una interfaz, ingrese al modo de configuración de interfaz para esa interfaz. Configure el comando **ip access-group** *access-list-number* {**in** | **out**} para aplicar la ACL a la interfaz.

Cada ACL filtra el tráfico entrante. Aplique la ACL 110 a Fast Ethernet 0/0 y la ACL 111 a Fast Ethernet 0/1.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

Compruebe que las ACL aparezcan en la configuración en ejecución del R1 y que se hayan aplicado a las interfaces correctas.

Paso 6. Probar las ACL configuradas en R1.

Ahora que las ACL se configuraron y aplicaron, es muy importante comprobar que el tráfico esté bloqueado o permitido según lo previsto.

- Desde la PC1, intente obtener acceso Telnet a cualquier dispositivo. Esto debe estar bloqueado.
- Desde la PC1, intente acceder al servidor Web/TFTP corporativo a través de HTTP. Esto debe estar permitido.
- Desde la PC2, intente acceder al servidor Web/TFTP a través de HTTP. Esto debe estar permitido.
- Desde la PC2, intente acceder al servidor Web externo a través de HTTP. Esto debe estar permitido.

Según su conocimiento sobre ACL, intente algunas otras pruebas de conectividad desde la PC1 y la PC2.

Paso 7. Verificar los resultados.

Packet Tracer no admite la prueba del acceso TFTP; por lo tanto, no podrá verificar esa política. Sin embargo, su porcentaje de finalización debe ser del 50%. De lo contrario, haga clic en **Verificar resultados** para observar qué componentes requeridos aún no se han completado.

Tarea 4: Configurar una ACL extendida y numerada para R3

Paso 1. Determinar la máscara wildcard.

La política de acceso para la mitad inferior de las direcciones IP en la red 192.168.30.0/24 requiere:

- Denegar el acceso a la red 192.168.20.0/24.
- Permitir el acceso al resto de los destinos.

La mitad superior de las direcciones IP en la red 192.168.30.0/24 tiene las siguientes restricciones:

- Permitir el acceso a 192.168.10.0 y 192.168.11.0.
- Denegar el acceso a 192.168.20.0.
- Permitir el acceso Web e ICMP al resto de las ubicaciones.

Para determinar la máscara wildcard, considere qué bits deben verificarse para que la ACL coincida con las direcciones IP 0–127 (mitad inferior) o 128–255 (mitad superior).

Recuerde que una manera de determinar la máscara wildcard es restar la máscara de red normal de 255.255.255.255. La máscara normal para las direcciones IP 0–127 y 128–255 para una dirección de clase C es 255.255.255.128. Mediante el método de sustracción, a continuación se muestra la máscara wildcard correcta:

```
   255.255.255.255
 - 255.255.255.128
-----------------
     0.  0.  0.127
```

Paso 2. Configurar la ACL extendida en R3.

En R3, ingrese al modo de configuración global y configure la ACL con 130 como el número de lista de acceso.

La primera sentencia bloquea el acceso de la 192.168.30.0/24 a todas las direcciones en la red 192.168.30.0/24.

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

La segunda sentencia permite que la mitad inferior de la red 192.168.30.0/24 acceda a cualquier otro destino.

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

Las sentencias restantes permiten explícitamente que la mitad superior de la red 192.168.30.0/24 acceda a las redes y los servicios que permite la política de red.

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

Paso 3. Aplicar las sentencias a la interfaz.

Para aplicar una ACL a una interfaz, ingrese al modo de configuración de interfaz para esa interfaz. Configure el comando **ip access-group** *access-list-number* {**in** | **out**} para aplicar la ACL a la interfaz.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

Paso 4. Verificar y probar las ACL.

Ahora que la ACL se configuró y aplicó, es muy importante comprobar que el tráfico esté bloqueado o permitido según lo previsto.

- Desde la PC3, haga ping al servidor Web/TFTP. Esto debe estar bloqueado.
- Desde la PC3, haga ping a cualquier otro dispositivo. Esto debe estar permitido.
- Desde la PC4, haga ping al servidor Web/TFTP. Esto debe estar bloqueado.
- Desde la PC4, haga telnet a R1 en 192.168.10.1 ó 192.168.11.1. Esto debe estar permitido.
- Desde la PC4, haga ping a la PC1 y la PC2. Esto debe estar permitido.
- Desde la PC4, haga telnet a R2 en 10.2.2.2. Esto debe estar bloqueado.

Después de haber realizado estas pruebas y haber obtenido los resultados correctos, utilice el comando EXEC privilegiado **show access-lists** en R3 para verificar que las sentencias ACL coincidan.

Según su conocimiento sobre ACL, realice otras pruebas para verificar que cada sentencia coincida con el tráfico correcto.

Paso 5. Verificar los resultados.

Su porcentaje de finalización debe ser del 75%. De lo contrario, haga clic en **Verificar resultados** para observar qué componentes requeridos aún no se han completado.

Tarea 5: Configurar una ACL extendida y nombrada

Paso 1. Configurar una ACL extendida y nombrada en R2.

Recuerde que la política en R2 se diseñará para filtrar el tráfico de Internet. Debido a que R2 tiene la conexión al ISP, ésta es la mejor ubicación para la ACL.

Configure una ACL nombrada con la denominación FIREWALL en R2 mediante el comando **ip access-list extended** *name*. Este comando coloca al router en modo de configuración de ACL extendida y nombrada. Observe el indicador del router cambiado.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

En el modo de configuración de ACL, agregue las sentencias para filtrar el tráfico tal como se describe en la política:

- Los hosts externos pueden establecer una sesión de Web con el servidor Web interno únicamente en el puerto 80.
- Sólo se permiten las sesiones TCP establecidas.
- Las respuestas de ping se permiten a través de R2.

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

Después de configurar la ACL en R2, utilice el comando **show access-lists** para confirmar que la ACL tenga las sentencias correctas.

Paso 2. Aplicar las sentencias a la interfaz.

Utilice el comando **ip access-group** *name* {**in** | **out**} para aplicar la ACL entrante en la interfaz opuesta al ISP del R2.

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

Paso 3. Verificar y probar las ACL.

Realice las siguientes pruebas para asegurarse de que la ACL esté funcionando según lo previsto:

- Desde el host externo, abra una página Web en el servidor Web/TFTP interno. Esto debe estar permitido.
- Desde el host externo, haga ping al servidor Web/TFTP interno. Esto debe estar bloqueado.
- Desde el host externo, haga ping a la PC1. Esto debe estar bloqueado.
- Desde la PC1, haga ping al servidor Web externo en 209.165.201.30. Esto debe estar permitido.
- Desde la PC1, abra una página Web en el servidor Web externo. Esto debe estar permitido.

Después de haber realizado estas pruebas y haber obtenido los resultados correctos, utilice el comando EXEC privilegiado **show access-lists** en R2 para verificar que las sentencias de ACL coincidan.

Según su conocimiento sobre ACL, realice otras pruebas para verificar que cada sentencia coincida con el tráfico correcto.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para observar qué componentes requeridos aún no se han completado.

Actividad de PT 5.5.1: Listas de control de acceso básicas

Diagrama de topología

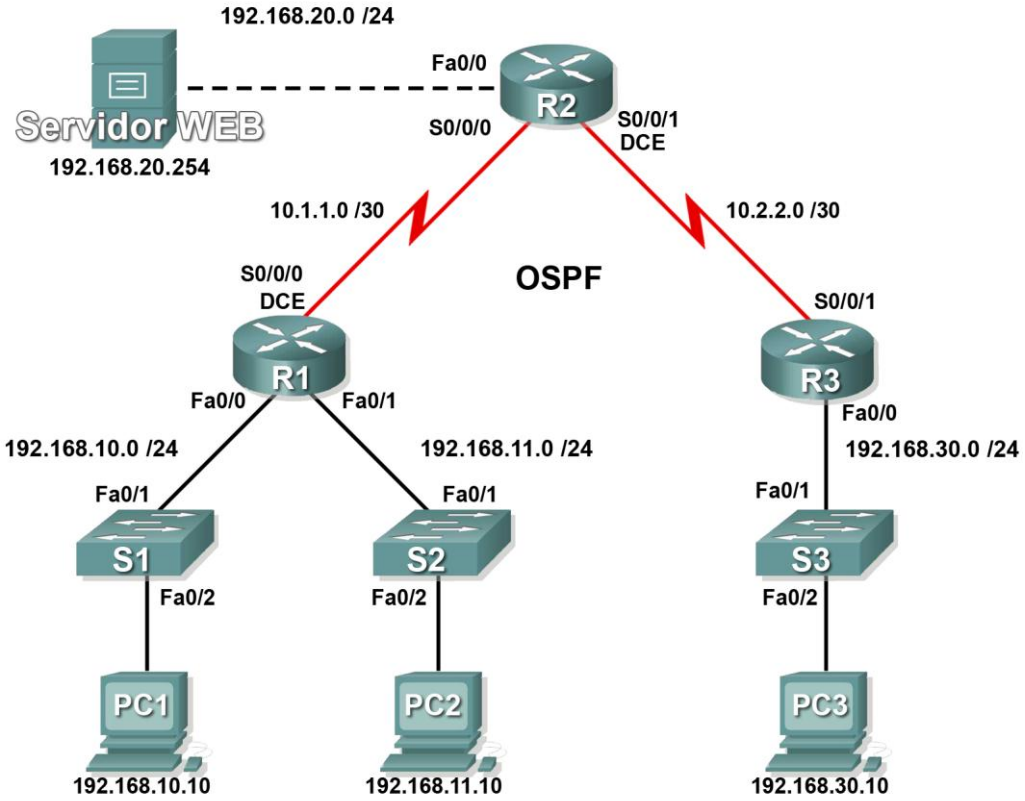


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/0**	192.168.10.1	255.255.255.0	No aplicable
	Fa0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
R2	**Fa0/0**	192.168.20.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
	Lo0	209.165.200.225	255.255.255.224	No aplicable
R3	**Fa0/0**	192.168.30.1	255.255.255.0	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable

Tabla de direccionamiento en la siguiente página

Tabla de direccionamiento (continuación)

S1	**VLAN 1**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**VLAN 1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**VLAN 1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

- Realizar las configuraciones básicas del router y el switch
- Configurar una ACL estándar
- Configurar una ACL extendida
- Controlar el acceso a las líneas vty con una ACL estándar
- Resolver problemas de las ACL

Introducción

En esta actividad se diseñarán, aplicarán y probarán las configuraciones de la lista de acceso y se resolverán sus problemas.

Tarea 1: Realizar las configuraciones básicas del router y el switch

Configure los routers R1, R2, R3 y los switches S1, S2 y S3 de acuerdo con las siguientes instrucciones:

- Configure los nombres de host para que coincidan con el diagrama de topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure un **mensaje del día**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones vty.
- Configure máscaras y direcciones IP en todos los dispositivos. Frecuencia de reloj de **64 000**.
- Habilite OSPF mediante el ID de proceso 1 en todos los routers para todas las redes.
- Configure una interfaz loopback en R2.
- Configure direcciones IP para la interfaz VLAN 1 en cada switch.
- Configure cada switch con la gateway predeterminada apropiada.
- Verifique la conectividad IP completa mediante el comando **ping**.

Tarea 2: Configurar una ACL estándar

Las ACL estándar pueden filtrar el tráfico según la dirección IP de origen únicamente. En esta tarea, se configura una ACL estándar que bloquea el tráfico desde la red 192.168.11.0 /24. Esta ACL se aplicará en dirección entrante en la interfaz serial del R3. Recuerde que cada ACL tiene un “deny all” implícito, por lo cual todo el tráfico que no tiene coincidencia con una sentencia en la ACL queda bloqueado. Por esta razón, agregue la sentencia **permit any** al final de la ACL.

Paso 1. Crear la ACL.

En el modo de configuración global, cree una ACL estándar nombrada, llamada **std-1**.

```
R3(config)#ip access-list standard std-1
```

En el modo de configuración de ACL estándar, agregue una sentencia que deniegue cualquier paquete con una dirección de origen de 192.168.11.0 /24 e imprima un mensaje a la consola por cada paquete coincidente.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255
```

Permita todo el tráfico restante.

```
R3(config-std-nacl)#permit any
```

Paso 2. Aplicar la ACL.

Aplique la ACL std-1 como filtro en los paquetes que ingresan al R3 a través de la interfaz serial 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group std-1 in
```

Paso 3. Probar la ACL.

Pruebe la ACL haciendo ping de la PC2 a la PC3. Debido a que la ACL está diseñada para bloquear el tráfico con direcciones de origen de la red 192.168.11.0 /24, la PC2 (192.168.11.10) no debería poder hacer ping a la PC3.

En el modo EXEC privilegiado en R3, ejecute el comando **show access-lists**. El resultado debe ser similar a lo siguiente. Cada línea de una ACL tiene un contador asociado que muestra cuántos paquetes han coincidido con la regla.

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

Tarea 3: Configurar una ACL extendida

Cuando se requiere un mayor nivel de detalle, se debe usar una ACL extendida. Las ACL extendidas pueden filtrar el tráfico basándose no sólo en la dirección de origen. Las ACL extendidas pueden filtrar según el protocolo, las direcciones IP de origen y destino, y los números de puerto de origen y destino.

Una política adicional para esta red establece que los dispositivos de la LAN 192.168.10.0/24 sólo tienen permitido alcanzar redes internas. Las computadoras en esta LAN no pueden acceder a Internet. Por lo tanto, estos usuarios deben tener bloqueada la posibilidad de alcanzar la dirección IP 209.165.200.225. Debido a que este requisito debe imponer tanto el origen como el destino, se necesita una ACL extendida.

En esta tarea, se configura una ACL extendida en R1 que bloquea el acceso del tráfico que se origina en cualquier dispositivo de la red 192.168.10.0 /24 al host 209.165.200.255 Esta ACL se aplicará en dirección saliente en la interfaz Serial 0/0/0 del R1.

Paso 1. Configurar una ACL extendida y nombrada.

En el modo de configuración global, cree una ACL extendida y nombrada, llamada **extend-1**.

```
R1(config)#ip access-list extended extend-1
```

Observe que el indicador del router cambia para señalar que ahora se encuentra en el modo de configuración de ACL extendida. Desde este indicador, agregue las sentencias necesarias para bloquear el tráfico de la red 192.168.10.0 /24 al host. Use la palabra clave **host** cuando defina el destino.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recuerde que el “deny all” implícito bloquea el resto del tráfico sin la sentencia adicional **permit**. Agregue la sentencia **permit** para asegurarse de que no se bloquee otro tráfico.

```
R1(config-ext-nacl)#permit ip any any
```

Paso 2. Aplicar la ACL.

Con las ACL estándar, lo más conveniente es ubicar a la ACL lo más cerca posible del destino. Las ACL extendidas normalmente se colocan cerca del origen. La ACL **extend-1** se colocará en la interfaz Serial y filtrará el tráfico saliente.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group extend-1 out
```

Paso 3. Probar la ACL.

Desde la PC1 o cualquier otro dispositivo en la red 192.168.10.0 /24, haga ping a la interfaz loopback en R2. Estos pings deben fallar porque todo el tráfico proveniente de la red 192.168.10.0 /24 se filtra cuando el destino es 209.165.200.225. Si el destino es cualquier otra dirección, los pings deben tener éxito. Confirme esto haciendo ping al R3 desde el dispositivo de red 192.168.10.0 /24.

Es posible verificarlo nuevamente al ejecutar **show ip access-list** en R1 después de hacer ping.

Deben aparecer coincidencias para ambas reglas de la ACL. Esto se debe a que el ping de la PC1 a la interfaz loopback del R2 se denegó, mientras que el ping al R3 se aceptó.

```
R1#show ip access-list
Extended IP access list extend-1
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))
    permit ip any any (4 match(es))
```

Tarea 4: Controlar el acceso a las líneas vty con una ACL estándar

Es conveniente restringir el acceso a las líneas vty del router para la administración remota. Una ACL puede aplicarse a las líneas vty, lo cual permite restringir el acceso a hosts o redes específicos. En esta tarea se configurará una ACL estándar para permitir que los hosts de dos redes accedan a las líneas vty. El resto de los hosts tiene denegado el acceso.

Verifique que pueda hacer telnet a R2 desde R1 y R3.

Paso 1. Configurar la ACL.

Configure una ACL estándar nombrada en R2 que permita el tráfico desde 10.2.2.0 /29 y 192.168.30.0 /24. Debe denegarse todo el tráfico restante. Denomine a la ACL **Task-4**.

```
R2(config)#ip access-list standard Task-4
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Paso 2. Aplicar la ACL.

Entre al modo de configuración de línea para las líneas vty de 0 a 4.

```
R2(config)#line vty 0 16
```

Utilice el comando **access-class** para aplicar la ACL a las líneas vty en dirección entrante. Observe que esto difiere del comando que se utiliza para aplicar las ACL a otras interfaces.

```
R2(config-line)#access-class Task-4 in
```

Paso 3. Probar la ACL.

Haga telnet a R2 desde R1. Observe que R1 no tiene direcciones IP en el rango de dirección mencionado en las sentencias de permiso de la ACL Task-4. Los intentos de conexión deben fallar.

Desde R3, haga telnet a R2 o a cualquier dispositivo en la red 192.168.30.0 /24. Se le presentará una petición de entrada para la contraseña de la línea vty.

¿Por qué los intentos de conexión desde otras redes fallan aunque no se enumeren específicamente en la ACL?

_____

_____

Tarea 5: Resolver problemas en las ACL

Cuando una ACL se configura o aplica mal a la interfaz incorrecta o en la dirección equivocada, el tráfico de red puede verse afectado de manera no deseada.

Paso 1. Probar la ACL.

En una tarea anterior, se creó y aplicó una ACL estándar y nombrada en R3. Utilice el comando **show running-config** para visualizar la ACL y su ubicación. Debe observar que una ACL llamada **std-1** se configuró y aplicó en dirección entrante en la interfaz Serial 0/0/1. Recuerde que esta ACL se diseñó para bloquear el acceso del tráfico de red con una dirección de origen de la red 192.168.11.0 /24 a la LAN en R3.

Para eliminar la ACL, ingrese al modo de configuración de interfaz para Serial 0/0/1 en R3.

```
R3(config)#interface serial 0/0/1
```

Use el comando **no ip access-group std-1 in** para eliminar la ACL de la interfaz.

```
R3(config-if)#no ip access-group std-1 in
```

Use el comando **show running-config** para confirmar que la ACL se haya eliminado de la Serial 0/0/1.

Paso 2. Aplicar la ACL std-1 en S0/0/1 con dirección saliente.

Para probar la importancia de la dirección de filtrado de la ACL, aplique nuevamente la ACL **std-1** a la interfaz Serial 0/0/1. Esta vez la ACL filtrará el tráfico saliente en lugar del tráfico entrante. Recuerde usar la palabra clave **out** al aplicar la ACL.

```
R3(config-if)#ip access-group std-1 out
```

Paso 3. Probar la ACL.

Pruebe la ACL haciendo ping de la PC2 a la PC3. Como alternativa, use un ping extendido desde R1. Observe que esta vez los pings tienen éxito y los contadores de la ACL no aumentan. Es posible confirmarlo mediante el comando **show ip access-list** en R3.

Paso 4. Restaurar la configuración inicial de la ACL.

