Cisco | Networking Academy®
Mind Wide Open™

Switching y routing CCNA: Principios básicos de routing y switching

Manual de Packet Tracer para el instructor

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

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

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Objetivos

- Configurar los nombres de host y las direcciones IP en dos switches con sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Utilizar comandos del IOS de Cisco para especificar o limitar el acceso a las configuraciones de los dispositivos.
- Utilizar comandos del IOS para guardar la configuración en ejecución.
- Configurar dos dispositivos host con direcciones IP.
- Verificar la conectividad entre dos terminales PC.

Situación

Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante el IOS de Cisco y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

Requisitos

- Utilice una conexión de consola para acceder a cada switch.
- Nombre los switches **[[S1Name]]** y **[[S2Name]]**.
- Utilice la contraseña **[[LinePW]]** para todas las líneas.
- Utilice la contraseña secreta **[[SecretPW]]**.
- Cifre todas las contraseñas de texto no cifrado.
- Incluya la palabra **warning** (advertencia) en el aviso del mensaje del día (MOTD).
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos.

Nota: haga clic en **Check Results (Verificar resultados)** para ver su progreso. Haga clic en **Reset Activity (Restablecer actividad)** para generar un nuevo conjunto de requisitos.

Notas para el instructor

La siguiente información se encuentra solo en la versión para el instructor.

En esta actividad, se utilizan variables que se generan de forma aleatoria cada vez la actividad se abre o se hace clic en el botón “Reset Activity”. Aunque en las tablas que se incluyen debajo se muestran nombres de dispositivos asignados a esquemas de direcciones específicos, los nombres y las direcciones no están vinculados. Por ejemplo, un estudiante podría obtener los nombres de los dispositivos presentados en la situación 1 con el direccionamiento que se muestra en la situación 2. Además, el estudiante recibirá una de tres versiones de topología.

Escenario 1

Dispositivo	Interfaz	Dirección	Máscara de subred
Clase-A	VLAN 1	128.107.20.10	255.255.255.0
Clase-B	VLAN1	128.107.20.15	255.255.255.0
Estudiante-1	NIC	128.107.20.25	255.255.255.0
Estudiante-2	NIC	128.107.20.30	255.255.255.0

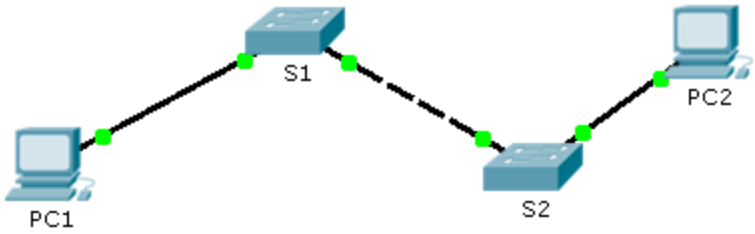
Escenario 2

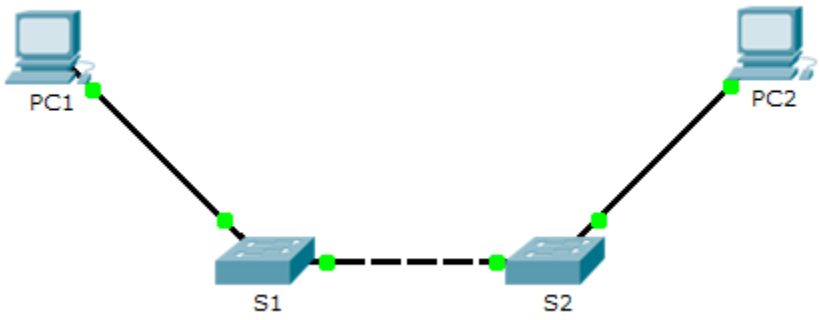
Dispositivo	Interfaz	Dirección	Máscara de subred
Sala 145	VLAN 1	172.16.5.35	255.255.255.0
Sala 146	VLAN 1	172.16.5.40	255.255.255.0
Administrador	NIC	172.16.5.50	255.255.255.0
Recepción	NIC	172.16.5.60	255.255.255.0

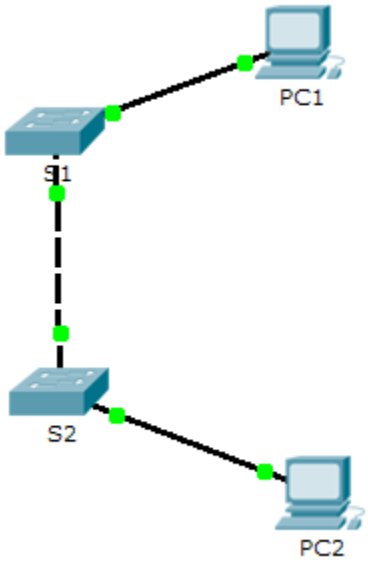
Escenario 3

Dispositivo	Interfaz	Dirección	Máscara de subred
ASw-1	VLAN 1	10.10.10.100	255.255.255.0
ASw-2	VLAN 1	10.10.10.150	255.255.255.0
Usuario-01)	NIC	10.10.10.4	255.255.255.0
Usuario-02)	NIC	10.10.10.5	255.255.255.0

Isomorfos de la topología







Packet Tracer: configuración de SSH (versión para el instructor)

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

Topología

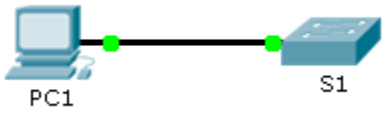


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

Parte 1: proteger las contraseñas

Parte 2: cifrar las comunicaciones

Parte 3: verificar la implementación de SSH

Información básica

SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos. En esta actividad, protegerá un switch remoto con el cifrado de contraseñas y SSH.