Elimine la ACL de la dirección saliente y aplíquela nuevamente a la dirección entrante.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group std-1 out
R3(config-if)#ip access-group std-1 in
```

Paso 5. Aplicar Task-4 a la interfaz serial 0/0/0 de R2 en dirección entrante.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

Paso 6. Probar la ACL.

Intente comunicarse con cualquier dispositivo conectado a R2 o R3 desde R1 o sus redes conectadas. Observe que la comunicación está bloqueada; sin embargo, los contadores de la ACL no aumentan. Esto se debe al “deny all” implícito al final de cada ACL.

Después de que expiran los temporizadores muertos de OSPF, deben verse mensajes impresos en las consolas de R1 y R2 similares a los siguientes

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Elimine la ACL Task-4 de la interfaz.

Actividad de PT 5.5.2: Desafío de Listas de control de acceso

Diagrama de topología

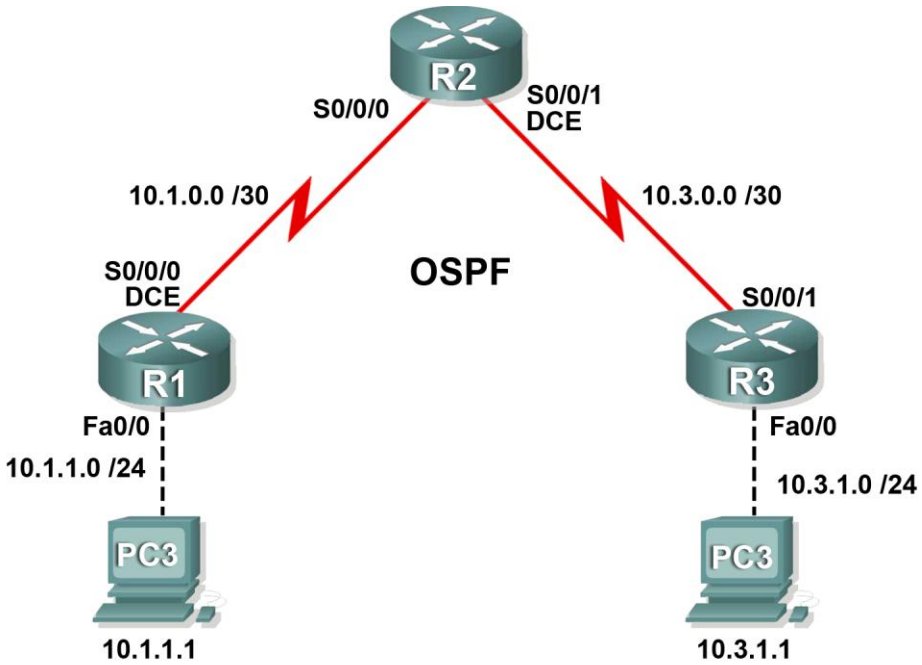


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**S0/0/0**	10.1.0.1	255.255.255.252	No aplicable
	Fa0/0	10.1.1.254	255.255.255.0	No aplicable
R2	**S0/0/0**	10.1.0.2	255.255.255.252	No aplicable
	S0/0/1	10.3.0.1	255.255.255.252	No aplicable
R3	**S0/0/1**	10.3.0.2	255.255.255.252	No aplicable
	Fa0/0	10.3.1.254	255.255.255.0	No aplicable
PC1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC2	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Objetivos de aprendizaje

- Realizar las configuraciones básicas del router
- Configurar las ACL estándar
- Configurar las ACL extendidas
- Verificar las ACL

Introducción

En esta actividad se diseñarán, aplicarán y probarán las configuraciones de la lista de acceso y se resolverán sus problemas.

Tarea 1: Realizar las configuraciones básicas del router

Configure todos los dispositivos según las siguientes pautas:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC: **class**.
- Configure un **mensaje del día**.
- Configure la contraseña **cisco** para las conexiones de consola.
- Configure la contraseña **cisco** para las conexiones vty.
- Configure máscaras y direcciones IP en todos los dispositivos. Frecuencia de reloj de **64 000**.
- Habilite OSPF mediante el ID de proceso 1 en todos los routers para todas las redes.
- Verifique la conectividad IP completa mediante el comando **ping**.

Tarea 2: Configurar las ACL estándar

Configure las ACL estándar y nombradas en las líneas vty de R1 y R3, de modo que los hosts directamente conectados a sus subredes Fast Ethernet tengan acceso a Telnet. Deniegue todos los demás intentos de conexión. Denomine **VTY-Local** a estas ACL estándar y aplíquelas a todas las líneas telnet. Documente la configuración de ACL.

_____

_____

_____

_____

_____

_____

_____

Tarea 3: Configurar las ACL extendidas

Complete los siguientes requisitos mediante las ACL extendidas en R2:

- Asigne un nombre al bloque de la ACL.
- Prohiba que el tráfico que se origina desde las subredes conectadas de R1 alcance las subredes conectadas de R3.
- Prohiba que el tráfico que se origina desde las subredes conectadas de R3 alcance las subredes conectadas de R1.
- Permita todo el tráfico restante.

Documente la configuración de ACL.

Tarea 4: Verificar las ACL

Paso 1. Probar telnet.

- La PC1 debe poder hacer telnet a R1.
- La PC3 debe poder hacer telnet a R3.
- R2 debe tener denegado el acceso telnet a R1 y R3.

Paso 2. Probar el tráfico.

Los pings entre PC1 y PC3 deben fallar.

Actividad del PT 5.6.1: Desafío de integración de aptitudes del Packet Tracer

Diagrama de topología

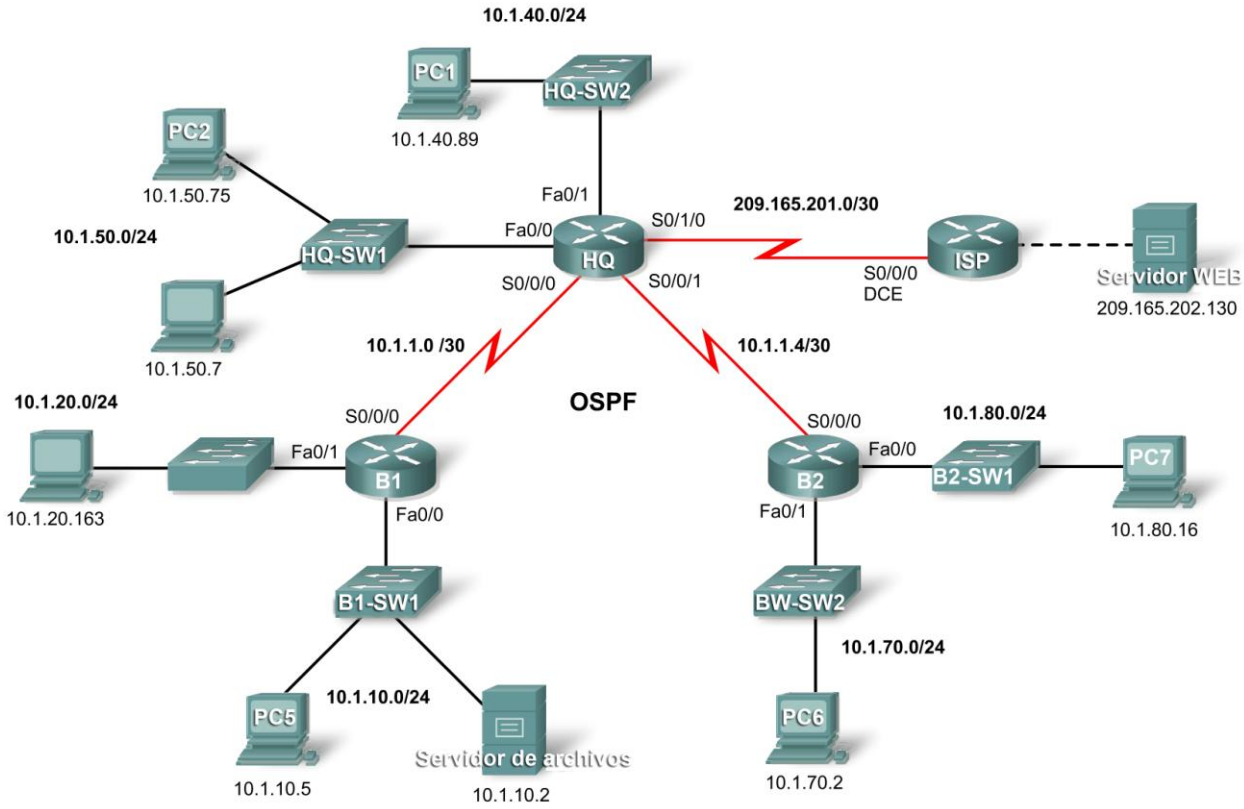


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
HQ	**S0/0/0**	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	**S0/0/0**	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	**S0/0/0**	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Servidor Web	**NIC**	209.165.202.130	255.255.255.252

Objetivos de aprendizaje

- Configurar PPP con autenticación CHAP
- Configurar enrutamiento predeterminado
- Configurar el enrutamiento OSPF
- Implementar y verificar diversas políticas de seguridad de ACL

Introducción

En esta actividad, demostrará su capacidad para configurar las ACL que cumplen con cinco políticas de seguridad. Además, configurará PPP y el enrutamiento OSPF. Los dispositivos ya están configurados con direccionamiento IP. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiada es **class**.

Tarea 1: Configurar PPP con autenticación CHAP

Paso 1. Configurar el enlace entre HQ y B1 para utilizar la encapsulación PPP con autenticación CHAP.

La contraseña para la autenticación CHAP es **cisco123**.

Paso 2. Configurar el enlace entre HQ y B2 para utilizar la encapsulación PPP con autenticación CHAP.

La contraseña para la autenticación CHAP es **cisco123**.

Paso 3. Verificar que se haya restablecido la conectividad entre los routers.

HQ debe poder hacer ping a B1 y B2. Es posible que las interfaces demoren algunos minutos en volver a activarse. Para acelerar el proceso puede alternar entre el modo Tiempo Real y Simulación. Otra solución posible ante esta respuesta de Packet Tracer es utilizar los comandos **shutdown** y **no shutdown** en las interfaces.

Nota: Es posible que las interfaces dejen de funcionar en momentos esporádicos durante la actividad debido a un defecto del Packet Tracer. Normalmente la interfaz vuelve a activarse automáticamente después de algunos segundos.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 29%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar enrutamiento predeterminado

Paso 1. Configurar el enrutamiento predeterminado de HQ al ISP.

Configure una ruta predeterminada en HQ mediante el argumento de *interfaz de salida* para enviar todo el tráfico predeterminado al ISP.

Paso 2. Probar la conectividad al servidor Web.

HQ debe poder hacer ping con éxito al servidor Web en 209.165.202.130 siempre que el origen del ping sea la interfaz Serial0/1/0.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 32%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar el enrutamiento OSPF

Paso 1. Configurar OSPF en HQ.

- Configure OSPF mediante el ID de proceso 1.
- Publique todas las subredes, excepto la red 209.165.201.0.
- Propague la ruta predeterminada a vecinos OSPF.
- Deshabilite las actualizaciones de OSPF al ISP y a las LAN de HQ.

Paso 2. Configurar OSPF en B1 y B2.

- Configure OSPF mediante el ID de proceso 1.
- En cada router, configure las subredes apropiadas.
- Deshabilite las actualizaciones de OSPF a las LAN.

Paso 3. Probar la conectividad en toda la red.

Ahora la red debe tener conectividad total de extremo a extremo. Todos los dispositivos deben poder hacer ping con éxito a todos los demás dispositivos, incluso al servidor Web en 209.165.202.130.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 76%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Implementar diversas políticas de seguridad de ACL

Paso 1. Implementar la política de seguridad número 1.

Bloquee a la red 10.1.10.0 el acceso a la red 10.1.40.0. Se permite todo el acceso restante a 10.1.40.0. Configure la ACL en HQ mediante la ACL número 10.

- ¿Usará una ACL estándar o extendida? _____
- ¿A qué interfaz aplicará la ACL? _____

- ¿En qué dirección aplicará la ACL? _____

_____

_____

_____

_____

_____

Paso 2. Verificar la implementación de la política de seguridad número 1.

Un ping de la PC5 a la PC1 debe fallar.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 80%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Paso 4. Implementar la política de seguridad número 2.

El host 10.1.10.5 no tiene permitido el acceso al host 10.1.50.7. Todos los hosts restantes pueden acceder a 10.1.50.7. Configure la ACL en B1 mediante la ACL número 115.

- ¿Usará una ACL estándar o extendida? _____
- ¿A qué interfaz aplicará la ACL? _____
- ¿En qué dirección aplicará la ACL? _____

_____

_____

_____

_____

_____

Paso 5. Verificar la implementación de la política de seguridad número 2.

Un ping de la PC5 a la PC3 debe fallar.

Paso 6. Verificar los resultados.

Su porcentaje de finalización debe ser del 85%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Paso 7. Implementar la política de seguridad número 3.

El rango de hosts de 10.1.50.1 a través de 10.1.50.63 no tienen permitido el acceso Web al servidor de Intranet en 10.1.80.16. Se permite todo el acceso restante. Configure la ACL en el router apropiado y utilice la ACL número 101.

- ¿Usará una ACL estándar o extendida? _____
- ¿En qué router configurará la ACL? _____
- ¿A qué interfaz aplicará la ACL? _____
- ¿En qué dirección aplicará la ACL? _____

_____

_____

_____

_____

_____

Paso 8. Verificar la implementación de la política de seguridad número 3.

Para probar esta política, haga clic en PC3, luego en la ficha **Escritorio** y luego en **explorador Web**. Para el URL, escriba la dirección IP para el servidor de Intranet, 10.1.80.16 y presione **Intro**. Después de algunos segundos, debe recibir un mensaje de solicitud de tiempo de espera. La PC2 y cualquier otra PC de la red deben poder acceder al servidor de Intranet.

Paso 9. Verificar los resultados.

Su porcentaje de finalización debe ser del 90%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Paso 10. Implementar la política de seguridad número 4.

Use el nombre **NO_FTP** para configurar una ACL nombrada que bloquee a la red 10.1.70.0/24 el acceso a servicios FTP (puerto 21) en el servidor de archivos de 10.1.10.2. Se debe permitir cualquier otro acceso.

Nota: Los nombres distinguen mayúsculas de minúsculas.

- ¿Usará una ACL estándar o extendida? _____
- ¿En qué router configurará la ACL? _____
- ¿A qué interfaz aplicará la ACL? _____
- ¿En qué dirección aplicará la ACL? _____

_____

_____

_____

_____

_____

Paso 11. Verificar los resultados.

Packet Tracer no admite la prueba del acceso FTP; por lo tanto, no podrá verificar esta política. Sin embargo, su porcentaje de finalización debe ser del 95%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Paso 12. Implementar la política de seguridad número 5.

Dado que el ISP representa la conectividad a Internet, configure una ACL nombrada con la denominación **FIREWALL** en el siguiente orden:

1. Permita únicamente respuestas de ping entrantes desde el ISP y cualquier otro origen.
2. Permita únicamente sesiones TCP establecidas desde el ISP y cualquier otro origen.
3. Bloquee explícitamente cualquier otro acceso entrante desde el ISP y cualquier otro origen.

- ¿Usará una ACL estándar o extendida? _____
- ¿En qué router configurará la ACL? _____
- ¿A qué interfaz aplicará la ACL? _____
- ¿En qué dirección aplicará la ACL? _____

_____

_____

_____

_____

_____

Paso 13. Verificar la implementación de la política de seguridad número 5.

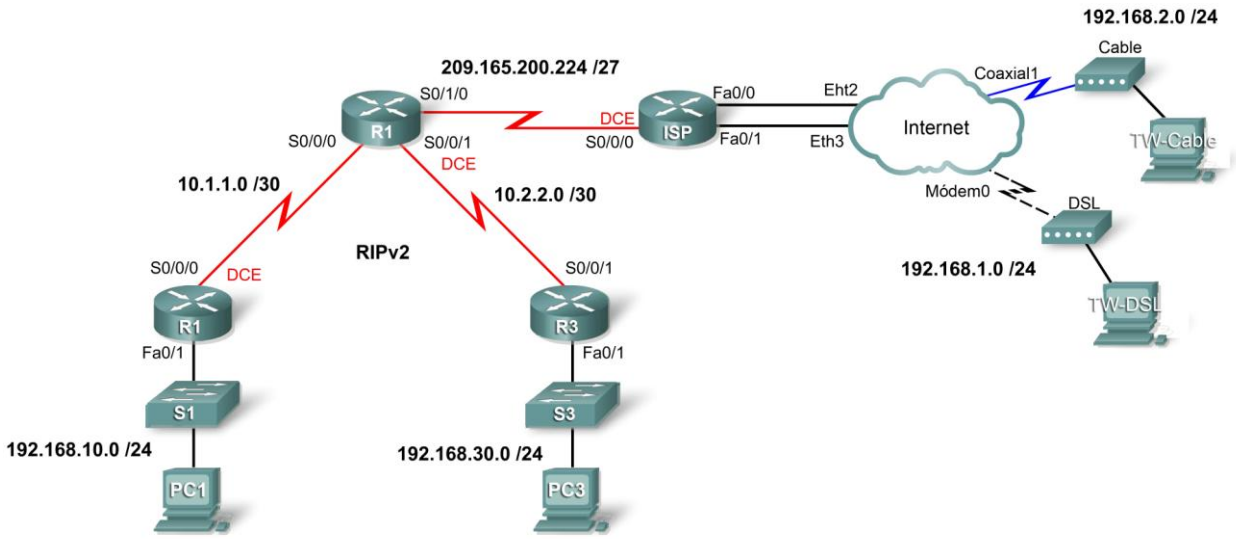
Para probar esta política, cualquier PC debe poder hacer ping al ISP o al servidor Web. Sin embargo, ni el ISP ni el servidor Web deben poder hacer ping a HQ o a cualquier otro dispositivo detrás de la ACL. **FIREWALL**

Paso 14. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Actividad de PT 6.2.4: Servicios de banda ancha

Diagrama de topología



Objetivos de aprendizaje

- Conectar el ISP a la nube de Internet
- Agregar dispositivos WAN
- Conectar un dispositivo WAN a la nube de Internet
- Conectar las PC de teletrabajador a los dispositivos WAN
- Probar la conectividad

Introducción

En esta actividad, demostrará su capacidad para agregar dispositivos y conexiones de banda ancha al Packet Tracer. Aunque no puede configurar DSL ni módem por cable, puede simular la conectividad de extremo a extremo a dispositivos de teletrabajadores.

Tarea 1: Conectar el ISP a la nube de Internet

Paso 1. Realizar conexiones mediante las interfaces que se muestran en la topología.

- Conecte Fa0/0 en ISP a Eth2 en la Nube de Internet.
- Conecte Fa0/1 en ISP a Eth3 en la Nube de Internet.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 25%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Agregar dispositivos WAN

Paso 1. Agregar dispositivos por cable y DSL.

Los dispositivos de **módem DSL** y **módem por cable** se encuentran en el menú **Emulación WAN**. Colóquelos como lo haría con cualquier otro dispositivo.

Paso 2. Nombrar los dispositivos WAN.

Use la ficha Configuración para cambiar el nombre de visualización de cada dispositivo WAN a **Cable** y **DSL**, respectivamente.

Tarea 3: Conectar los dispositivos WAN a la nube de Internet

Paso 1. Conecte el módem por cable a la nube de Internet.

Seleccione el tipo de conexión **Coaxial** en el menú **Conexión**.

Paso 2. Conectar el módem DSL a la nube de Internet.

Seleccione el tipo de conexión **Telefónica** en el menú **Conexión**.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 75%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Conectar las PC de teletrabajador a los dispositivos WAN

Paso 1. Conectar el cable del teletrabajador al cable.

Paso 2. Conectar la DSL del teletrabajador a la DSL.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Probar la conectividad

Haga clic en **Verificar resultados** y luego en la ficha Pruebas de conectividad para verificar que los dispositivos de teletrabajador puedan comunicarse con las PC internas.

Actividad del PT 6.4.1: Desafío de integración de aptitudes del Packet Tracer

Diagrama de topología

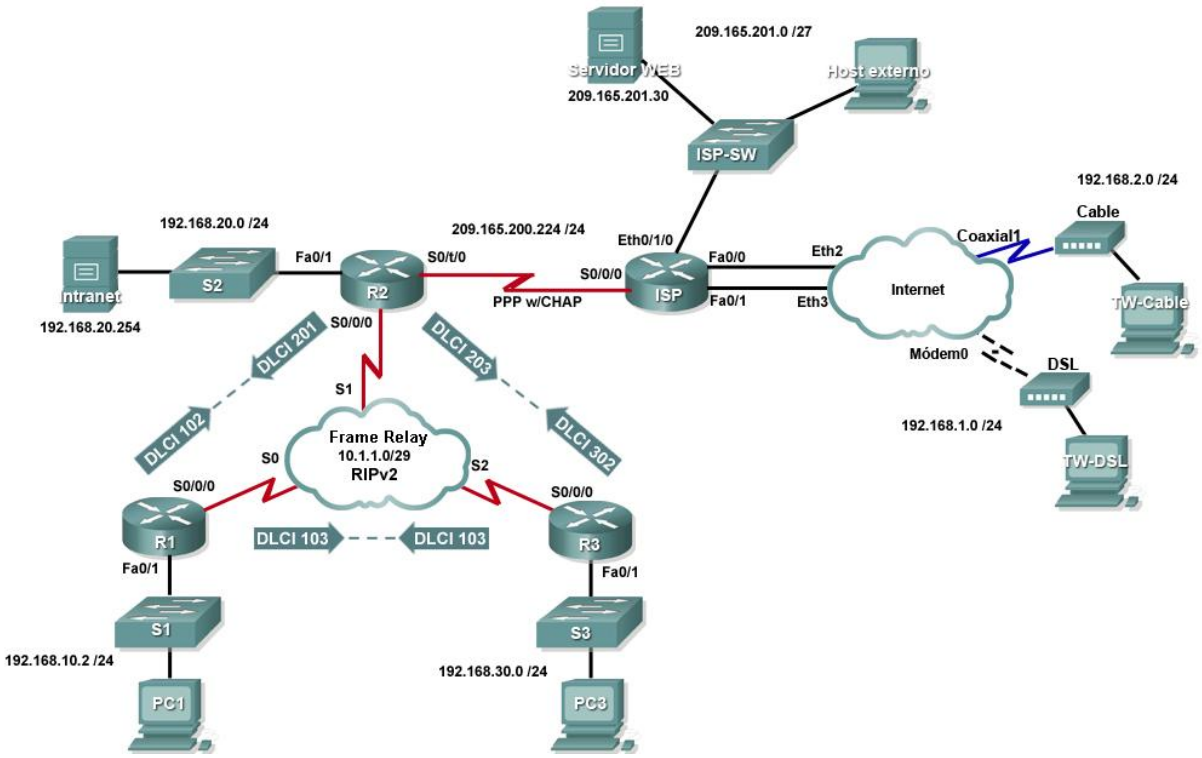


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.248
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.248
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.1.1.3	255.255.255.248
ISP	**S0/0/0**	209.165.200.226	255.255.255.224
	Eth0/1/0	209.165.201.1	255.255.255.224
	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.2.1	255.255.255.0
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
Intranet	**NIC**	192.168.20.254	255.255.255.0
DSL del teletrabajador	**NIC**	192.168.1.10	255.255.255.0
Cable del teletrabajador	**NIC**	192.168.2.10	255.255.255.0
Servidor Web	**NIC**	209.165.201.30	255.255.255.224
Host externo	**NIC**	209.165.201.10	255.255.255.224

Objetivos de aprendizaje

- Aplicar las configuraciones básicas del router
- Configurar el enrutamiento dinámico y predeterminado
- Establecer servicios de teletrabajador
- Probar la conectividad antes de la configuración de ACL
- Aplicar políticas de ACL
- Probar la conectividad después de la configuración de ACL

Introducción

Esta actividad requiere que configure una ruta predeterminada y el enrutamiento dinámico mediante la versión 2 del RIP. También se agregan servicios de banda ancha a la red. Por último, se configuran las ACL en dos routers para controlar el tráfico de red. Debido a que el Packet Tracer es muy específico en la manera de clasificar las ACL, las reglas de ACL se deberán configurar en el orden dado.

Tarea 1: Aplicar las configuraciones básicas del router

Mediante la información en el diagrama de topología y la tabla de direccionamiento, realice las configuraciones básicas de dispositivos en R1, R2 y R3. Los nombres de hosts ya se configuraron.

Incluya lo siguiente:

- Líneas de consola y vty
- Mensajes
- Deshabilite la búsqueda de nombre de dominio
- Descripción de las interfaces

Tarea 2: Configurar el enrutamiento dinámico y predeterminado

Paso 1. Configurar el enrutamiento predeterminado.

R2 necesita una ruta predeterminada. Use el argumento de *interfaz de salida* en la configuración de la ruta predeterminada.

Paso 2. Configurar el enrutamiento dinámico.

Configure RIPv2 en R1, R2 y R3 para todas las redes disponibles. R2 debe pasar su configuración de red predeterminada a los otros routers. Además, asegúrese de utilizar el comando **passive-interface** en todas las interfaces activas que no se utilizan para el enrutamiento.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 59%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Establecer servicios de teletrabajador

Paso 1. Agregar los dispositivos WAN.

Agregue un módem por cable y un DSL según el diagrama de topología.

Paso 2. Nombrar los dispositivos WAN.

Use la ficha **Configuración** para cambiar el nombre de visualización de cada dispositivo WAN a **Cable** y **DSL**, respectivamente.

Paso 3. Conectar los dispositivos WAN.

Conecte los dispositivos WAN a sus PC e Internet mediante los cables y las interfaces adecuados.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 86%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Probar la conectividad antes de la configuración de ACL

En este momento, todas las ramas de la topología deben tener conectividad. Si alterna entre el modo Simulación y Tiempo Real, se puede acelerar la convergencia.

Tarea 5: Aplicar políticas de ACL

Paso 1. Crear y aplicar la política de seguridad número 1.

Implemente las siguientes reglas de ACL mediante la ACL número 101:

1. Permita que los hosts de la red 192.168.30.0/24 tengan acceso Web a cualquier destino.

2. Permita que los hosts de la red 192.168.30.0/24 tengan acceso mediante ping a cualquier destino.
3. Deniegue cualquier otro acceso que se origine en la red.

Paso 2. Crear y aplicar la política de seguridad número 2.

Dado que el ISP representa la conectividad a Internet, configure una ACL nombrada, llamada **FIREWALL**, en el siguiente orden:

1. Permita el acceso Web de la DSL del teletrabajador al servidor de Intranet.
2. Permita el acceso Web del cable del teletrabajador al servidor de Intranet.
3. Permita únicamente respuestas de ping entrantes desde el ISP y cualquier otro origen.
4. Permita únicamente sesiones TCP establecidas desde el ISP y cualquier otro origen.
5. Bloquee explícitamente cualquier otro acceso entrante desde el ISP y cualquier otro origen.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Probar la conectividad después de la configuración de ACL

Los teletrabajadores no deben poder hacer ping al servidor de Intranet, pero sí deben poder acceder a su servidor HTTP a través del explorador Web. En esta actividad se incluyen tres PDU, dos de los cuales deben fallar y uno debería tener éxito. Verifique las **Pruebas de conectividad** en el menú **Verificar resultados** a fin de asegurarse de que los resultados de finalización sean del 100%.

Actividad de PT 7.1.8: Configuración de DHCP mediante Easy IP

Diagrama de topología

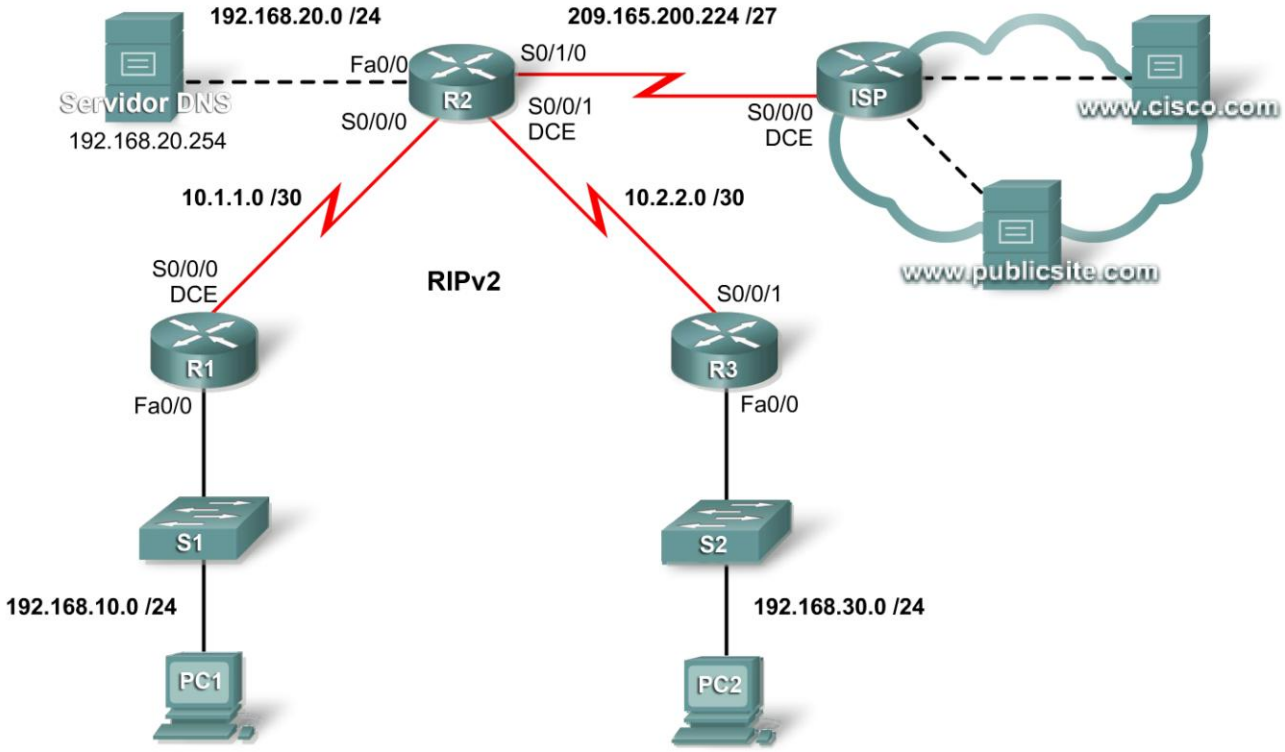


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Objetivos de aprendizaje

- Configurar los routers con Easy IP
- Verificar que las PC se configuren automáticamente con detalles de direccionamiento
- Configurar un servidor DNS con entradas DNS
- Probar la conectividad de la PC a los nombres de dominio

Introducción

DHCP asigna direcciones IP y otra información de configuración de red importante en forma dinámica. Los routers Cisco pueden utilizar el conjunto de funciones Cisco IOS; es decir, Easy IP, como servidor de DHCP opcional con todas las funciones. Easy IP alquila las configuraciones por 24 horas de manera predeterminada. En esta actividad se configurarán los servicios DHCP en dos routers y se probará su configuración.

Tarea 1: Configurar los routers con Easy IP

Paso 1. Configurar las direcciones excluidas para R1 y R3.

Defina un conjunto de direcciones que se reservan para hosts que necesitan direcciones estáticas, como servidores, routers e impresoras. Estas direcciones no se incluyen en el conjunto de direcciones disponibles para asignar a clientes de DHCP. Para R1 y R3, excluya las primeras nueve direcciones del pool de DHCP.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#

R3(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
R3(config)#
```