Parte 1: Contraseñas seguras

a. Desde el símbolo del sistema en la **PC1**, acceda al **S1** mediante Telnet. La contraseña de los modos EXEC del usuario y EXEC privilegiado es **cisco**.

b. Guarde la configuración actual, de manera que pueda revertir cualquier error que cometa reiniciando el **S1**.

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado. Introduzca el comando para cifrar las contraseñas de texto no cifrado:

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

d. Verifique que las contraseñas estén cifradas.

Parte 2: cifrar las comunicaciones

Paso 1: establecer el nombre de dominio IP y generar claves seguras.

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio **netacad.pka.**

```
S1(config)# ip domain-name netacad.pka
```

b. Se necesitan claves seguras para cifrar los datos. Genere las claves RSA con la longitud de clave 1024.

```
S1(config)# crypto key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Paso 2: crear un usuario de SSH y reconfigurar las líneas VTY para que solo admitan acceso por SSH.

a. Cree un usuario llamado **administrator** con la contraseña **cisco**.

```
S1(config)# username administrator password cisco
```

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

```
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# no password cisco
```

Parte 3: verificar la implementación de SSH

a. Cierre la sesión de Telnet e intente volver a iniciar sesión mediante Telnet. El intento debería fallar.

b. Intente iniciar sesión mediante SSH. Escriba **ssh** y presione la tecla **Enter**, sin incluir ningún parámetro que revele las instrucciones de uso de comandos. Sugerencia: la opción **-l** representa la letra “L”, no el número 1.

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC privilegiado y guarde la configuración. Si no pudo acceder de forma correcta al **S1**, reinicie y comience de nuevo en la parte 1.

Packet Tracer: configuración de seguridad de puertos de switch (versión para el instructor)

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

Topología

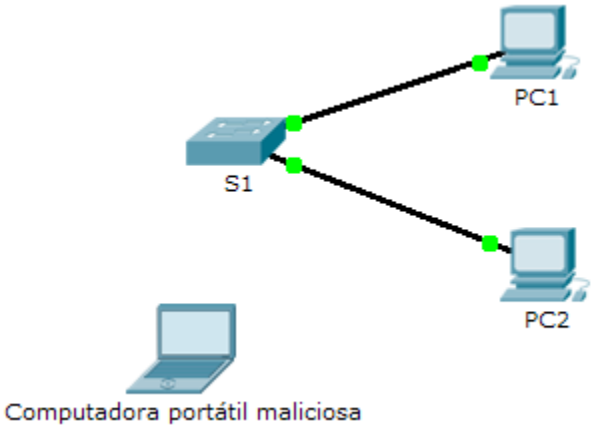


Tabla de direccionamiento

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

Objetivo

Parte 1: configurar la seguridad de puertos

Parte 2: verificar la seguridad de puertos

Información básica

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

Parte 1: Configurar la seguridad del puerto

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

```
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# switchport port-security
```

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

```
S1(config-if-range)# switchport port-security maximum 1
```

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

```
S1(config-if-range)# switchport port-security mac-address sticky
```

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

```
S1(config-if-range)# switchport port-security violation restrict
```

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

```
S1(config-if-range)# interface range fa0/3 - 24 , gi1/1 - 2
S1(config-if-range)# shutdown
```

Parte 2: Verificar la seguridad de puerto

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

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

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

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

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

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

```
S1# show port-security interface fa0/2
```

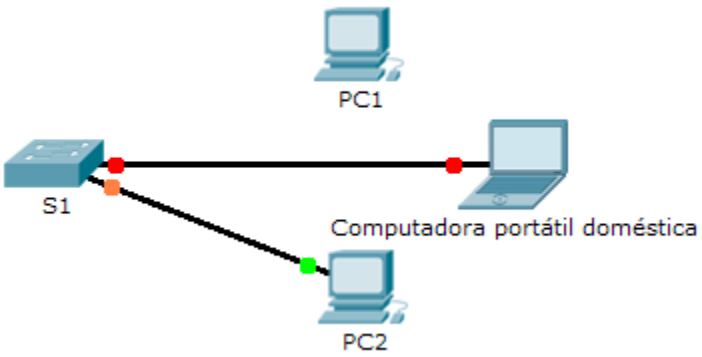
g. Desconecte la **Computadora portátil maliciosa** y vuelva a conectar la **PC2**. Verifique que la **PC2** pueda hacer ping a la **PC1**.

h. ¿Por qué la **PC2** puede hacer ping a la **PC1**, pero la **Computadora portátil maliciosa** no puede? La seguridad de puertos que se habilitó solo permite que el dispositivo cuya MAC se detectó primero acceda al puerto e impide el acceso de cualquier otro dispositivo.

Packet Tracer: resolución de problemas de seguridad de puertos de switch (versión para el instructor)

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

Topología



Situación

El empleado que normalmente usa la PC1 trajo la computadora portátil de su hogar, desconectó la PC1 y conectó la computadora portátil a la toma de telecomunicaciones. Después de recordarle que la política de seguridad no permite dispositivos personales en la red, usted debe volver a conectar la PC1 y volver a habilitar el puerto.

Requisitos

- Desconecte la **Computadora portátil doméstica** y vuelva a conectar la **PC1** al puerto correspondiente.
  - Cuándo se volvió a conectar la **PC1** al puerto de switch, ¿se modificó el estado del puerto? No
  - Introduzca el comando para ver el estado del puerto. ¿Cuál es el estado del puerto?