Paso 2. Configurar el conjunto de direcciones para R1.

Defina el conjunto de direcciones desde las que DHCP asigna direcciones a clientes de DHCP en la LAN de R1. Las direcciones disponibles son todas las direcciones en la red 192.168.10.0, excepto las que se excluyen en el Paso 1.

En R1, asigne al conjunto de direcciones el nombre R1LAN. Especifique el conjunto de direcciones, la gateway predeterminada y el servidor DNS que se asignan a cada dispositivo cliente que solicita el servicio DHCP.

```
R1(config)#ip dhcp pool R1LAN
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 192.168.20.254
```

Paso 3. Configurar el conjunto de direcciones para R3.

En R3, asigne al conjunto de direcciones el nombre R3LAN. Especifique el conjunto de direcciones, la gateway predeterminada y el servidor DNS que se asignan a cada dispositivo cliente que solicita el servicio DHCP.

```
R3(config)#ip dhcp pool R3LAN
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.30.1
```

```
R3(dhcp-config)#dns-server 192.168.20.254
```

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 43%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Verificar que las PC se configuren automáticamente

Paso 1. Configurar la PC1 y PC3 para la configuración DHCP.

En la ficha **Escritorio** de cada PC, haga clic en **Configuración IP** y luego seleccione **DHCP**. La información de configuración IP debe actualizarse de inmediato.

Paso 2. Verificar la operación DHCP en los routers.

Para verificar la operación DHCP en los routers, ejecute el comando **show ip dhcp binding**. Los resultados deben mostrar una dirección IP ligada a cada uno de los routers.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 86%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar un servidor DNS con entradas DNS

Paso 1. Configurar el servidor DNS.

Para configurar DNS en el servidor DNS, haga clic en el botón **DNS** de la ficha **Configuración**.

Asegúrese de que el DNS esté encendido e ingrese las siguientes entradas DNS:

- www.cisco.com 209.165.201.30
- www.publicsite.com 209.165.202.158

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Probar la conectividad de la PC a los nombres de dominio

Paso 1. Verificar que la PC1 pueda conectarse a los servidores mediante el nombre de dominio.

En la PC1, abra el explorador Web e ingrese **www**.**cisco**.**com** en la barra de direcciones. Debe aparecer una página Web.

Paso 2. Verificar que la PC3 pueda conectarse a los servidores mediante el nombre de dominio.

En la PC3, abra el explorador Web e ingrese **www**.**publicsite**.**com** en la barra de direcciones. Debe aparecer una página Web.

Actividad de PT 7.2.8: Escalabilidad de redes con NAT

Diagrama de topología

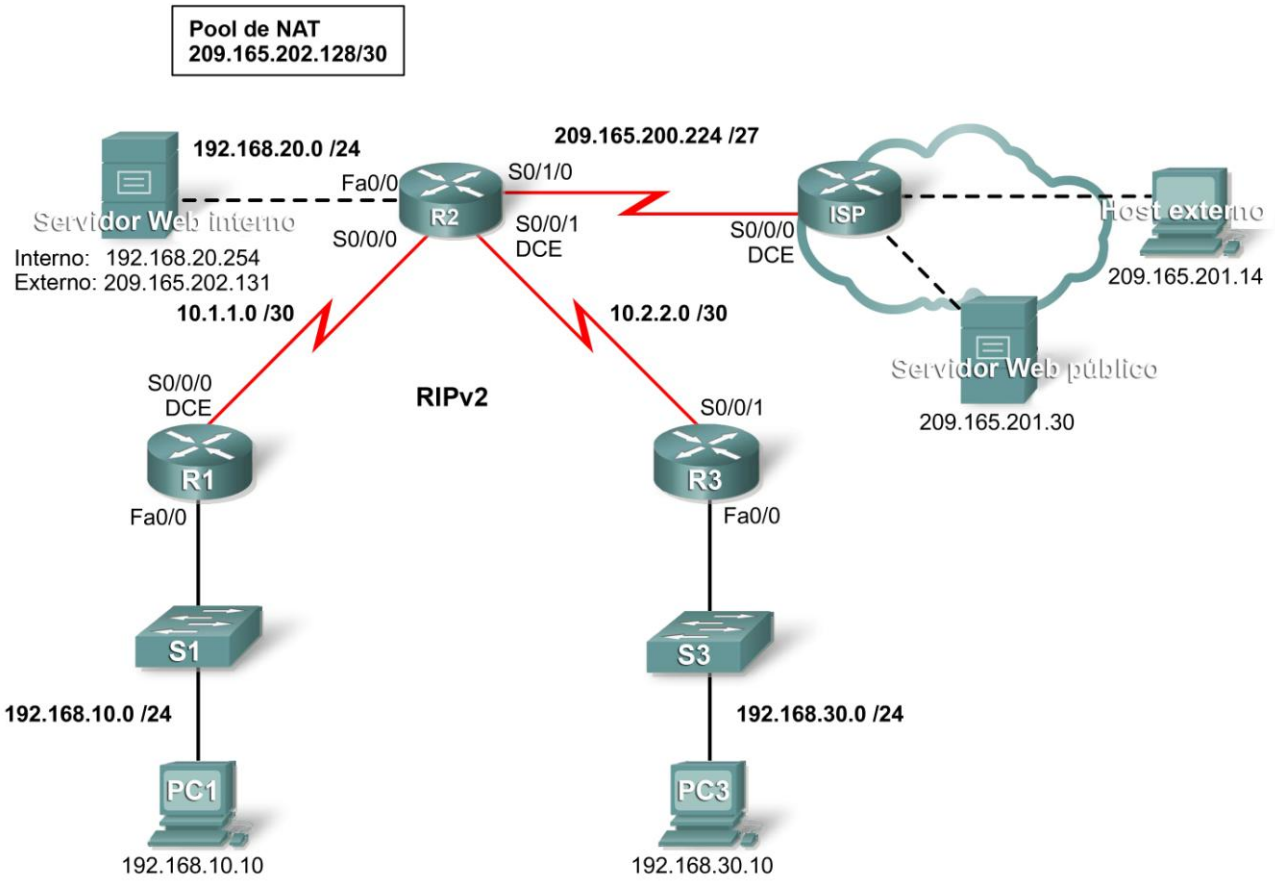


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

La tabla de direccionamiento continúa en la siguiente página.

Tabla de direccionamiento (continuación)

Servidor Web interno	**NIC**	Local: 192.168.20.254	255.255.255.252
	NIC	Global: 209.165.202.131	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
Host externo	**NIC**	209.165.201.14	255.255.255.240
Servidor Web público	**NIC**	209.265.201.30	255.255.255.240

Objetivos de aprendizaje

- Configurar una ACL para permitir NAT
- Configurar NAT estática
- Configurar NAT dinámica con sobrecarga
- Configurar el router ISP con ruta estática
- Probar la conectividad

Introducción

NAT traduce direcciones privadas internas no enrutables en direcciones públicas enrutables. NAT tiene el beneficio adicional de proporcionar a una red cierto grado de privacidad y seguridad, ya que oculta las direcciones IP internas de las redes externas. En esta actividad, se configurará NAT dinámica y estática.

Tarea 1: Configurar una ACL para permitir NAT

Paso 1. Crear una ACL estándar y nombrada.

Para definir las direcciones internas que se traducen a direcciones públicas en el proceso NAT, cree una ACL estándar y nombrada, llamada R2NAT. Esta lista se usa en los siguientes pasos de configuración NAT.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 11%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar NAT estática

Paso 1. Configurar NAT estática para un servidor Web interno.

El servidor Web interno debe tener una dirección IP pública que nunca cambie para que se pueda acceder a él desde afuera de la red. La configuración de una dirección NAT estática permite la configuración del servidor Web con una dirección interna privada. Luego, el proceso NAT asigna paquetes mediante la dirección pública del servidor a la dirección privada.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 22%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar NAT dinámica con sobrecarga

Además de la dirección IP pública asignada a un servidor Web interno, el ISP ha asignado tres direcciones públicas para que las use. Estas direcciones se asignan a todos los demás hosts internos que acceden a Internet.

Para permitir que más de tres hosts internos accedan a Internet al mismo tiempo, configure NAT con sobrecarga para incorporar a los hosts adicionales. NAT con sobrecarga, llamada también Traducción de la dirección del puerto (PAT), utiliza números de puerto para distinguir paquetes de diferentes hosts que se asignan a la misma dirección IP pública.

Paso 1. Definir el conjunto de direcciones y configurar NAT dinámica.

Ingrese los siguientes comandos para configurar el conjunto de direcciones públicas que se asignan en forma dinámica a hosts internos.

El primer comando define el pool de tres direcciones públicas que se asignan a direcciones internas.

El segundo comando indica al proceso NAT que asigna las direcciones en el pool a las direcciones definidas en la lista de acceso que se creó en la Tarea 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask
255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

Paso 2. Configurar las interfaces en R2 para aplicar NAT.

En el modo de configuración de interfaz en R2, configure cada una de las interfaces mediante el comando **ip nat** {**inside** | **outside**}. Debido a que las direcciones internas están en redes conectadas a las interfaces Fa0/0, Serial 0/0/0 y Serial0/0/1, utilice el comando **ip nat inside** al configurar estas interfaces. Internet está conectada a Serial0/1/0; por lo tanto, utilice el comando **ip nat outside** en esta interfaz.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 89%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar ISP con una ruta estática

Paso 1. Configurar ISP con una ruta estática a R2.