```
S1# sh int fa0/1
FastEthernet0/1 is administratively down, line protocol is down (disabled)
```

  - ¿Qué comandos de seguridad de puertos habilitaron esta característica? `switchport port-security violation shutdown`
- Habilite el puerto con el comando necesario.

```
S1(config)# int fa0/1
S1(config-if)# no shut
```

- Verifique la conectividad. Ahora, la **PC1** debe poder hacer ping a la **PC2**.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 90 puntos. Las respuestas a las preguntas valen 10 puntos.

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

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

Topología

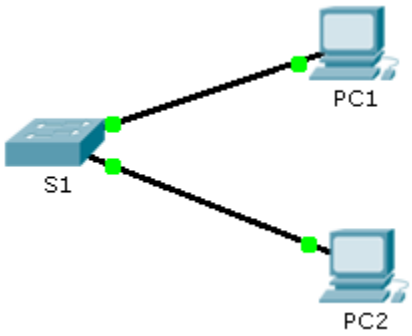


Tabla de direccionamiento

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

Situación

El administrador de red le solicitó que configure un nuevo switch. En esta actividad, usará una lista de requisitos para configurar el nuevo switch con las configuraciones iniciales, SSH y la seguridad de puertos.

Requisitos

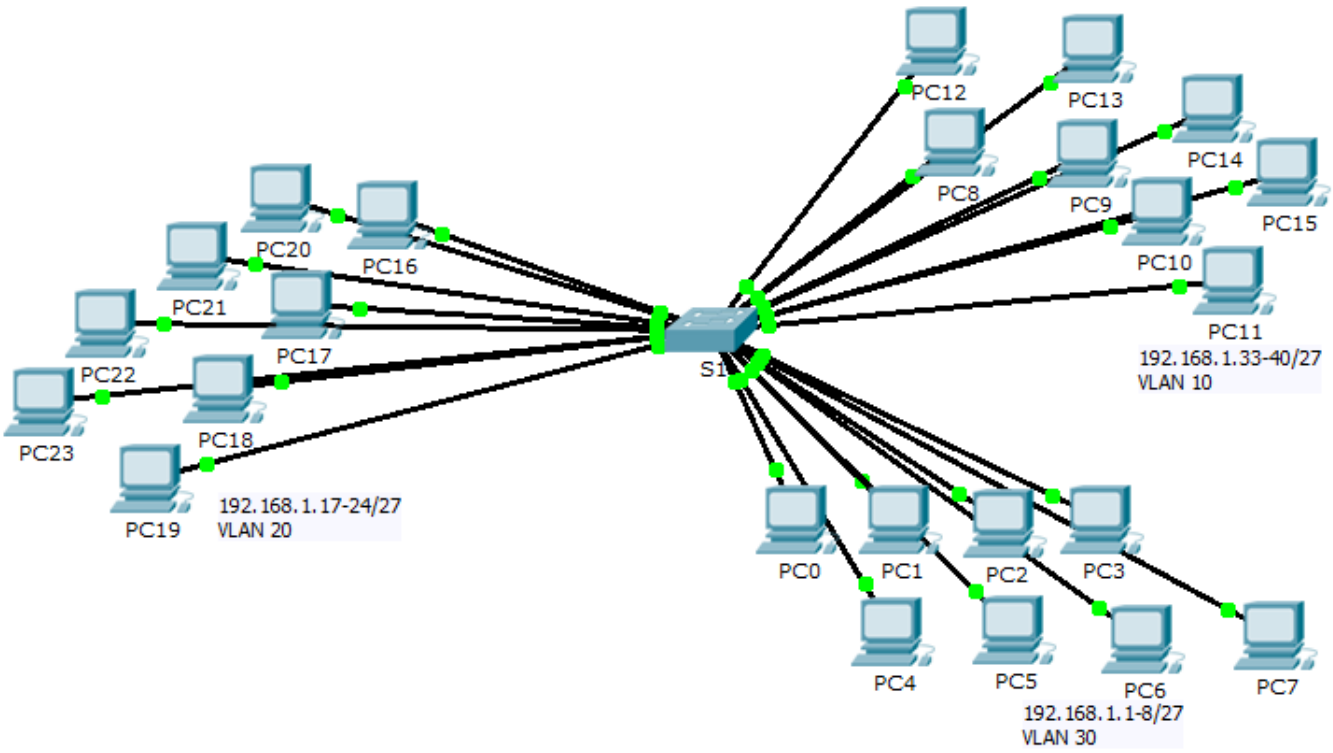
- Configure el **S1** con los siguientes parámetros iniciales:
  - Nombre de host
  - Aviso con la palabra **warning** (advertencia)
  - Usuario y contraseña de puerto de consola **cisco**
  - Contraseña de enable cifrada **class**
  - Cifrado de contraseñas de texto no cifrado
  - Direccionamiento de interfaces de administración
- Configure SSH para proteger el acceso remoto con los siguientes parámetros:
  - Nombre de dominio **cisco.com.**
  - Parámetros de par de claves RSA compatibles con SSH, versión 2.
  - Establecimiento de SSH, versión 2.

  - Usuario **admin** con contraseña **ccna.**
  - Las líneas VTY solo aceptan conexiones SSH y utilizan el inicio de sesión local para la autenticación.
- Configure la característica de seguridad de puertos para restringir el acceso a la red.
  - Deshabilite todos los puertos sin utilizar.
  - Establezca la interfaz en modo de acceso.
  - Habilite la seguridad de puertos para permitir solo dos hosts por puerto.
  - Registre la dirección MAC en la configuración en ejecución.
  - Asegúrese de que los puertos se deshabiliten cuando se produzcan infracciones de puertos.

Packet Tracer: ¿quién escucha la difusión? (Versión para el instructor)

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

Topología



Objetivos

Parte 1: observar el tráfico de difusión en una implementación de VLAN

Parte 2: completar las preguntas de repaso

Situación

En esta actividad, se ocupa la totalidad de un switch Catalyst 2960 de 24 puertos. Se utilizan todos los puertos. Observará el tráfico de difusión en una implementación de VLAN y responderá algunas preguntas de reflexión.

Parte 1: Observar el tráfico de difusión en la implementación de una VLAN

Paso 1: utilizar ping para generar tráfico.

a. Haga clic en **PC0** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

b. Introduzca el comando **ping 192.168.1.8**. El ping debe tener éxito.