ISP necesita una ruta estática hacia las direcciones públicas de R2. Use el siguiente comando para configurar esta ruta.

```
ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Probar la conectividad

Ahora debe poder hacer ping desde cualquier host interno a un host externo o un servidor Web público.

Para comprobar los efectos de NAT en un paquete específico, ingrese al modo Simulación y observe el paquete que se origina en la PC1.

Haga clic en el cuadro de información de color asociado con ese paquete cuando pasa de R1 a R2. Al hacer clic en **Detalles de la PDU entrantes**, se puede observar que la dirección de origen es 192.168.10.10. Al hacer clic en **Detalles de la PDU salientes**, se puede observar que la dirección de origen se tradujo a la dirección 209.165.x.x.

Actividad 7.4.1: Configuración básica de DHCP y NAT

Diagrama de topología

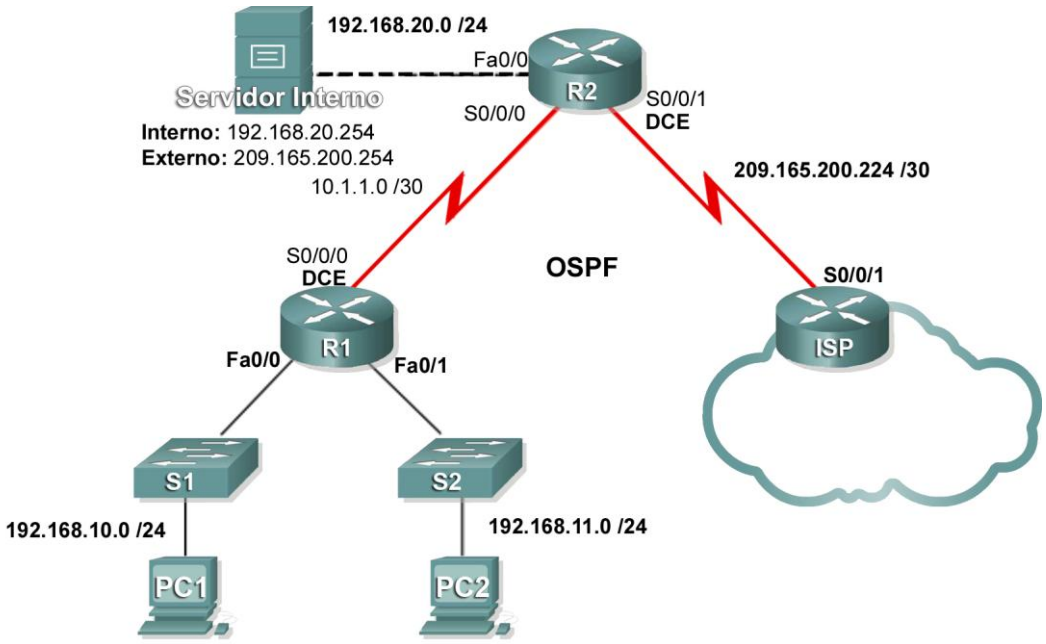


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Preparar la red
- Realizar las configuraciones básicas del router
- Configurar un servidor de DHCP del IOS de Cisco
- Configurar el enrutamiento estático y predeterminado
- Configurar NAT estática

- Configurar NAT dinámica con un conjunto de direcciones
- Configurar NAT con sobrecarga

Escenario

En esta práctica de laboratorio se configurarán los servicios IP de DHCP y NAT. Un router es el servidor de DHCP. El otro router envía solicitudes de DHCP al servidor. Además, realizará configuraciones de NAT estática y dinámica, entre ellas NAT con sobrecarga. Cuando haya completado las configuraciones, verifique la conectividad entre las direcciones internas y externas.

Tarea 1: Realizar las configuraciones básicas del router

Configure los routers R1, R2 e ISP de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del dispositivo.
- Desactive la búsqueda DNS.
- Configure una contraseña de modo EXEC privilegiado.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para todas las conexiones de vty.
- Configure direcciones IP en todos los routers. Las PC reciben direccionamiento IP desde DHCP más adelante en esta actividad.
- Habilite OSPF con el ID de proceso 1 en R1 y R2. No publique la red 209.165.200.224/27.

Tarea 2: Configurar un servidor de DHCP del IOS de Cisco

Paso 1. Excluir las direcciones asignadas en forma estática.

El servidor de DHCP supone que todas las direcciones IP en una subred de conjunto de direcciones DHCP están disponibles para la asignación a los clientes de DHCP. Es necesario especificar las direcciones IP que el servidor de DHCP no debe asignar a los clientes. Estas direcciones IP generalmente son direcciones estáticas reservadas para la interfaz del router, la dirección IP para administración del switch, los servidores y la impresora de red local. El comando **ip dhcp excluded-address** impide que el router asigne direcciones IP dentro del rango configurado. Los siguientes comandos excluyen las primeras 10 direcciones IP de cada pool para las LAN conectadas a R1. Estas direcciones no serán asignadas a ningún cliente de DHCP.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Paso 2. Configurar el pool.

Cree el pool de DHCP mediante el comando **ip dhcp pool** y asígnele el nombre **R1Fa0**.

```
R1(config)#ip dhcp pool R1Fa0
```

Especifique la subred que se usará cuando se asignen las direcciones IP. Los pools de DHCP se asocian automáticamente con una interfaz según la sentencia de red. El router ahora actúa como servidor de DHCP que distribuye direcciones en la subred 192.168.10.0/24, a partir de 192.168.10.1.

```
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure el router predeterminado y el servidor de nombre de dominio para la red. Los clientes reciben estas configuraciones a través de DHCP, junto con una dirección IP.

```
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.10.1
```

Nota: No hay un servidor DNS en 192.168.11.5. Se configura el comando a modo de práctica únicamente.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

Paso 3. Verificar la configuración del DHCP.

Puede verificar la configuración del servidor de DHCP de diversas formas. La manera más básica es configurar un host en la subred para que reciba una dirección IP a través de DHCP. Luego pueden ejecutarse comandos en el router para obtener más información. El comando **show ip dhcp binding** proporciona información sobre todas las direcciones de DHCP asignadas actualmente. Por ejemplo: el siguiente resultado muestra que la dirección IP 192.168.10.11 se asignó a la dirección MAC 3031.632e.3537.6563. El arrendamiento de IP vence el 14 de septiembre de 2007 a las 7:33 p. m.

```
R1#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Dirección de Hardware
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA -- Automatic
```

Tarea 3: Configurar el enrutamiento estático y predeterminado

ISP utiliza enrutamiento estático para llegar a todas las redes más allá de R2. Sin embargo, R2 traduce las direcciones privadas en direcciones públicas antes de enviar el tráfico al ISP. Por lo tanto, ISP debe configurarse con las direcciones públicas que forman parte de la configuración de NAT en R2. Ingrese la siguiente ruta estática en ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Esta ruta estática incluye todas las direcciones asignadas a R2 para uso público.

Configure una ruta predeterminada en R2 y propáguela en OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Espere unos segundos hasta que R1 aprenda la ruta predeterminada desde R2 y luego verifique la tabla de enrutamiento de R1. También puede borrar la tabla de enrutamiento con el comando **clear ip route ***. En la tabla de enrutamiento del R1 debe aparecer una ruta predeterminada que apunte al R2. Desde R1, haga ping a la interfaz serial 0/0/1 en R2 (209.165.200.225). Los pings deben tener éxito. Si los pings fallan, resuelva el problema según corresponda.

Tarea 4: Configurar NAT estática

Paso 1. Asignar una dirección IP pública en forma estática a una dirección IP privada.

Los hosts externos más allá del ISP pueden acceder al servidor interno conectado a R2. Asigne la dirección IP pública 209.165.200.254 en forma estática como la dirección que NAT utilizará para asignar paquetes a la dirección IP privada del servidor interno en 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Paso 2. Especificar las interfaces NAT internas y externas.

Antes de que NAT pueda actuar, debe especificar las interfaces internas y las externas.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Paso 3. Verificar la configuración de NAT estática.

Desde el ISP, haga ping a la dirección IP pública 209.165.200.254.

Tarea 5: Configurar NAT dinámica con un conjunto de direcciones

Mientras que NAT estática proporciona una asignación permanente entre una dirección interna y una dirección pública específica, NAT dinámica asigna direcciones IP privadas a direcciones públicas. Estas direcciones IP públicas provienen de un pool de NAT.

Paso 1. Definir un conjunto de direcciones globales.

Cree un conjunto de direcciones a las que se traducen las direcciones de origen coincidentes. El siguiente comando crea un pool llamado **MY-NAT-POOL** que traduce las direcciones coincidentes a una dirección IP disponible en el rango 209.165.200.241 - 209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Paso 2. Crear una lista de control de acceso estándar para identificar qué direcciones internas se traducen.

```
R2(config)#ip access-list extended NAT
R2(config-std-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-std-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Paso 3. Establecer la traducción dinámica de origen al crear un enlace entre el pool y la lista de control de acceso.

Un router puede tener más de un pool de NAT y más de una ACL. El siguiente comando le indica al router qué conjunto de direcciones debe usar para traducir los hosts que permite la ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Paso 4. Especificar las interfaces NAT internas y externas.

Ya ha especificado las interfaces internas y externas de la configuración de NAT estática. Ahora agregue la interfaz serial conectada a R1 como interfaz interna.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Paso 5. Verificar la configuración.

Desde la PC1 y la PC2, haga ping al ISP. Luego utilice el comando **show ip nat translations** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
---  209.165.200.241   192.168.10.11      ---                ---
---  209.165.200.242   192.168.11.11      ---                ---
---  209.165.200.254   192.168.20.254     ---                ---
```

Tarea 6: Configurar NAT con sobrecarga

En el ejemplo anterior, ¿qué sucedería si necesitara más que las seis direcciones IP públicas que el pool permite?

Al hacer un seguimiento de los números de puerto, NAT con sobrecarga permite a varios usuarios internos volver a usar una dirección IP pública.

En esta tarea se eliminará el pool y la sentencia de asignación configurada en la tarea anterior. Luego se configurará NAT con sobrecarga en R2 de manera tal que todas las direcciones IP internas se traduzcan a la dirección S0/0/1 de R2 al conectarse a cualquier dispositivo externo.

Paso 1. Eliminar el pool de NAT y la sentencia de asignación.

Utilice los siguientes comandos para eliminar el pool de NAT y la asignación a la ACL de NAT.

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

Si recibe el siguiente mensaje, borre las traducciones de NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Paso 2. Configurar PAT en R2 mediante la dirección IP pública de la interfaz serial 0/0/1.

La configuración es similar a NAT dinámica, excepto que en lugar de un conjunto de direcciones se utiliza la palabra clave **interface** para identificar la dirección IP externa. Por lo tanto, no se define ningún pool de NAT. La palabra clave **overload** permite agregar el número de puerto a la traducción.

Debido a que ya se configuró una ACL para identificar qué direcciones IP internas deben traducirse y qué interfaces son internas y externas, sólo se debe configurar lo siguiente:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Paso 3. Verificar la configuración.

Desde la PC1 y la PC2, haga ping al ISP. Luego utilice el comando **show ip nat translations** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.11:3    209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024192.168.11.11:3    209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                ---
```

Nota: En la tarea anterior, se podría haber agregado la palabra clave **overload** al comando **ip nat inside source list NAT pool MY-NAT-POOL** para permitir más de seis usuarios simultáneos.

Tarea 7: Documentar la red

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 1: Preparar la red

Paso 1. Conectar una red que sea similar a la del diagrama de topología.

Puede utilizar cualquier router que actualmente tenga en el laboratorio, siempre y cuando cuente con las interfaces necesarias que se muestran en la topología.

Nota: Si utiliza un router serie 1700, 2500 ó 2600, los resultados y las descripciones de interfaz del router pueden tener un aspecto diferente.

Paso 2. Borrar todas las configuraciones que tengan los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2 e ISP de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del dispositivo.
- Desactive la búsqueda DNS.
- Configure una contraseña de modo EXEC privilegiado.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para todas las conexiones de vty.
- Configure direcciones IP en todos los routers. Las PC reciben direccionamiento IP desde DHCP más adelante en la práctica de laboratorio.
- Habilite OSPF con el ID de proceso 1 en R1 y R2. No publique la red 209.165.200.224/27.

Nota: En lugar de conectar un servidor a R2, se puede configurar una interfaz loopback en R2 para usar la dirección IP 192.168.20.254/24. De este modo, no hace falta configurar la interfaz Fast Ethernet.

Tarea 3: Configurar un servidor de DHCP del IOS de Cisco

El software IOS de Cisco admite una configuración del servidor de DHCP llamada Easy IP. El objetivo de esta práctica de laboratorio es hacer que los dispositivos en las redes 192.168.10.0/24 y 192.168.11.0/24 soliciten direcciones IP a través de DHCP desde R2.

Paso 1. Excluir las direcciones asignadas en forma estática.

El servidor de DHCP supone que todas las direcciones IP en una subred de conjunto de direcciones DHCP están disponibles para la asignación a los clientes de DHCP. Es necesario especificar las direcciones IP que el servidor de DHCP no debe asignar a los clientes. Estas direcciones IP generalmente son direcciones estáticas reservadas para la interfaz del router, la dirección IP para administración del switch, los servidores y la impresora de red local. El comando **ip dhcp excluded-address** impide que el router asigne direcciones IP dentro del rango configurado. Los siguientes comandos excluyen las primeras 10 direcciones IP de cada pool para las LAN conectadas a R1. Estas direcciones no serán asignadas a ningún cliente de DHCP.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Paso 2. Configurar el pool.

Cree el pool de DHCP mediante el comando **ip dhcp pool** y asígnele el nombre **R1Fa0**.

```
R2(config)#ip dhcp pool R1Fa0
```

Especifique la subred que se usará cuando se asignen las direcciones IP. Los pools de DHCP se asocian automáticamente con una interfaz según la sentencia de red. El router ahora actúa como servidor de DHCP que distribuye direcciones en la subred 192.168.10.0/24, a partir de 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure el router predeterminado y el servidor de nombre de dominio para la red. Los clientes reciben estas configuraciones a través de DHCP, junto con una dirección IP.

```
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
```

Nota: No hay un servidor DNS en 192.168.11.5. Se configura el comando a modo de práctica únicamente.

Debido a que los dispositivos de la red 192.168.11.0/24 también solicitan direcciones a R2, debe crearse un pool por separado para atender a los dispositivos en esa red. Los comandos son similares a los que se muestran arriba:

```
R2(config)#ip dhcp pool R1Fa1
R2(dhcp-config)#network 192.168.11.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.11.1
```

Paso 3. Configurar una dirección de ayudante.

Los servicios de red como DHCP dependen de broadcasts de Capa 2 para funcionar. Cuando los dispositivos que proporcionan estos servicios existen en una subred distinta de la de los clientes, no pueden recibir los paquetes de broadcast. Debido a que el servidor de DHCP y los clientes de DHCP no están en la misma subred, configure R1 para que envíe broadcasts de DHCP a R2, que es el servidor de DHCP, mediante el comando de configuración de interfaz **ip helper-address**.

Tenga en cuenta que **ip helper-address** debe configurarse en cada interfaz involucrada.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

Paso 4. Verificar la configuración de DHCP.

Puede verificar la configuración del servidor de DHCP de diversas formas. La manera más básica es configurar un host en la subred para que reciba una dirección IP a través de DHCP. Luego pueden ejecutarse comandos en el router para obtener más información. El comando **show ip dhcp binding** proporciona información sobre todas las direcciones de DHCP asignadas actualmente. Por ejemplo: el siguiente resultado muestra que la dirección IP 192.168.10.11 se asignó a la dirección MAC 3031.632e.3537.6563. El arrendamiento de IP vence el 14 de septiembre de 2007 a las 7:33 p. m.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
                  Hardware address/
                  User name
192.168.10.11     0063.6973.636f.2d30.  Sep 14 2007 07:33 PM    Automatic
                  3031.632e.3537.6563.
                  2e30.3634.302d.566c.
                  31
```

El comando **show ip dhcp pool** muestra información sobre todos los pools de DHCP configurados actualmente en el router. En este resultado, el pool **R1Fa0** está configurado en R1. Se ha arrendado una dirección de este pool. El próximo cliente que solicite una dirección recibirá 192.168.10.12.

```
R2#show ip dhcp pool
Pool R1Fa0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.10.12        192.168.10.1     - 192.168.10.254    1
```

El comando **debug ip dhcp server events** puede resultar muy útil para la resolución de problemas de arrendamientos de DHCP con un servidor de DHCP del IOS de Cisco. A continuación se muestra el resultado de la depuración en R1 después de conectar un host. Observe que la parte resaltada muestra a DHCP otorgando al cliente una dirección de 192.168.10.12 y una máscara de subred de 255.255.255.0.

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072:  DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:   DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076:  DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:   DHCPD: lease time remaining (secs) = 86400
```

Tarea 4: Configurar el enrutamiento estático y predeterminado

ISP utiliza enrutamiento estático para llegar a todas las redes más allá de R2. Sin embargo, R2 traduce las direcciones privadas en direcciones públicas antes de enviar el tráfico al ISP. Por lo tanto, ISP debe

configurarse con las direcciones públicas que forman parte de la configuración de NAT en R2. Ingrese la siguiente ruta estática en ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Esta ruta estática incluye todas las direcciones asignadas a R2 para uso público.

Configure una ruta predeterminada en R2 y propáguela en OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Espere unos segundos hasta que R1 aprenda la ruta predeterminada desde R2 y luego verifique la tabla de enrutamiento de R1. También puede borrar la tabla de enrutamiento con el comando **clear ip route ***. En la tabla de enrutamiento del R1 debería aparecer una ruta predeterminada que apunte al R2. Desde R1, haga ping a la interfaz serial 0/0/1 en R2 (209.165.200.226). Los pings deben tener éxito. Si los pings fallan, resuelva el problema según corresponda.

Tarea 5: Configurar NAT estática

Paso 1. Asignar una dirección IP pública en forma estática a una dirección IP privada.

Los hosts externos más allá del ISP pueden acceder al servidor interno conectado a R2. Asigne la dirección IP pública 209.165.200.254 en forma estática como la dirección que NAT utilizará para asignar paquetes a la dirección IP privada del servidor interno en 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Paso 2. Especificar las interfaces NAT internas y externas.

Antes de que NAT pueda actuar, debe especificar las interfaces internas y las externas.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Nota: Si se usa un servidor interno simulado, asigne el comando **ip nat inside** a la interfaz loopback.

Paso 3. Verificar la configuración de NAT estática.

Desde el ISP, haga ping a la dirección IP pública 209.165.200.254.

Tarea 6: Configurar NAT dinámica con un conjunto de direcciones

Mientras que NAT estática proporciona una asignación permanente entre una dirección interna y una dirección pública específica, NAT dinámica asigna direcciones IP privadas a direcciones públicas. Estas direcciones IP públicas provienen de un pool de NAT.

Paso 1. Definir un conjunto de direcciones globales.

Cree un conjunto de direcciones a las que se traducen las direcciones de origen coincidentes. El siguiente comando crea un pool llamado **MY-NAT-POOL** que traduce las direcciones coincidentes a una dirección IP disponible en el rango 209.165.200.241–209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Paso 2. Crear una lista de control de acceso extendida para identificar qué direcciones internas se traducen.

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Paso 3. Establecer la traducción dinámica de origen al crear un enlace entre el pool y la lista de control de acceso.

Un router puede tener más de un pool de NAT y más de una ACL. El siguiente comando le indica al router qué conjunto de direcciones debe usar para traducir los hosts que permite la ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Paso 4. Especificar las interfaces NAT internas y externas.

Ya ha especificado las interfaces internas y externas de la configuración de NAT estática. Ahora agregue la interfaz serial conectada a R1 como interfaz interna.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Paso 5. Verificar la configuración

Haga ping al ISP desde la PC1 o la interfaz Fast Ethernet en R1 mediante un **ping** extendido. Luego utilice los comandos **show ip nat translations** y **show ip nat statistics** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4     209.165.200.226:4  209.165.200.226:4
--- 209.165.200.241    192.168.10.1       ---                ---
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23  Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
 pool MY-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.241 end 209.165.200.246
        type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

Para resolver problemas con NAT se puede utilizar el comando **debug ip nat**. Active la depuración de NAT y repita el ping desde la PC1.

```
R2#debug ip nat
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
```

```
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

Tarea 7: Configurar NAT con sobrecarga

En el ejemplo anterior, ¿qué sucedería si necesitara más que las seis direcciones IP públicas que el pool permite?

_____

Al hacer un seguimiento de los números de puerto, NAT con sobrecarga permite a varios usuarios internos volver a usar una dirección IP pública.

En esta tarea se eliminará el pool y la sentencia de asignación configurada en la tarea anterior. Luego se configurará NAT con sobrecarga en R2 de manera tal que todas las direcciones IP internas se traduzcan a la dirección S0/0/1 de R2 al conectarse a cualquier dispositivo externo.