A diferencia de las LAN, las VLAN son dominios de difusión creados por switches. Utilice el modo **Simulation** (Simulación) de Packet Tracer para hacer ping a las terminales dentro de su propia VLAN. Responda las preguntas del paso 2 de acuerdo con lo observado.

Paso 2: generar y examinar el tráfico de difusión.

a. Cambie a modo de **simulación**.

b. En el panel de simulación, haga clic en **Edit Filters** (Editar filtros). Desmarque la casilla de verificación **Show All/None** (Mostrar todos/ninguno). Active la casilla de verificación **ICMP**.

c. Haga clic en la herramienta **Add Complex PDU** (Agregar PDU compleja), la cual está representada con el ícono del sobre abierto en la barra de herramientas derecha.

d. Pase el cursor del mouse sobre la topología, y el puntero cambiará a un sobre con un signo más (+).

e. Haga clic en la **PC0** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de diálogo **Create Complex PDU** (Crear PDU compleja). Introduzca los siguientes valores:

- Dirección IP de destino: 255.255.255.255 (dirección de difusión)
- Número de secuencia: 1
- Tiempo de intento único: 0

Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP y OTHER.

f. Haga clic en **Create PDU** (Crear PDU). Este paquete de difusión de prueba ahora aparece en **Simulation Panel Event List** (Lista de eventos del panel de simulación). También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para Scenario 0 (Situación 0).

g. Haga clic en **Capture/Forward** (Capturar/Adelantar) dos veces. ¿Qué sucede con el paquete? El paquete se envía al switch y, luego, se transmite por difusión a todas las computadoras que pertenecen a la misma VLAN y, en este caso, la VLAN 10.

h. Repita este proceso para la **PC8** y la **PC16**.

Parte 2: completar las preguntas de repaso

1. Si una computadora en la VLAN 10 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todas las terminales en la VLAN 10.
2. Si una computadora en la VLAN 20 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todas las terminales en la VLAN 20.
3. Si una computadora en la VLAN 30 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todas las terminales en la VLAN 30.
4. ¿Qué le sucede a una trama enviada desde una computadora en la VLAN 10 hacia una computadora en la VLAN 30? Se descarta, porque no están en la misma VLAN.
5. ¿Qué puertos del switch se encienden si una computadora conectada al puerto 11 envía un mensaje de unidifusión a una computadora conectada al puerto 13? Los puertos 11 y 13.
6. ¿Qué puertos del switch se encienden si una computadora conectada al puerto 2 envía un mensaje de unidifusión a una computadora conectada al puerto 23? El paquete se descartará.

7. Desde el punto de vista de los puertos, ¿cuáles son los dominios de colisiones en el switch? Cada puerto es su propio dominio de colisiones.
8. Desde el punto de vista de los puertos, ¿cuáles son los dominios de difusión en el switch? Cada VLAN es su propio dominio de difusión.

Tabla de calificación sugerida

Hay 10 preguntas que valen 10 puntos cada una.

Packet Tracer: investigación de la implementación de una VLAN (versión para el instructor)

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

Topología

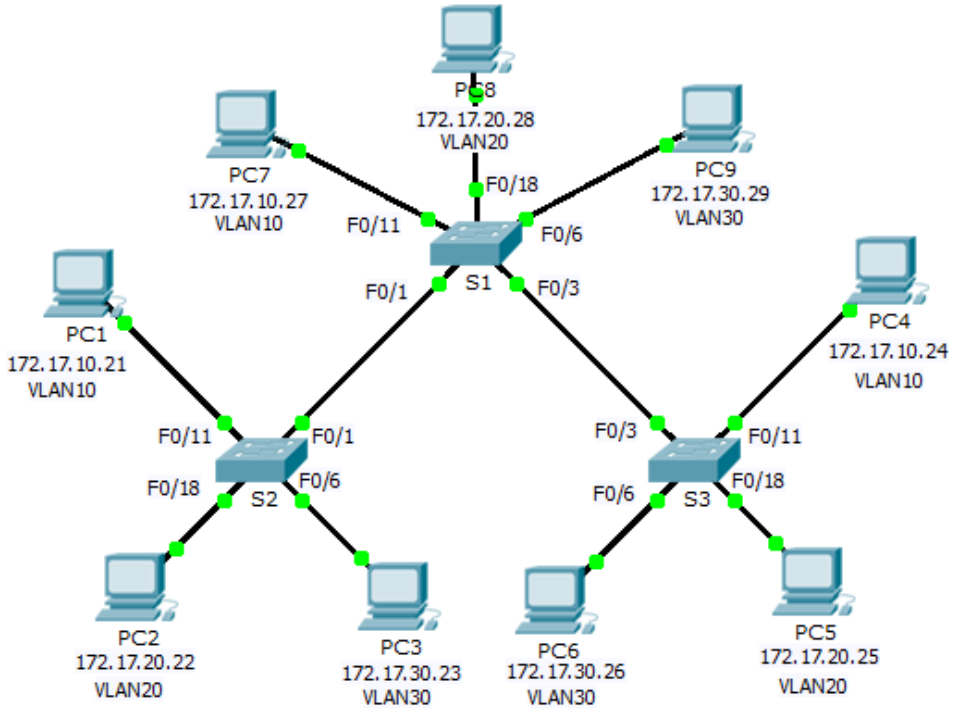


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.17.99.31	255.255.255.0	N/A
S2	VLAN 99	172.17.99.32	255.255.255.0	N/A
S3	VLAN 99	172.17.99.33	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1
PC7	NIC	172.17.10.27	255.255.255.0	172.17.10.1
PC8	NIC	172.17.20.28	255.255.255.0	172.17.20.1
PC9	NIC	172.17.30.29	255.255.255.0	172.17.30.1

Objetivos

Parte 1: observar el tráfico de difusión en una implementación de VLAN

Parte 2: observar el tráfico de difusión sin VLAN

Parte 3: completar las preguntas de reflexión

Información básica

En esta actividad, observará el modo en que los switches reenvían el tráfico de difusión cuando hay VLAN configuradas y cuando no las hay.

Parte 1: Observar el tráfico de difusión en la implementación de una VLAN

Paso 1: Haga ping de PC1 a PC6.

a. Espere que todas las luces de enlace se pongan en verde. Para acelerar este proceso, haga clic en la opción **Fast Forward Time** (Adelantar el tiempo), ubicada en la barra de herramientas inferior amarilla.

b. Haga clic en la pestaña **Simulation** y utilice la herramienta **Add Simple PDU**. Haga clic en **PC1** y, a continuación, haga clic en **PC6**.

c. Haga clic en el botón **Capture/Forward** para avanzar por el proceso. Observe las peticiones ARP a medida que atraviesan la red. Cuando aparezca la ventana Buffer Full (Búfer lleno), haga clic en el botón **View Previous Events** (Ver eventos anteriores).

d. ¿Tuvieron éxito los pings? ¿Por qué? No, los pings no se realizaron correctamente, porque la PC1 está en una VLAN diferente que la PC6, lo que no permite que estos dispositivos se comuniquen entre sí porque están separados de manera lógica.

e. Examine el panel de simulación, ¿dónde envió el paquete el **S3** después de recibirlo? El S3 lo envió a la PC4 porque estaba en la misma VLAN que la PC1.

En funcionamiento normal, cuando un switch recibe una trama de difusión en uno de sus puertos, envía la trama a todos los demás puertos. Observe que el **S2** solo envía la solicitud de ARP al **S1** por Fa0/1. También observe que el **S3** solo envía la solicitud de ARP a la **PC4** por F0/11. Tanto la **PC1** como la **PC4** pertenecen a la VLAN 10. La **PC6** pertenece a la VLAN 30. Dado que el tráfico de difusión está dentro de la VLAN, la **PC6** nunca recibe la solicitud de ARP de la **PC1**. Debido a que la **PC4** no es el destino, descarta la solicitud de ARP. El ping de la **PC1** falla debido a que la **PC1** nunca recibe una respuesta de ARP.

Paso 2: hacer ping de la PC1 a la PC4.