Paso 1. Eliminar el pool de NAT y la sentencia de asignación.

Utilice los siguientes comandos para eliminar el pool de NAT y la asignación a la ACL de NAT.

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

Si recibe el siguiente mensaje, borre las traducciones de NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Paso 2. Configurar PAT en R2 mediante la dirección IP pública de la interfaz serial 0/0/1.

La configuración es similar a NAT dinámica, excepto que en lugar de un conjunto de direcciones, se utiliza la palabra clave **interface** para identificar la dirección IP externa. Por lo tanto, no se define ningún pool de NAT. La palabra clave **overload** permite agregar el número de puerto a la traducción.

Debido a que ya se configuró una ACL para identificar qué direcciones IP internas deben traducirse y qué interfaces son internas y externas, sólo se debe configurar lo siguiente:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Paso 3. Verificar la configuración

Haga ping al ISP desde la PC1 o la interfaz Fast Ethernet en R1 mediante un **ping** extendido. Luego utilice los comandos **show ip nat translations** y **show ip nat statistics** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6    209.165.200.226:6  209.165.200.226:6
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
```

```
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48  Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

Nota: En la tarea anterior, se podría haber agregado la palabra clave **overload** al comando **ip nat inside source list NAT pool MY-NAT-POOL** para permitir más de seis usuarios simultáneos.

Tarea 8: Documentar la red

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 9: Limpieza

Borre las configuraciones y vuelva a cargar los routers. Desconecte y guarde el cableado. Para las PC host que normalmente están conectadas a otras redes, como la LAN de la escuela o de Internet, vuelva a conectar los cables correspondientes y restaure las configuraciones TCP/IP.

Actividad 7.4.2: Desafío de configuración de DHCP y NAT

Diagrama de topología

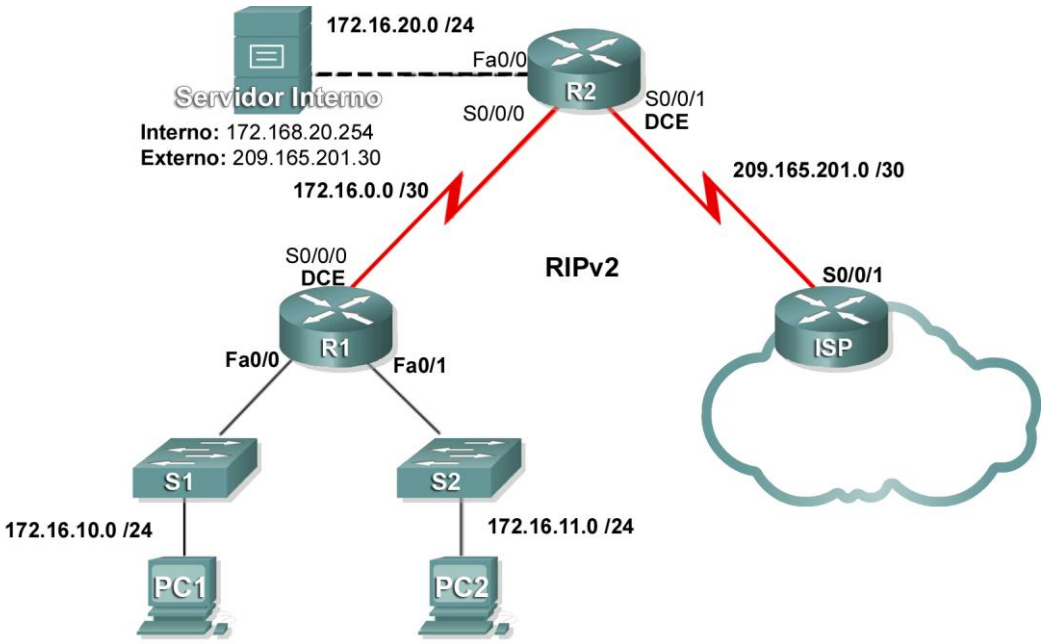


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	**S0/0/0**	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.201.2	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Preparar la red
- Realizar las configuraciones básicas del router
- Configurar un servidor de DHCP del IOS de Cisco
- Configurar el enrutamiento estático y predeterminado

- Configurar NAT estática
- Configurar NAT dinámica con un conjunto de direcciones
- Configurar NAT con sobrecarga

Escenario

En esta práctica de laboratorio, configure los servicios de dirección IP a través de la red que se muestra en el diagrama de topología. Si necesita ayuda, vuelva a consultar la práctica de laboratorio de configuración básica de DHCP y NAT. Sin embargo, intente hacer todo lo posible por su cuenta.

Tarea 1: Realizar las configuraciones básicas del router

Configure los routers R1, R2 e ISP de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del dispositivo.
- Desactive la búsqueda DNS.
- Configure una contraseña de modo EXEC privilegiado.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para todas las conexiones de vty.
- Configure direcciones IP en todos los routers. Las PC reciben direccionamiento IP desde DHCP más adelante en la práctica de laboratorio.
- Habilite RIPv2 en R1 y R2. No publique la red 209.165.200.224/27.

Tarea 2: Configurar un servidor de DHCP del IOS de Cisco

Configure R1 como servidor de DHCP para las dos LAN directamente conectadas.

Paso 1. Excluir las direcciones asignadas en forma estática.

Excluya las primeras tres direcciones de cada pool.

Paso 2. Configurar el pool de DHCP.

- Cree dos pools de DHCP. A uno de ellos asígnele el nombre **R1_LAN10** para la red 172.16.10.0/24, al otro denomínelo **R1_LAN11** para la red 172.16.11.0/24.
- Configure cada pool con una gateway predeterminada y un DNS simulado en 172.16.20.254.

Paso 3. Verificar la configuración de DHCP.

Tarea 3: Configurar el enrutamiento estático y predeterminado

- Configure ISP con una ruta estática para la red 209.165.201.0/27. Utilice la interfaz de salida como argumento.
- Configure una ruta predeterminada en R2 y propáguela en OSPF. Utilice la dirección IP del siguiente salto como argumento.

Tarea 4: Configurar NAT estática

Paso 1. Asignar una dirección IP pública en forma estática a una dirección IP privada.

Asigne en forma estática la dirección IP del servidor interno a la dirección pública 209.165.201.30.

Paso 2. Especificar las interfaces NAT internas y externas.

Paso 3. Verificar la configuración de NAT estática.

Tarea 5: Configurar NAT dinámica con un conjunto de direcciones

Paso 1. Definir un conjunto de direcciones globales.

Cree un pool llamado **NAT_POOL** para las direcciones IP de 209.165.201.9 a 209.165.201.14 mediante una máscara de subred /29.

Paso 2. Crear una lista de control de acceso estándar para identificar qué direcciones internas se traducen.

Utilice el nombre **NAT_ACL** y permita a todos los hosts conectados a las dos LAN en R1.

Nota: La LAN **.10** debe configurarse primero, luego la LAN **.11**. De lo contrario, Packet Tracer no calificará a la ACL como correcta.

Paso 3. Establecer la traducción dinámica de origen.

Vincule el pool de NAT con la ACL y permita NAT con sobrecarga.

Paso 4. Especificar las interfaces NAT internas y externas.

Verifique que todas las interfaces internas y externas se especifiquen correctamente.

Paso 5. Verificar la configuración de NAT dinámica haciendo ping de la PC1 y la PC2 al ISP.

Tarea 6: Documentar la red

En cada router, ejecute el comando **show run** y capture las configuraciones.

Actividad de PT 7.4.3: Resolución de problemas de DHCP y NAT

Diagrama de topología

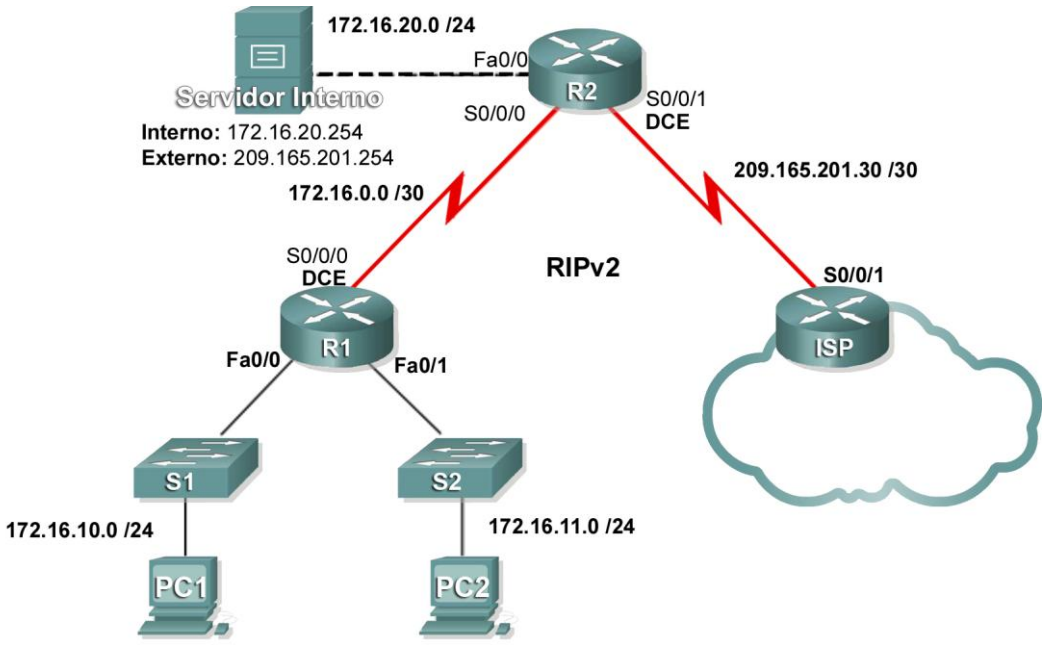


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	**S0/0/0**	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.201.2	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio podrá:

- Detectar y corregir errores de red
- Documentar la red corregida

Escenario

Un ingeniero de redes inexperto configuró los routers de su empresa. Diversos errores en la configuración produjeron problemas de conectividad. Su jefe le pidió que resuelva y corrija los errores de configuración y que documente su trabajo. Detecte y corrija los errores utilizando sus conocimientos del DHCP, la NAT y los métodos estándar de evaluación. Asegúrese de que todos los clientes tengan conectividad total.

Tarea 1: Detectar y corregir errores de red

Utilice los comandos de resolución de problemas para detectar los errores y luego corregirlos. Una vez que se hayan corregido todos los errores, debe poder hacer ping desde PC1 y PC2 hasta el ISP. El ISP debe poder hacer ping al servidor Web interno en su dirección IP pública.

Tarea 2: Documentar la red corregida

En cada router, ejecute el comando **show run** y capture las configuraciones.

Actividad de PT 7.5.1: Desafío de integración de aptitudes del Packet Tracer

Diagrama de topología

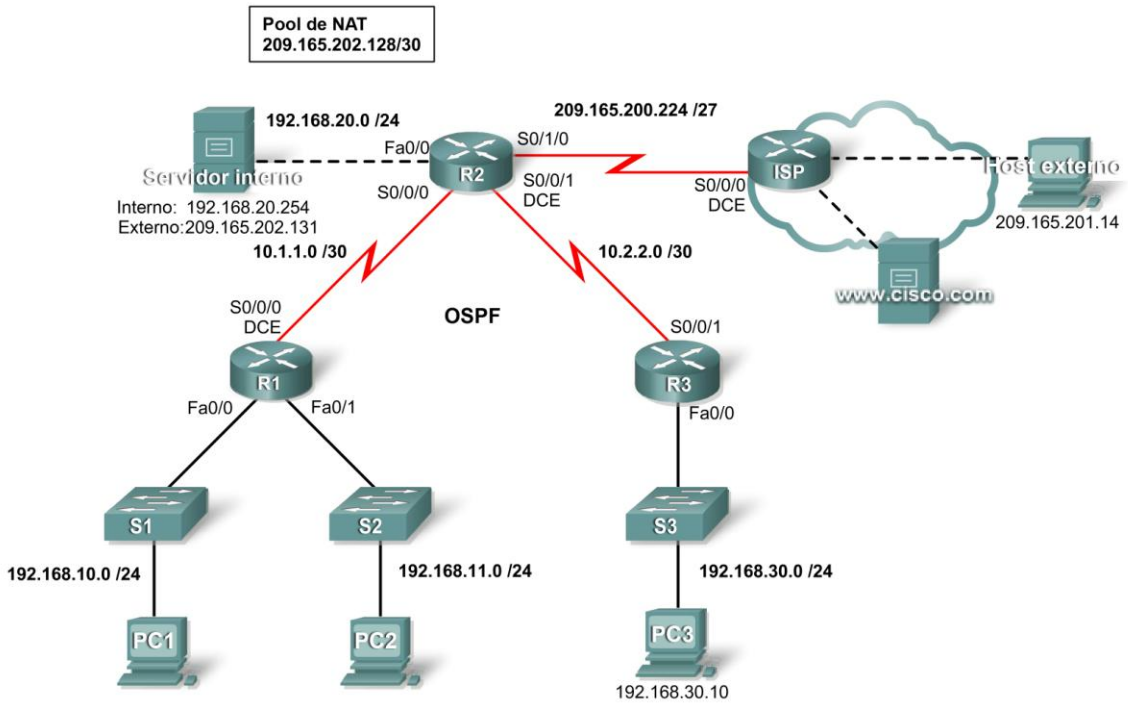


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**Fa0/0**	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
Servidor interno	**NIC**	Local: 192.168.20.254	255.255.255.0
	NIC	Global: 209.165.202.131	255.255.255.252
Host externo	**NIC**	209.165.201.14	255.255.255.240

Objetivos de aprendizaje

- Aplicar las configuraciones básicas
- Configurar la encapsulación PPP con CHAP
- Configurar el enrutamiento dinámico y predeterminado
- Configurar los routers con Easy IP
- Verificar que las PC se configuren automáticamente con detalles de direccionamiento
- Configurar un servidor DNS con entradas DNS
- Configurar una ACL para permitir NAT
- Configurar NAT estática
- Configurar NAT dinámica con sobrecarga
- Configurar el router ISP con una ruta estática
- Probar la conectividad

Introducción

En esta actividad final, configurará PPP, OSPF, DHCP, NAT y el enrutamiento predeterminado a ISP. Luego verificará su configuración.

Tarea 1: Aplicar las configuraciones básicas

Paso 1. Configurar R1, R2 y R3 con la configuración global básica.

- Nombre de host como se indica en la tabla de direccionamiento
- Línea de consola para iniciar sesión con la contraseña **cisco**
- Vtys de 0 a 4 para iniciar sesión con la contraseña **cisco**
- Constraseña secreta **class**
- Mensaje de “SÓLO ACCESO AUTORIZADO”

Sólo se clasifican el nombre de host y el mensaje.

Paso 2. Configurar las interfaces de R1, R2 y R3.

Utilice la tabla de direccionamiento para determinar las direcciones de la interfaz. Use el diagrama de topología para determinar qué interfaces son interfaces DCE. Configure las interfaces DCE para una frecuencia de reloj de 64 000.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 38%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 2: Configurar la encapsulación PPP con CHAP

Paso 1. Configurar el enlace entre R1 y R2 para utilizar la encapsulación PPP con autenticación CHAP.

La contraseña para la autenticación CHAP es **cisco123**.

Paso 2. Configurar el enlace entre R2 y R3 para utilizar la encapsulación PPP con autenticación CHAP.

La contraseña para la autenticación CHAP es **cisco123**.

Paso 3. Verificar que se haya restablecido la conectividad entre los routers.

R2 debe poder hacer ping a R1 y R3. Es posible que las interfaces demoren unos minutos en volver a activarse. Puede alternar entre los modos Tiempo real y Simulación para acelerar el proceso. Otra solución alterna posible para esta respuesta del Packet Tracer consiste en utilizar los comandos **shutdown** y **no shutdown** en las interfaces.

Nota: Es posible que las interfaces dejen de funcionar en momentos esporádicos durante la actividad debido a un defecto del Packet Tracer. Si espera unos segundos, normalmente la interfaz vuelve a funcionar automáticamente.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 51%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 3: Configurar el enrutamiento dinámico y predeterminado

Paso 1. Configurar R1, R2 y R3 para utilizar el protocolo de enrutamiento OSPF.

- Utilice un ID de proceso de 1 al configurar OSPF en los routers.
- Publique todas las redes conectadas a R1 y R3, pero no envíe actualizaciones de enrutamiento desde las interfaces de la LAN.
- En R2, no publique la red 209.165.200.224 ni envíe actualizaciones de enrutamiento desde las interfaces Fa0/0 o serial0/1/0.

Paso 2. Configurar una ruta predeterminada en R2.

Configure una ruta predeterminada al ISP y especifique la interfaz de salida en R2 como dirección del siguiente salto.

Paso 3. Configurar OSPF para publicar la ruta predeterminada.

En R2, ingrese el comando para publicar la ruta predeterminada a R1 y R3 a través de OSPF.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 66%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 4: Configurar los routers con Easy IP

Paso 1. Configurar R1 para que funcione como servidor de DHCP para las redes 192.168.10.0 y 192.68.11.0.

- Asigne el nombre **R1LAN1** al pool de DHCP para la red 192.168.10.0. Para la red 192.168.11.0, utilice el nombre **R1LAN2**.
- Excluya las primeras nueve direcciones de cada red para asignaciones dinámicas.
- Además de la dirección IP y la máscara de subred, asigne las direcciones del servidor DNS y la gateway predeterminada.

Paso 2. Configurar R3 para que funcione como servidor de DHCP para la red 192.168.30.0.

- Asigne el nombre **R3LAN** al pool de DHCP para la red 192.168.30.0.
- Excluya las primeras nueve direcciones de cada red para asignaciones dinámicas.
- Además de la dirección IP y la máscara de subred, asigne las direcciones del servidor DNS y la gateway predeterminada.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 75%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 5: Verificar que las PC se configuren automáticamente con detalles de direccionamiento

Paso 1. Configurar PC1, PC2 y PC3 para una configuración IP automática mediante DHCP.

Paso 2. Verificar que a cada PC se le asigne una dirección del pool de DHCP correcto.

Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 88%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 6: Configurar un servidor DNS con entradas DNS

Paso 1. Configurar el servidor DNS.

Para configurar DNS en el servidor interno, haga clic en el botón **DNS** en la ficha **Configuración**.

Asegúrese de que DNS esté encendido e ingrese la siguiente entrada de DNS:

- www.cisco.com 209.165.201.30

Paso 2. Verificar los resultados.

No podrá hacer ping al servidor **www**.**cisco**.**com** por nombre de dominio hasta que configure la ruta estática en la Tarea 10. Su porcentaje de finalización debe ser del 90%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 7: Configurar una ACL para permitir NAT

Paso 1. Crear una ACL estándar y nombrada.

Cree la ACL nombrada y estándar, **R2NAT**, que permita que la NAT asigne todas las redes internas.

Nota: Para que Packet Tracer clasifique esta tarea correctamente, debe ingresar las redes permitidas en el siguiente orden:

- 192.168.10.0
- 192.168.20.0
- 192.168.30.0
- 192.168.11.0

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 91%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 8: Configurar NAT estática

Paso 1. Configurar NAT estática para un servidor Web interno.

Configure una NAT estática para asignar la dirección IP local y las direcciones IP globales para el servidor interno. Utilice las direcciones indicadas en la tabla de direccionamiento.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 92%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 9: Configurar NAT dinámica con sobrecarga

Paso 1. Configurar el pool de NAT dinámica.

Configure un conjunto de direcciones de NAT dinámicas mediante el pool de NAT especificado en el diagrama de topología. Asigne el nombre **R2POOL** al conjunto de direcciones.

Paso 2. Configurar la asignación de NAT dinámica.

Asigne las direcciones en R2POOL a las redes definidas anteriormente en R2NAT.

Paso 3. Aplicar NAT a las interfaces interna y externa de R2.

Paso 4. Verificar los resultados.

Su porcentaje de finalización debe ser del 99%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 10: Configurar el router ISP con una ruta estática

Paso 1. Configurar una ruta estática a las direcciones IP globales de R2.

Ésta es la red 209.165.202.128/27. Use la interfaz serial de ISP como dirección del siguiente salto.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

Tarea 11: Probar la conectividad

- Los hosts internos deben poder hacer ping al host externo.
- Los hosts internos deben poder hacer ping a www.cisco.com.
- El host externo debe poder hacer ping al servidor interno mediante su dirección IP global.