a. Haga clic en el botón **New** (Nuevo) en la ficha desplegable Scenario 0 (Situación 0). Ahora, haga clic en el ícono **Add Simple PDU** (Agregar PDU simple) ubicado en el lado derecho de Packet Tracer y haga ping de la **PC1** a la **PC4**.

b. Haga clic en el botón **Capture/Forward** para avanzar por el proceso. Observe las peticiones ARP a medida que atraviesan la red. Cuando aparezca la ventana Buffer Full (Búfer lleno), haga clic en el botón **View Previous Events** (Ver eventos anteriores).

c. ¿Tuvieron éxito los pings? ¿Por qué? Sí, porque tanto la PC1 como la PC4 pertenecen a la VLAN 10, por lo tanto, la ruta de la solicitud de ARP es la misma que antes. Como PC4 es el destino, responde a la petición ARP. Entonces, PC1 puede enviar el ping con la dirección MAC de destino para PC4.

d. Examine el panel de simulación. Cuando el paquete llegó al **S1**, ¿por qué también se reenvió a la **PC7**? Porque la PC7 también pertenece a la VLAN 10, y las solicitudes de ARP eran para la VLAN 10. Los switches reenvían los paquetes a cualquier dispositivo que esté conectado a la VLAN 10 en su puerto.

Parte 2: observar el tráfico de difusión sin VLAN

Paso 1: borrar las configuraciones en los tres switches y eliminar la base de datos de VLAN.

a. Vuelva al modo **Realtime**.

b. Elimine la configuración de inicio en los tres switches. ¿Qué comando se utiliza para eliminar la configuración de inicio de los switches? `Switch# erase startup-config`

c. ¿Dónde se almacena el archivo VLAN en los switches? flash:vlan.dat

d. Elimine el archivo VLAN en los tres switches. ¿Qué comando elimina el archivo VLAN almacenado en los switches? `Switch# delete vlan.dat`

Paso 2: volver a cargar los switches.

Utilice el comando **reload** en el modo EXEC privilegiado para reiniciar todos los switches. Espere a que todo el enlace se torne verde. Para acelerar este proceso, haga clic en la opción **Fast Forward Time** (Adelantar el tiempo), ubicada en la barra de herramientas inferior amarilla.

Paso 3: Haga clic en Capture/Forward para enviar las solicitudes de ARP y los pings.

a. Luego de que los switches se vuelven a cargar y las luces de enlace vuelven a ponerse en verde, la red está lista para enviar su tráfico ARP y ping.

b. Seleccione **Scenario 0** en la ficha desplegable para volver a la situación 0.

c. En el modo **Simulation (Simulación)**, haga clic en **Capture/Forward** para continuar con el proceso. Observe que los switches ahora envían las solicitudes ARP a todos los puertos, excepto al puerto en el que se recibió la petición ARP. Esta acción predeterminada de los switches es la razón por la que las VLAN pueden mejorar el rendimiento de la red. El tráfico de difusión se encuentra dentro de cada VLAN. Cuando aparezca la ventana **Buffer Full** (Búfer lleno), haga clic en el botón **View Previous Events** (Ver eventos anteriores).

Parte 3: completar las preguntas de reflexión

1. Si una computadora en la VLAN 10 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todos los dispositivos que están en la VLAN 10.
2. Si una computadora en la VLAN 20 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todos los dispositivos que están en la VLAN 20.
3. Si una computadora en la VLAN 30 envía un mensaje de difusión, ¿qué dispositivos lo reciben? Todos los dispositivos que están en la VLAN 30.
4. ¿Qué le sucede a una trama enviada desde una computadora en la VLAN 10 hacia una computadora en la VLAN 30? Lo descarta.
5. Desde el punto de vista de los puertos, ¿cuáles son los dominios de colisiones en el switch? Cada puerto es un dominio de colisiones diferente.
6. Desde el punto de vista de los puertos, ¿cuáles son los dominios de difusión en el switch? Se dividen por la cantidad de VLAN en el switch.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: observar el tráfico de difusión en una implementación de VLAN	Paso 1d	6	
	Paso 1e	5	
	Paso 2c	6	
	Paso 2d	5	
	Total de la parte 1	**22**	
Parte 2: observar el tráfico de difusión sin VLAN	Paso 1b	6	
	Paso 1c	6	
	Paso 1d	6	
	Total de la parte 2	**18**	
Parte 3: completar las preguntas de reflexión	1	10	
	2	10	
	3	10	
	4	10	
	5	10	
	6	10	
	Total de la parte 3	**60**	
	Puntuación total	**100**	

Packet Tracer: configuración de redes VLAN (versión para el instructor)

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

Topología

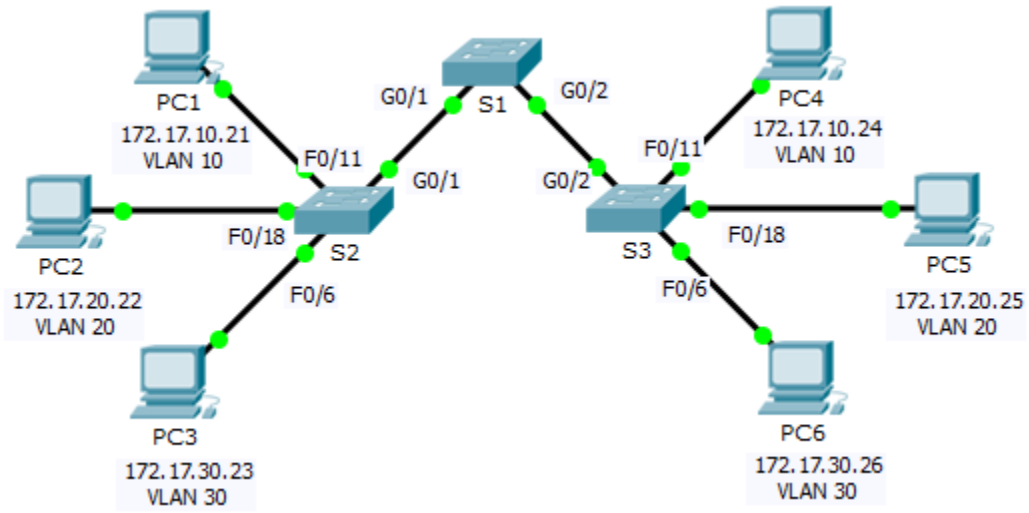


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Objetivos

Parte 1: verificar la configuración de VLAN predeterminada

Parte 2: configurar las VLAN

Parte 3: asignar las VLAN a los puertos

Información básica

Las VLAN son útiles para la administración de grupos lógicos y permiten mover, cambiar o agregar fácilmente a los miembros de un grupo. Esta actividad se centra en la creación y la denominación de redes VLAN, así como en la asignación de puertos de acceso a VLAN específicas.

Parte 1: Visualizar la configuración de VLAN predeterminada

Paso 1: mostrar las VLAN actuales.

En el S1, emita el comando que muestra todas las VLAN configuradas. Todas las interfaces están asignadas a la VLAN 1 de forma predeterminada.

Paso 2: verificar la conectividad entre dos computadoras en la misma red.

Observe que cada computadora puede hacer ping a otra que comparta la misma red.

- PC1 puede hacer ping a PC4
- PC2 puede hacer ping a PC5
- PC3 puede hacer ping a PC6

Los pings a las PC de otras redes fallan.

¿Qué beneficios proporciona configurar las VLAN a la configuración actual? Los principales beneficios de usar VLAN son seguridad, reducción de costos, mayor rendimiento, mitigación de las tormentas de difusión, aumento de la eficiencia del personal de TI y simplificación de la administración de proyectos y aplicaciones.

Parte 2: Configurar las VLAN

Paso 1: crear y nombrar las VLAN en el S1.

Cree las siguientes VLAN. Los nombres distinguen mayúsculas de minúsculas.

- VLAN 10: Cuerpo docente/Personal
- VLAN 20: Estudiantes
- VLAN 30: Invitado (predeterminada)
- VLAN 99: Administración y Nativa