Actividad de PT 8.1.2: Descubrimiento y documentación de la red

Diagrama de topología

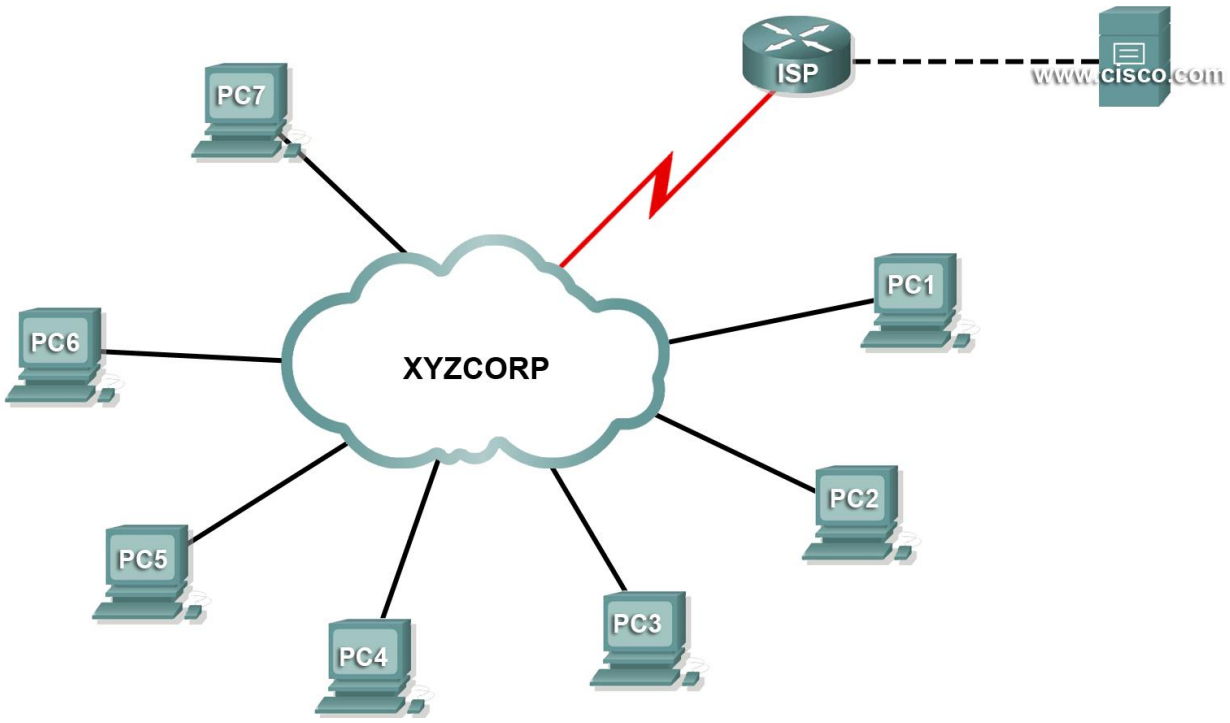


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
PC1	**NIC**			
PC2	**NIC**			
PC3	**NIC**			
PC4	**NIC**			
PC5	**NIC**			
PC6	**NIC**			
PC7	**NIC**			

Objetivos de aprendizaje

- Probar la conectividad
- Descubrir información de configuración de la PC
- Descubrir información de configuración de la gateway predeterminada
- Descubrir rutas y vecinos en la red
- Trazar la topología de la red

Introducción

Esta actividad cubre los pasos que se deben seguir para descubrir una red principalmente mediante los comandos **telnet**, **show cdp neighbors detail** y **show ip route**. Ésta es la Parte I de una actividad de dos partes.

La topología que ve al abrir la actividad del Packet Tracer no revela todos los detalles de la red. Los detalles se han escondido con la función clúster del Packet Tracer. La infraestructura de la red ha colapsado y la topología del archivo sólo muestra los dispositivos finales. Su tarea consiste en utilizar sus conocimientos de redes y comandos de descubrimiento para aprender acerca de la topología de toda la red y documentarla.

Tarea 1: Probar la conectividad

Paso 1. Converger y probar la red.

Packet Tracer necesita cierta ayuda para converger la red. Haga ping entre las PC y entre la PC y el servidor www.cisco.com para acelerar la convergencia y probar la red. Todas las PC deben poder hacer ping entre ellas y con el servidor. Recuerde que quizá sea necesario hacer varios pings para que tengan éxito.

Tarea 2: Descubrir información de configuración de la PC

Paso 1. Acceder a la petición de entrada de comandos de la PC1.

Haga clic en **PC1**, en la ficha **Escritorio** y luego en **Indicador de comandos**.

Paso 2. Determinar la información de direccionamiento de la PC1.

Para determinar la configuración de direccionamiento IP actual, ingrese el comando **ipconfig /all**.

Nota: En Packet Tracer, debe ingresar un espacio entre **ipconfig** y **/all**.

Paso 3. Documentar la información de la PC1 en la tabla de direccionamiento.

Paso 4. Repitir para las otras PC.

Repita los pasos del 1 al 3 para las PC 2 a 7.

Tarea 3: Descubrir información de configuración de la gateway predeterminada

Paso 1. Probar la conectividad entre la PC1 y su gateway predeterminada.

Desde la PC1, haga ping a la gateway predeterminada para cerciorarse de que tiene conectividad.

Paso 2. Hacer telnet a la gateway predeterminada.

Utilice el comando **telnet** *ip-address*. La dirección IP es la de la gateway predeterminada. Cuando se le pida la contraseña, escriba **cisco**.

Paso 3. Observar las configuraciones actuales de la interfaz.

Utilice los comandos **show ip interface brief** y **show protocols** para determinar las configuraciones actuales de la interfaz.

¿Cuál es la diferencia entre estos dos comandos?

_____

Paso 4. Documentar la configuración de la interfaz y el nombre de host en la tabla de direccionamiento.

Utilice el siguiente espacio para realizar un boceto a grandes rasgos de la topología.

Boceto de la topología

Tarea 4: Descubrir rutas y vecinos en la red

Paso 1. En el mismo router, mostrar la tabla de enrutamiento.

Muestre la tabla de enrutamiento con el comando **show ip route**. Debe observar cinco rutas conectadas y seis rutas aprendidas a través de RIP, una de las cuales es una ruta predeterminada.

Además de las rutas, ¿qué otra información útil brinda la tabla de enrutamiento para ayudarlo a seguir descubriendo y documentando la red?

_____

Paso 2. Descubrir dispositivos Cisco directamente conectados.

En el mismo router, use el comando **show cdp neighbors detail** para descubrir otros dispositivos Cisco directamente conectados.

Paso 3. Documentar la información de los vecinos y probar la conectividad.

El comando **show cdp neighbors detail** enumera información de un vecino, incluida su dirección IP. Documente el nombre de host y la dirección IP del vecino. Luego haga ping a la dirección IP para probar la conectividad. Los primeros dos o tres pings fallan mientras el ARP resuelve la dirección MAC.

Paso 4. Hacer telnet al vecino y descubrir dispositivos Cisco directamente conectados.

Haga telnet al vecino y use el comando **show cdp neighbors detail** para descubrir otros dispositivos Cisco directamente conectados.

Esta vez debe ver tres dispositivos en la lista. ¿Por qué el router aparece más de una vez?

_____

Paso 5. Documentar los nombres de host y las direcciones IP de los vecinos, y probar la conectividad.

Documente y haga ping a los nuevos vecinos que haya descubierto. Recuerde: los primeros dos o tres pings fallan mientras el ARP resuelve las direcciones MAC.

Paso 6. Hacer telnet a cada vecino y verificar otros dispositivos Cisco.

Haga telnet a cada uno de los vecinos que haya descubierto y use el comando **show cdp neighbors detail** para buscar otros dispositivos Cisco. La contraseña de acceso es **cisco**.

Paso 7. Continuar con el descubrimiento y la documentación de la red.

Salga de las sesiones telnet para regresar al router de la gateway predeterminada de la PC1. Desde este router, haga telnet a los otros routers de la red para continuar descubriendo y documentando la red. Recuerde utilizar los comandos **show ip route** y **show ip cdp neighbors** para descubrir direcciones IP que puede utilizar para telnet.

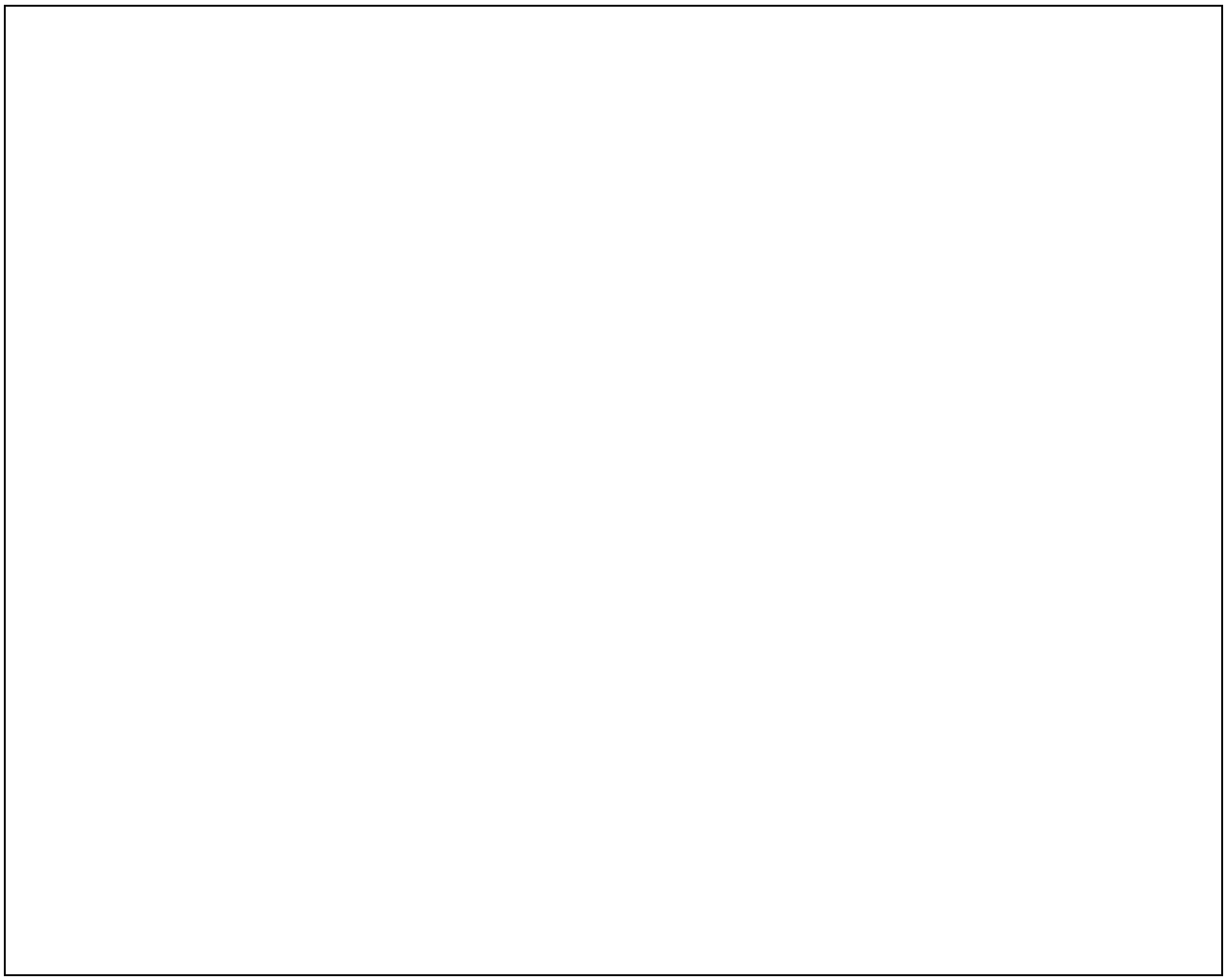
Tarea 5: Trazar la topología de la red

Paso 1. Trazar la topología.

Ahora que ha descubierto todos los dispositivos de la red y documentado sus direcciones, use la tabla de direccionamiento y su boceto de la topología para trazar una versión final de la topología.

Ayuda: Hay una nube Frame Relay en el medio de la red.

Diagrama final de la topología

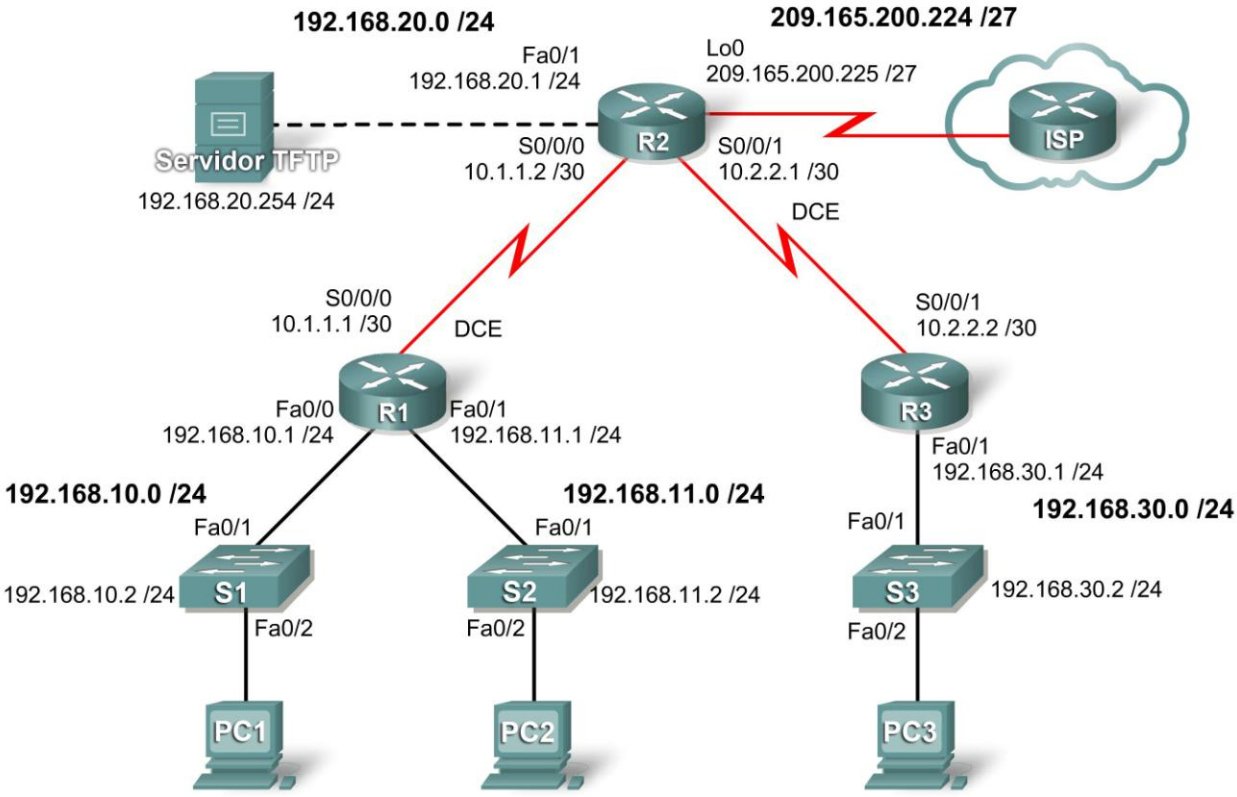


Paso 2. Guardar esta documentación.

Necesitará su diagrama de topología y tabla de enrutamiento para la siguiente actividad 8.4.6: Resolución de problemas de red.

Actividad 8.3.7: Dramatización de resolución de problemas

Diagrama de topología



Objetivos de aprendizaje

- Crear una red
- Probar una red
- Dividir una red
- Resolver un problema
- Reunir información acerca de los síntomas
- Corregir el problema
- Documentar el problema y la solución

Escenario

En esta actividad, usted y otro estudiante crearán la red que se muestra en el diagrama de topología. Configurarán NAT, DHCP y OSPF, y luego verificarán la conectividad. Cuando la red funcione completamente, un estudiante introducirá diversos errores. Luego, el otro estudiante utilizará las habilidades de resolución de problemas para aislar y solucionar el problema. A continuación, los estudiantes intercambiarán los roles y repetirán el proceso. Esta actividad puede realizarse con equipos reales o con Packet Tracer.

Tarea 1: Crear la red

Paso 1: Cablear y configurar los dispositivos de acuerdo con el diagrama de topología.

Paso 2: Configurar NAT, DHCP y OSPF.

Tarea 2: Probar la red

Paso 1: Asegurarse de que haya conectividad de extremo a extremo.

Paso 2: Verificar que el DHCP y la NAT funcionen correctamente.

Paso 3: Familiarizarse con cada uno de los dispositivos mediante los comandos show y debug.

Tarea 3: Dividir la red

Un estudiante se retira del aula, si fuera necesario, mientras el otro estudiante divide la configuración. La división debe ser sólo un problema. La idea es que se ayuden mutuamente a desarrollar las habilidades de resolución de problemas. La creación de múltiples problemas magnifica el alcance del trabajo, que no es el objetivo de la práctica de laboratorio. El objetivo es ayudarlos a que conozcan los diversos cambios que pueden producirse en la red a partir de sólo un problema.

Tarea 4: Resolver el problema

El estudiante regresa y le pregunta al otro estudiante acerca de los síntomas del problema. Comience con preguntas generales y trate de limitar el alcance del problema. Cuando el estudiante a quien se le hacen las preguntas considera que brindó información suficiente, pueden dejar de hacerse preguntas.

Tarea 5: Reunir la información acerca de los síntomas de los dispositivos que probablemente tienen problemas

Comience a reunir información acerca de los síntomas mediante diversos comandos **show** y **debug**. Utilice el comando **show running-config** sólo como última opción.

Tarea 6: Corregir el problema

Corrija la configuración y pruebe la solución.

Tarea 7: Documentar el problema y la solución

Ambos estudiantes deben registrar el problema en sus diarios y documentar la solución.

Tarea 8: Intercambiar roles y repetir el proceso.

Ahora los estudiantes deben intercambiar roles y repetir todo el proceso.

Tarea 9: Limpieza

Borre las configuraciones y vuelva a cargar los routers. Desconecte y guarde el cableado. Para las PC host que normalmente están conectadas a otras redes, como la LAN de la escuela o de Internet, vuelva a conectar los cables correspondientes y restaure las configuraciones TCP/IP.

Actividad de PT 8.4.6: Resolución de problemas de la red

Objetivos de aprendizaje

- Reunir documentación de la red
- Probar la conectividad
- Reunir datos e implementar soluciones
- Probar la conectividad

Introducción

En esta actividad, resolverá problemas de conectividad entre las PC que se enrutan a través de XYZCORP. La actividad se completa cuando logra un 100% y todas las PC pueden hacer ping entre ellas y con el servidor www.cisco.com. Cualquier solución que implemente debe ajustarse al diagrama de topología.

Tarea 1: Reunir documentación de la red

Para llevar a cabo satisfactoriamente esta actividad, necesita la documentación final de la actividad PT del 8.1.2: Descubrimiento y documentación de la red, que completó previamente en este capítulo. Esta documentación debe incluir una tabla de direccionamiento y un diagrama de topología precisos. Si no cuenta con esta documentación, pídale al instructor versiones precisas.

Tarea 2: Probar la conectividad

Al final de esta actividad, debe haber conectividad completa entre todas las PC y entre las PC y el servidor www.cisco.com. Para comenzar a resolver problemas de conectividad, haga ping a lo siguiente:

- de las PC al servidor www.cisco.com
- de PC a PC
- de las PC a la gateway predeterminada

¿Tuvo éxito alguno de los pings? ¿Cuál falló?

_____

_____

_____

_____

_____

Tarea 3: Reunir datos e implementar soluciones

Paso 1. Elegir una PC para comenzar a reunir datos.

Elija cualquier PC y comience a reunir datos. Para ello, pruebe la conectividad a la gateway predeterminada. También puede utilizar **traceroute** para ver dónde falla la conectividad.

Paso 2. Hacer telnet a la gateway predeterminada y continuar reuniendo datos.

Si la PC que eligió no tiene conectividad a la gateway predeterminada, elija otra PC para abordar el problema desde una dirección diferente.

Cuando establezca conectividad a través de una gateway predeterminada, la contraseña de inicio de sesión es **cisco**.

Paso 3. Usar las herramientas de resolución de problemas para verificar la configuración.

En el router de la gateway predeterminada, use las herramientas de resolución de problemas para verificar la configuración con su propia documentación. Recuerde verificar los switches además de los routers. No se olvide de verificar la siguiente información:

- información de direccionamiento
- activación de la interfaz
- encapsulación
- enrutamiento
- configuración de la VLAN
- desajustes de velocidad o dúplex
- operación del VTP

A medida que descubra síntomas del problema de conectividad de la PC, documéntelos en el espacio que aparece en el próximo paso.

Paso 4. Documentar los síntomas de la red y las posibles soluciones.

Paso 5. Hacer cambios en función de las soluciones del paso anterior.

Tarea 4: Probar la conectividad

Paso 1. Probar la conectividad de la PC.

Ahora todas las PC deben poder hacer ping entre sí y al servidor www.cisco.com. Si cambió alguna configuración IP, cree nuevos pings ya que los anteriores usan la dirección IP anterior.

Si todavía hay problemas de conectividad entre las PC o de una PC al servidor, regrese a la Tarea 3 y continúe con la resolución de problemas.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De no ser así, regrese a la Tarea 3 y continúe resolviendo problemas e implementando las soluciones que sugirió. No podrá hacer clic en **Verificar resultados** ni ver qué componentes necesarios todavía no se completaron.

Actividad de PT 8.5.1: Resolución de problemas de redes empresariales 1

Diagrama de topología

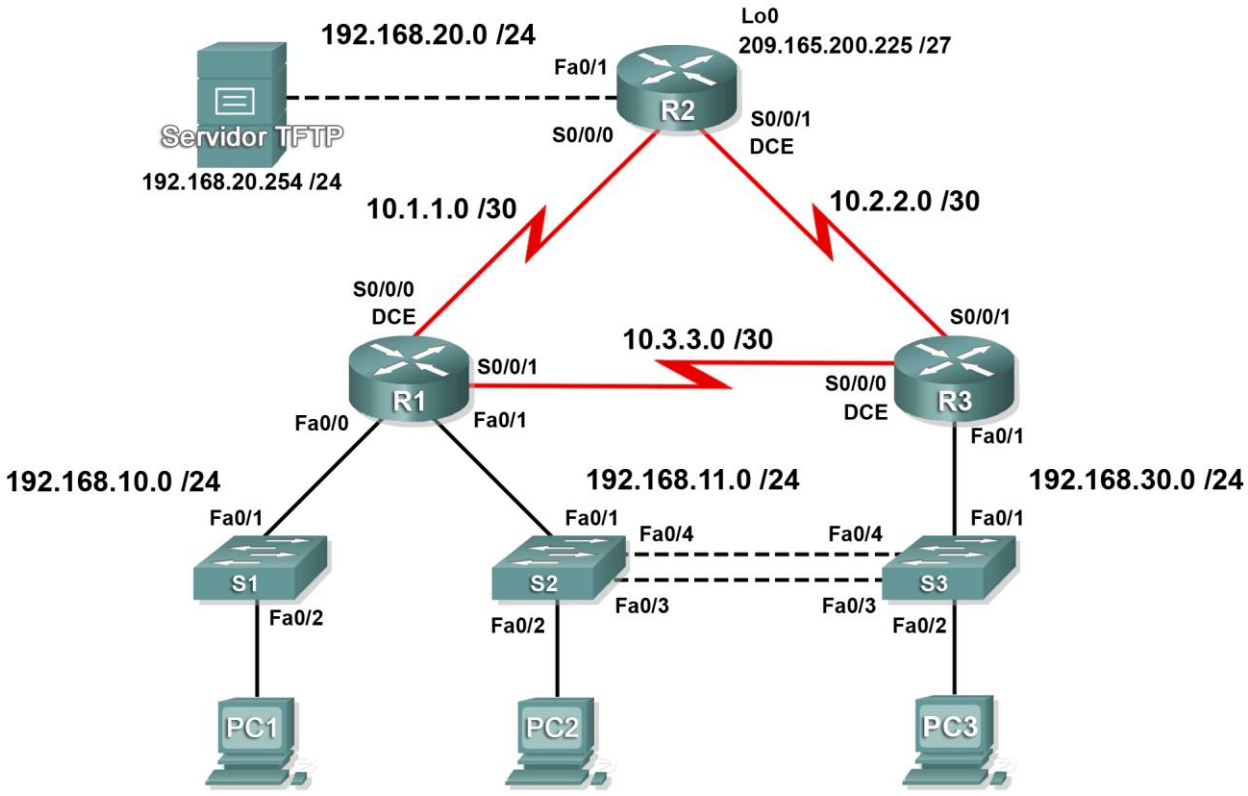


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/0**	192.168.10.1	255.255.255.0	No aplicable
	Fa0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
	S0/0/1	10.3.3.1	255.255.255.252	No aplicable
R2	**Fa0/1**	192.168.20.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

La tabla de direccionamiento continúa en la siguiente página

Tabla de direccionamiento (continuación)

R3	**Fa0/1**	No aplicable	No aplicable	No aplicable
	Fa0/1.11	192.168.11.3	255.255.255.0	No aplicable
	Fa0/1.30	192.168.30.1	255.255.255.0	No aplicable
	S0/0/0	10.3.3.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
S1	**VLAN10**	DHCP	255.255.255.0	No aplicable
S2	**VLAN11**	192.168.11.2	255.255.255.0	No aplicable
S3	**VLAN30**	192.168.30.2	255.255.255.0	No aplicable
PC1	**NIC**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

- Detectar y corregir todos los errores de red
- Verificar que se cumpla totalmente con los requisitos
- Documentar la red corregida

Escenario

Se le pidió que corrija errores de configuración en la red de la empresa. Para esta actividad, no utilice protección de contraseña o inicio de sesión en ninguna línea de consola para evitar el bloqueo accidental. Use **ciscoccna** para todas las contraseñas de esta situación.

Nota: Dado que esta actividad es acumulativa, deberá utilizar todos los conocimientos y las técnicas de resolución de problemas que ha adquirido con el material anterior para completar con éxito esta actividad.

Requisitos

- S2 es la raíz del spanning tree para VLAN 11 y S3 es la raíz del spanning tree para VLAN 30.
- S3 es un servidor VTP con S2 como cliente.
- El enlace serial entre R1 y R2 es Frame Relay.
- El enlace serial entre R2 y R3 usa encapsulación HDLC.
- El enlace serial entre R1 y R3 usa PPP.
- El enlace serial entre R1 y R3 es autenticado por medio de CHAP.
- R2 debe tener procedimientos seguros de inicio de sesión, ya que es el router extremo de Internet.
- Todas las líneas vty, excepto las que pertenecen a R2, permiten conexiones sólo desde las subredes que se muestran en el diagrama de topología, sin incluir la dirección pública.
- Se debe evitar la suplantación de identidad de la dirección IP de origen en todos los enlaces que no se conectan al resto de los routers.
- R3 no debe poder hacer telnet a R2 a través del enlace serial conectado en forma directa.
- R3 tiene acceso a VLAN 11 y 30 a través de su puerto 0/0 Fast Ethernet.

- El servidor TFTP no debe recibir ningún tipo de tráfico que tenga una dirección de origen fuera de la subred. Todos los dispositivos tienen acceso al servidor TFTP.
- Todos los dispositivos de la subred 192.168.10.0 deben poder obtener sus direcciones IP del DHCP en R1.
- Se debe poder acceder a todas las direcciones que se muestran en el diagrama desde cada dispositivo.

Tarea 1: Detectar y corregir todos los errores de red

Tarea 2: Verificar que se cumpla totalmente con los requisitos

Debido a que las limitaciones de tiempo impiden resolver un problema sobre cada tema, sólo una cantidad selecta de temas tiene problemas. Sin embargo, para reforzar y fortalecer sus capacidades de resolución de problemas, debe verificar que se cumpla con cada uno de los requisitos. Para hacerlo, presente un ejemplo de cada requisito (por ejemplo, un comando **show** o **debug**).

Tarea 3: Documentar la red corregida

Actividad de PT 8.5.2: Resolución de problemas de redes empresariales 2

Diagrama de topología

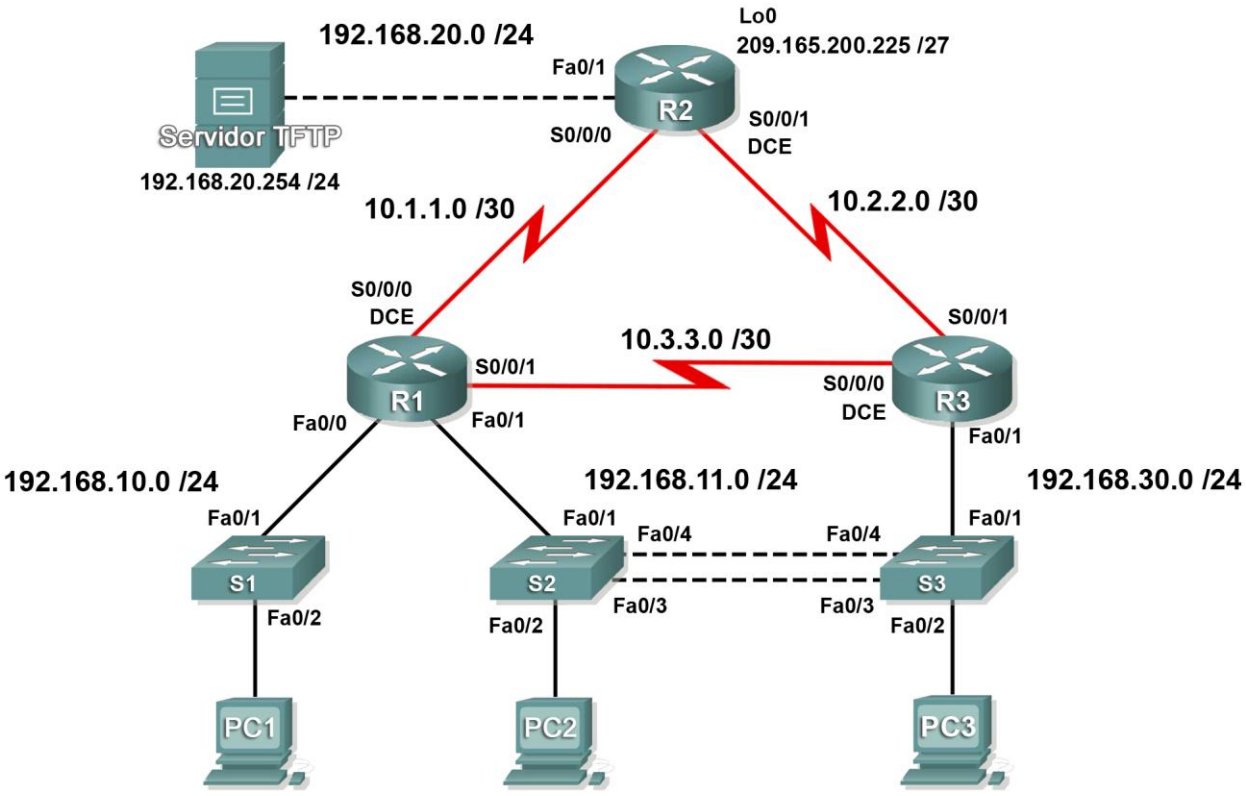


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/0**	192.168.10.1	255.255.255.0	No aplicable
	Fa0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
	S0/0/1	10.3.3.1	255.255.255.252	No aplicable
R2	**Fa0/1**	192.168.20.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

La tabla de direccionamiento continúa en la siguiente página

Tabla de direccionamiento (continuación)

R3	**Fa0/1**	No aplicable	No aplicable	No aplicable
	Fa0/1.11	192.168.11.3	255.255.255.0	No aplicable
	Fa0/1.30	192.168.30.1	255.255.255.0	No aplicable
	S0/0/0	10.3.3.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
S1	**VLAN10**	DHCP	255.255.255.0	No aplicable
S2	**VLAN11**	192.168.11.2	255.255.255.0	No aplicable
S3	**VLAN30**	192.168.30.2	255.255.255.0	No aplicable
PC1	**NIC**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

- Detectar y corregir todos los errores de red
- Verificar que se cumpla totalmente con los requisitos
- Documentar la red corregida

Escenario

Para esta actividad, no utilice protección de contraseña o inicio de sesión en ninguna línea de consola para evitar el bloqueo accidental. Use **ciscoccna** para todas las contraseñas de esta actividad.

Nota: Dado que esta actividad es acumulativa, deberá utilizar todos los conocimientos y las técnicas de resolución de problemas que ha adquirido con el material anterior para completar con éxito esta actividad.

Requisitos

- S2 es la raíz del spanning tree para VLAN 11 y S3 es la raíz del spanning tree para VLAN 30.
- S3 es un servidor VTP con S2 como cliente.
- El enlace serial entre R1 y R2 es Frame Relay.
- El enlace serial entre R2 y R3 usa encapsulación HDLC.
- El enlace serial entre R1 y R3 es autenticado por medio de CHAP.
- R2 debe tener procedimientos seguros de inicio de sesión, ya que es el router extremo de Internet.
- Todas las líneas vty, excepto las que pertenecen a R2, permiten conexiones sólo desde las subredes que se muestran en el diagrama de topología, sin incluir la dirección pública.
- Se debe evitar la suplantación de identidad de la dirección IP de origen en todos los enlaces que no se conectan al resto de los routers.
- Los protocolos de enrutamiento deben utilizarse en forma segura. En esta situación se usa EIGRP.
- R3 no debe poder hacer telnet a R2 a través del enlace serial conectado en forma directa.
- R3 tiene acceso a VLAN 11 y 30 a través de su puerto 0/1 Fast Ethernet.

- El servidor TFTP no debe recibir ningún tipo de tráfico que tenga una dirección de origen fuera de la subred. Todos los dispositivos tienen acceso al servidor TFTP.
- Todos los dispositivos de la subred 192.168.10.0 deben poder obtener sus direcciones IP del DHCP en R1. Esto incluye a S1.
- Se debe poder acceder a todas las direcciones que se muestran en el diagrama desde cada dispositivo.

Tarea 1: Detectar y corregir todos los errores de red

Utilice una frecuencia de reloj de **4 000 000** y una prioridad VLAN de **24 576** donde sea necesario.

Tarea 2: Verificar que se cumpla totalmente con los requisitos

Debido a que las limitaciones de tiempo impiden resolver un problema sobre cada tema, sólo una cantidad selecta de temas tiene problemas. Sin embargo, para reforzar y fortalecer sus capacidades de resolución de problemas, debe verificar que se cumpla con cada uno de los requisitos. Para hacerlo, presente un ejemplo de cada requisito (por ejemplo, un comando **show** o **debug**).

Tarea 3: Documentar la red corregida

Actividad de PT 8.5.3: Resolución de problemas de redes empresariales 3

Diagrama de topología

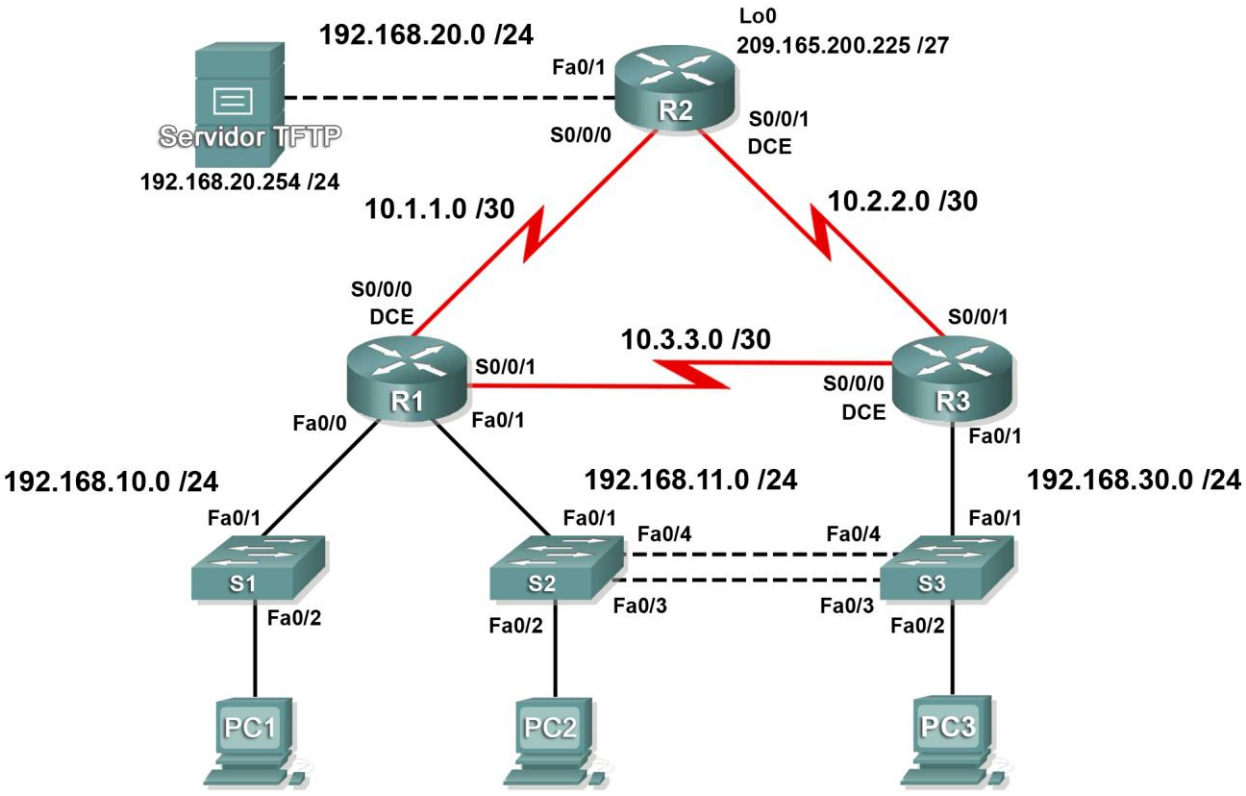


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminada
R1	**Fa0/0**	192.168.10.1	255.255.255.0	No aplicable
	Fa0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.1	255.255.255.252	No aplicable
	S0/0/1	10.3.3.1	255.255.255.252	No aplicable
R2	**Fa0/1**	192.168.20.1	255.255.255.0	No aplicable
	S0/0/0	10.1.1.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.1	255.255.255.252	No aplicable
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

La tabla de direccionamiento continúa en la siguiente página

Tabla de direccionamiento (continuación)

R3	**Fa0/1**	No aplicable	No aplicable	No aplicable
	Fa0/1.11	192.168.11.3	255.255.255.0	No aplicable
	Fa0/1.30	192.168.30.1	255.255.255.0	No aplicable
	S0/0/0	10.3.3.2	255.255.255.252	No aplicable
	S0/0/1	10.2.2.2	255.255.255.252	No aplicable
S1	**VLAN10**	DHCP	255.255.255.0	No aplicable
S2	**VLAN11**	192.168.11.2	255.255.255.0	No aplicable
S3	**VLAN30**	192.168.30.2	255.255.255.0	No aplicable
PC1	**NIC**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

- Detectar y corregir todos los errores de red
- Verificar que se cumpla totalmente con los requisitos
- Documentar la red corregida

Escenario

Para esta actividad, no utilice protección de contraseña o inicio de sesión en ninguna línea de consola para evitar el bloqueo accidental. Use **ciscoccna** para todas las contraseñas de esta actividad.

Nota: Dado que esta actividad es acumulativa, deberá utilizar todos los conocimientos y las técnicas de resolución de problemas que ha adquirido con el material anterior para completar con éxito esta actividad.

Requisitos

- S2 es la raíz del spanning tree para VLAN 11 y S3 es la raíz del spanning tree para VLAN 30.
- S3 es un servidor VTP con S2 como cliente.
- El enlace serial entre R1 y R2 es Frame Relay.
- El enlace serial entre R2 y R3 usa encapsulación HDLC.
- El enlace serial entre R1 y R3 es autenticado por medio de CHAP.
- R2 debe tener procedimientos seguros de inicio de sesión, ya que es el router extremo de Internet.
- Todas las líneas vty, excepto las que pertenecen a R2, permiten conexiones sólo desde las subredes que se muestran en el diagrama de topología, sin incluir la dirección pública.
- Se debe evitar la suplantación de identidad de la dirección IP de origen en todos los enlaces que no se conectan al resto de los routers.
- Los protocolos de enrutamiento deben utilizarse en forma segura. En esta situación se usa OSPF.
- R3 no debe poder hacer telnet a R2 a través del enlace serial conectado en forma directa.
- R3 tiene acceso a VLAN 11 y 30 a través de su puerto 0/1 Fast Ethernet.

- El servidor TFTP no debe recibir ningún tipo de tráfico que tenga una dirección de origen fuera de la subred. Todos los dispositivos tienen acceso al servidor TFTP.
- Todos los dispositivos de la subred 192.168.10.0 deben poder obtener sus direcciones IP del DHCP en R1. Esto incluye a S1.
- Se debe poder acceder a todas las direcciones que se muestran en el diagrama desde cada dispositivo.

Tarea 1: Detectar y corregir todos los errores de red

Utilice una frecuencia de reloj de **4 000 000** y una prioridad VLAN de **24 576** donde sea necesario.

Tarea 2: Verificar que se cumpla totalmente con los requisitos

Debido a que las limitaciones de tiempo impiden resolver un problema sobre cada tema, sólo una cantidad selecta de temas tiene problemas. Sin embargo, para reforzar y fortalecer sus capacidades de resolución de problemas, debe verificar que se cumpla con cada uno de los requisitos. Para hacerlo, presente un ejemplo de cada requisito (por ejemplo, un comando **show** o **debug**).

Tarea 3: Documentar la red corregida

Cisco | Networking Academy®
Mind Wide Open™

Actividad de PT 8.6.1: Desafío de integración de aptitudes de CCNA

Diagrama de topología

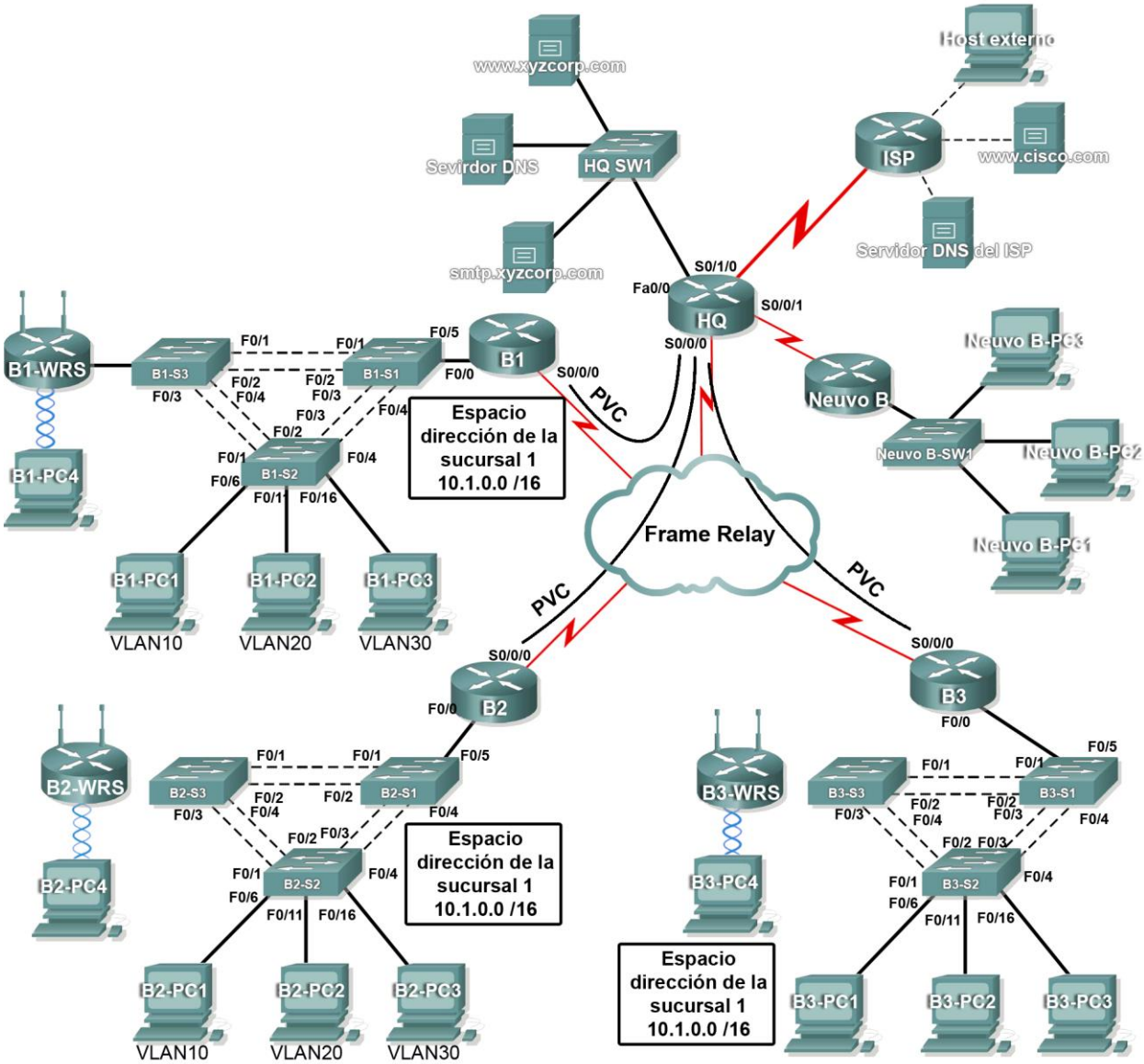


Tabla de direccionamiento para HQ

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Asignaciones de DLCI
HQ	Fa0/0	10.0.1.1	255.255.255.0	No aplicable
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 a B1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 a B2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 a B3
	S0/0/1	10.255.255.253	255.255.255.252	No aplicable
	S0/1/0	209.165.201.1	255.255.255.252	No aplicable

Tabla de direccionamiento para routers de Branch

Dispositivo	Interfaz	Dirección IP	Máscara de subred
BX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	2.ª dirección	255.255.255.252
BX-S1	VLAN 99	10.X.99.21	255.255.255.0
BX-S2	VLAN 99	10.X.99.22	255.255.255.0
BX-S3	VLAN 99	10.X.99.23	255.255.255.0
BX-WRS	VLAN 1	10.X.40.1	255.255.255.0

- Reemplace “X” por el número de router de Branch (B1, B2 o B3).
- Los PVC punto a punto con HQ utilizan esta segunda dirección en la subred. HQ utiliza la primera dirección.
- Los routers WRT300N obtienen la dirección de Internet a través de DHCP desde el router de Branch.

Configuración de VLAN y asignaciones de puertos

Número de VLAN	Dirección de red	Nombre de VLAN	Asignaciones de puertos
10	10.X.10.0/24	Admin	BX-S2, Fa0/6
20	10.X.20.0/24	Sales	BX-S2, Fa0/11
30	10.X.30.0/24	Production	BX-S2, Fa0/16
88	10.X.88.0/24	Inalámbrico	BX-S3, Fa0/7
99	10.X.99.0/24	Admin y Nativo	Todos los enlaces troncales

Objetivos de aprendizaje

- Configurar Frame Relay en una topología hub-and-spoke
- Configurar PPP con autenticación CHAP y PAP
- Configurar NAT estática y dinámica
- Configurar el enrutamiento estático y predeterminado

Introducción

En esta actividad integral de aptitudes de CCNA, la empresa XYZ usa una combinación de Frame Relay y PPP para las conexiones WAN. El router HQ proporciona acceso al conjunto de servidores y a Internet a través de la NAT. HQ también usa una ACL del firewall básico para filtrar el tráfico entrante. Cada router de Branch está configurado para el enrutamiento entre VLAN y DHCP. El enrutamiento se consigue mediante EIGRP y las rutas estáticas y predeterminadas. Las VLAN, el VTP y el STP se configuran en cada una de las redes conmutadas. La seguridad de puerto está activada y se proporciona acceso inalámbrico. Su trabajo consiste en implementar con éxito todas estas tecnologías, haciendo uso de lo que aprendió durante los cuatro cursos Exploration que lo condujeron a esta actividad final.

Es responsable de configurar HQ y los routers de Branch B1, B2 y B3. Además, debe configurar cada dispositivo que se conecte a la red a través de un router de Branch. El router NewB representa una nueva sucursal que se adquiere mediante la fusión con una empresa más pequeña. Como usuario, no tiene acceso al router NewB. Sin embargo, debe establecer un enlace entre HQ y NewB para que esta nueva sucursal pueda acceder a la red interna y a Internet.

Los routers y switches bajo su administración no tienen configuración. Packet Tracer no califica ninguna de las configuraciones básicas como nombre de host, contraseñas, mensajes y otros comandos de mantenimiento general ni serán parte de la especificación de la tarea. No obstante, se espera que el usuario los configure y el instructor puede optar por calificar estos comandos.

Debido a que esta actividad usa una red tan grande, con alrededor de 500 componentes necesarios dentro de los puntos de evaluación, no necesariamente verá incrementar su porcentaje de finalización cada vez que ingrese un comando. Además, no recibe un porcentaje específico que debe completarse al final de cada tarea, sino que utiliza las pruebas de conectividad para verificar las configuraciones de cada tarea. Sin embargo, en cualquier momento puede hacer clic en **Verificar resultados** para ver si un componente en particular está calificado y si lo configuró correctamente.

Debido a que los switches y los routers de Branch (B1, B2 y B3) se diseñan teniendo en cuenta la escalabilidad, puede volver a utilizar las secuencias de comandos. Por ejemplo: sus configuraciones para B1, B1-S1, B1-S2 y B1-S3 se pueden aplicar directamente a los dispositivos B2 con tan sólo unos ajustes mínimos.

Nota: Este Desafío de integración de aptitudes del CCNA también se encuentra disponible en una versión abierta, en la que puede elegir las tecnologías y el esquema de direccionamiento que desee implementar. Verifica su configuración al probar la conectividad de extremo a extremo.

Tarea 1: Configurar Frame Relay en una topología hub-and-spoke

Paso 1. Configurar el núcleo Frame Relay.

Utilice las tablas de direccionamiento y los siguientes requisitos.

HQ es el router hub. B1, B2 y B3 son los rayos.

- HQ utiliza una subinterfaz punto a punto para cada uno de los routers de Branch.
- B3 debe configurarse manualmente para usar la encapsulación IETF.
- El tipo LMI debe configurarse manualmente como q933 para HQ, B1 y B2. B3 usa ANSI.

Paso 2. Configurar la interfaz LAN en HQ.

Paso 3. Verificar que HQ pueda hacer ping a cada uno de los routers de Branch.

Tarea 2: Configurar PPP con autenticación CHAP y PAP

Paso 1. Configurar el enlace WAN desde HQ hasta ISP mediante encapsulación PPP y autenticación CHAP.

La contraseña de CHAP es **ciscochap**.

Paso 2. Configurar el enlace WAN desde HQ hasta NewB mediante encapsulación PPP y autenticación PAP.

Debe conectar un cable a las interfaces correctas. HQ es el lado DCE del enlace. Elija la frecuencia de reloj. La contraseña de PAP es **ciscopap**.

Paso 3. Verificar que HQ pueda hacer ping a ISP y NewB.

Tarea 3: Configurar NAT dinámica y estática en HQ

Paso 1. Configurar la NAT.

Utilice los siguientes requisitos:

- Permita que se traduzcan todas las direcciones para el espacio de direcciones 10.0.0.0/8.
- La empresa XYZ posee el espacio de direcciones 209.165.200.240/29. El pool, XYZCORP, utiliza las direcciones de .241 a .245 con una máscara /29.
- El sitio Web www.xyzcorp.com en 10.0.1.2 está registrado en el sistema público DNS en la dirección IP 209.165.200.246.

Paso 2. Verificar que la NAT funcione; para ello se debe usar un ping extendido.

Desde HQ, haga ping en la interfaz serial 0/0/0 de ISP mediante la interfaz LAN de HQ como dirección de origen. Este ping debe tener éxito.

Verifique que la NAT haya traducido el ping con el comando **show ip nat translations**.

Tarea 4: Configurar el enrutamiento estático y predeterminado

Paso 1. Configurar HQ con una ruta predeterminada al ISP y una ruta estática a la LAN de NewB.

Utilice como argumento la interfaz de salida.

Paso 2. Configurar los routers de Branch con una ruta predeterminada a HQ.

Utilice la dirección IP del siguiente salto como argumento.

Paso 3. Verificar la conectividad más allá del ISP.

Las tres PC NewB y la PC NetAdmin deben poder hacer ping al servidor web www.cisco.com.

Tarea 5: Configurar el enrutamiento entre VLAN

Paso 1. Configurar cada router de Branch para el enrutamiento entre VLAN.

Utilice la tabla de direccionamiento de los routers de Branch para configurar y activar la interfaz LAN para el enrutamiento entre VLAN. La VLAN 99 es la VLAN nativa.

Paso 2. Verificar las tablas de enrutamiento.
Ahora cada router de Branch debe tener seis redes conectadas en forma directa y una ruta estática predeterminada.

Tarea 6: Configurar y optimizar el enrutamiento EIGRP

Paso 1. Configurar HQ, B1, B2 y B3 con EIGRP.

- Use AS 100.
- Desactive las actualizaciones EIGRP en las interfaces apropiadas.
- Resuma en forma manual las rutas EIGRP de modo que cada router de Branch sólo publique el espacio de direcciones 10.X.0.0/16 a HQ.

Nota: Packet Tracer no simula con precisión el beneficio de las rutas resumidas EIGRP. Las tablas de enrutamiento aún muestran todas las subredes, a pesar de que el resumen manual no se configuró correctamente.

Paso 2. Verificar las tablas de enrutamiento y la conectividad.

Ahora HQ y los routers de Branch deben tener tablas de enrutamiento completas.

La PC NetAdmin ahora debe poder hacer ping a cada una de las subinterfaces VLAN de cada router de Branch.

Tarea 7: Configurar VTP, el enlace troncal, la interfaz VLAN y las VLAN

Los siguientes requisitos se aplican a los tres Branches. Configure un grupo de tres switches. Luego use las secuencias de comandos de esos switches en los otros dos grupos de switches.

Paso 1. Configurar los switches de Branch con VTP.

- BX-S1 es el servidor VTP. BX-S2 y BX-S3 son los clientes VTP.
- El nombre de dominio es **XYZCORP**.
- La contraseña es **xyzvtp**.

Paso 2. Configurar el enlace troncal en BX-S1, BX-S2 y BX-S3.

Configure las interfaces apropiadas en el modo de enlace troncal y asigne la VLAN 99 como VLAN nativa.

Paso 3. Configurar la interfaz VLAN y la gateway predeterminada en BX-S1, BX-S2 y BX-S3.

Paso 4. Crear las VLAN en BX-S1.

Cree y nombre las VLAN indicadas en la tabla Configuración de VLAN y asignaciones de puertos sólo en BX-S1. VTP publica las nuevas VLAN a BX-S1 y BX-S2.

Paso 5. Verificar que las VLAN se hayan enviado a BX-S2 y BX-S3.

Utilice los comandos apropiados para verificar que S2 y S3 ahora tengan las VLAN que se crearon en S1. Packet Tracer puede demorar algunos minutos en simular las publicaciones VTP. Una forma rápida de forzar el envío de publicaciones VTP consiste en cambiar uno de los switches cliente a modo transparente y luego volver a cambiarlo a modo cliente.

Tarea 8: Asignar las VLAN y configurar la seguridad de puerto

Paso 1. Asignar las VLAN a los puertos de acceso.

Utilice la tabla Configuración de VLAN y asignaciones de puertos para completar los siguientes requisitos:

- Configurar los puertos de acceso
- Asignar las VLAN a los puertos de acceso.

Paso 2. Configurar la seguridad de puerto.

Use la siguiente política para establecer la seguridad de puerto en los puertos de acceso BX-S2:

- Permitir sólo una dirección MAC
- Configurar la primera dirección MAC aprendida para que se “pegue” a la configuración
- Configurar el puerto para que se desconecte si se produce una violación de seguridad

Paso 3. Verificar las asignaciones de VLAN y la seguridad de puerto.

Utilice los comandos apropiados para verificar que las VLAN de acceso se asignen correctamente y que la política de seguridad de puerto se haya activado.

Tarea 9: Configurar el STP

Paso 1. Configurar BX-S1 como puente raíz.

Establezca el nivel de prioridad de 4096 en BX-S1 para que estos switches sean siempre el puente raíz para todas las VLAN.

Paso 2. Configurar BX-S3 como puente raíz de respaldo.

Establezca el nivel de prioridad de 8192 en BX-S3 para que estos switches sean siempre el puente raíz de respaldo para todas las VLAN.

Paso 3. Verificar que BX-S1 sea el puente raíz.

Tarea 10: Configurar el DHCP

Paso 1. Configurar los pools de DHCP para cada VLAN.

En los routers de Branch, configure los pools de DHCP para cada VLAN según los siguientes requisitos:

- Excluir las primeras 10 direcciones IP de cada pool para las LAN.
- Excluir las primeras 24 direcciones IP de cada pool para las LAN inalámbricas.
- El nombre del pool es **BX_VLAN##**, donde **X** es el número de router y ## es el número de VLAN.
- Incluir el servidor DNS conectado al conjunto de servidores HQ como parte de la configuración DHCP.

Paso 2. Configurar las PC para que utilicen DHCP.

Actualmente, las PC están configuradas para usar direcciones IP estáticas. Cambie esta configuración a DHCP.

Paso 3. Verificar que las PC y los routers inalámbricos tengan una dirección IP.

Paso 4. Verificar la conectividad.

Todas las PC físicamente conectadas a la red deben poder hacer ping al servidor Web www.cisco.com.

Tarea 11: Configurar una ACL del firewall

Paso 1. Verificar la conectividad desde el host externo.

La PC del host externo debe poder hacer ping al servidor en www.xyzcorp.com

Paso 2. Implementar una ACL firewall básica.

Debido a que el ISP representa la conectividad a Internet, configure una ACL nombrada, llamada **FIREWALL,** en el siguiente orden:

1. Permitir solicitudes HTTP entrantes para el servidor www.xyzcorp.com.
2. Sólo permitir sesiones TCP establecidas desde el ISP y cualquier otro origen.
3. Permita únicamente respuestas de ping entrantes desde el ISP y cualquier otro origen.
4. Bloquee explícitamente cualquier otro acceso entrante desde el ISP y cualquier otro origen más allá del ISP.

Paso 3. Verificar la conectividad desde el host externo.

La PC del host externo no debe poder hacer ping al servidor en www.xyzcorp.com. Sin embargo, la PC del host externo debe poder solicitar una página Web.

Tarea 12: Configurar la conectividad inalámbrica

Paso 1. Verificar la configuración DHCP.

Cada router BX-WRS ya debe tener direccionamiento IP desde el DHCP del router BX para VLAN 88.

Paso 2. Configurar la red y los parámetros de la LAN.

La “IP de router” en la página **Estado** de la ficha GUI debe ser la primera IP de la subred 10.x.40.0/24. Todos los demás parámetros deben ser los predeterminados.

Paso 3. Configurar los parámetros de la red inalámbrica.

Los SSID para los routers son **BX-WRS_LAN,** donde **X** es el número de router de Branch.

La clave WEP es **12345ABCDE**

Paso 4. Configurar los routers inalámbricos para el acceso remoto.

Configure la contraseña de administración como **cisco123** y active la administración remota.

Paso 5. Configurar las PC BX-PC4 para que accedan a la red inalámbrica mediante DHCP.

Paso 6. Verificar la conectividad y la capacidad de administración remota.

Cada una de las PC inalámbricas debe poder acceder al servidor Web www.cisco.com.

Verifique la capacidad de administración remota al acceder al router inalámbrico a través del explorador Web.

Tarea 13: Resolución de problemas de red

Paso 1. Dividir la red.

Un estudiante se retira del aula, si fuera necesario, mientras el otro estudiante divide la configuración.

Paso 2. Resolver el problema.

El estudiante regresa y usa las técnicas de resolución de problemas para aislar y resolver el problema.

Paso 3. Volver a dividir la red.

Los estudiantes intercambian los papeles y repiten los pasos 1 y 2.