```
S1#(config)# vlan 10
S1#(config-vlan)# name Faculty/Staff
S1#(config-vlan)# vlan 20
S1#(config-vlan)# name Students
S1#(config-vlan)# vlan 30
S1#(config-vlan)# name Guest(Default)
S1#(config-vlan)# vlan 99
S1#(config-vlan)# name Management&Native
```

Paso 2: verificar la configuración de la VLAN.

¿Con qué comando se muestran solamente el nombre y el estado de la VLAN y los puertos asociados en un switch?

```
S1# show vlan brief
```

Paso 3: crear las VLAN en el S2 y el S3.

Con los mismos comandos del paso 1, cree y nombre las mismas VLAN en el S2 y el S3.

Paso 4: verificar la configuración de la VLAN.

Parte 3: Asignar VLAN a los puertos

Paso 1: asignar las VLAN a los puertos activos en el S2.

Asigne las VLAN a los siguientes puertos:

- VLAN 10: Fast Ethernet 0/11
- VLAN 20: Fast Ethernet 0/18
- VLAN 30: Fast Ethernet 0/6

```
S2(config)# interface fa0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface fa0/18
S2(config-if)# switchport access vlan 20
S2(config-if)# interface fa0/6
S2(config-if)# switchport access vlan 30
```

Paso 2: Asigne VLAN a los puertos activos en S3.

El S3 utiliza las mismas asignaciones de puertos de acceso de VLAN que el S2.

Paso 3: verificar la pérdida de conectividad.

Anteriormente, las PC que compartían la misma red podían hacer ping entre sí con éxito. Intente hacer ping entre PC1 y PC4. Si bien los puertos de acceso están asignados a las VLAN adecuadas, ¿los pings se realizaron correctamente? ¿Por qué? No, los pings fallaron porque los puertos entre los switches se encuentran en la VLAN 1, y tanto la PC1 como la PC4 están en la VLAN 10.

¿Qué podría hacerse para resolver este problema? Configurar los puertos entre los switches como puertos de enlace troncal.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: verificar la configuración de VLAN predeterminada	Paso 2	**4**	
Parte 2: configurar las VLAN	Paso 2	**2**	
Parte 3: asignar las VLAN a los puertos	Paso 3	**4**	
Puntuación de Packet Tracer		**90**	
Puntuación total		**100**	

Packet Tracer: configuración de enlaces troncales (versión para el instructor)

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

Topología

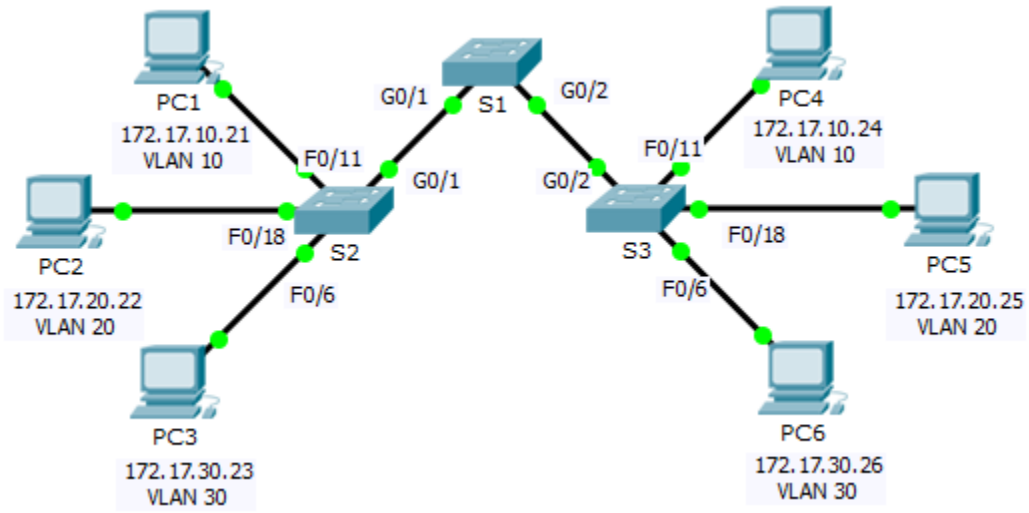


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerto del switch	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S1 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S1 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S1 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S2 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S2 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S2 F0/6	30

Objetivos

Parte 1: verificar las VLAN

Parte 2: configurar enlaces troncales

Información básica

Se requieren enlaces troncales para transmitir información de VLAN entre switches. Un puerto de un switch es un puerto de acceso o un puerto de enlace troncal. Los puertos de acceso transportan el tráfico de una VLAN específica asignada al puerto. Un puerto de enlace troncal pertenece a todas las VLAN de manera predeterminada; por lo tanto, transporta el tráfico para todas las VLAN. Esta actividad se centra en la creación de puertos de enlace troncal y en la asignación a una VLAN nativa distinta de la predeterminada.

Parte 1: verificar las VLAN

Paso 1: mostrar las VLAN actuales.

a. En el **S1**, emita el comando que muestra todas las VLAN configuradas. Debe haber nueve VLAN en total. Observe de qué manera los 26 puertos del switch se asignan a un puerto o a otro.

b. En el **S2** y el **S3**, muestre la información y verifique que todas las VLAN estén configuradas y asignadas a los puertos de switch adecuados según la **tabla de direccionamiento**.

Paso 2: verificar la pérdida de conectividad entre dos computadoras en la misma red.

Aunque la **PC1** y la **PC4** estén en la misma red, no pueden hacer ping entre sí. Esto es porque los puertos que conectan los switches se asignaron a la VLAN 1 de manera predeterminada. Para proporcionar conectividad entre las computadoras en la misma red y VLAN, se deben configurar enlaces troncales.

Parte 2: configurar los enlaces troncales

Paso 1: configurar el enlace troncal en el S1 y utilizar la VLAN 99 como VLAN nativa.

a. Configure las interfaces G0/1 y G0/2 en el S1 para el uso de enlaces troncales.

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

b. Configure la VLAN 99 como VLAN nativa para las interfaces G0/1 y G0/2 en el **S1**.

```
S1(config-if)# switchport trunk native vlan 99
```

El puerto de enlace troncal demora aproximadamente un minuto en activarse debido al árbol de expansión, sobre lo que aprenderá en los próximos capítulos. Haga clic en **Fast Forward Time (Adelantar el tiempo)** para acelerar el proceso. Una vez que los puertos se activan, recibirá de forma periódica los siguientes mensajes de syslog:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2
(99), with S3 GigabitEthernet0/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(99), with S2 GigabitEthernet0/1 (1).
```

Configuró la VLAN 99 como VLAN nativa en el S1. Sin embargo, y según lo indicado por el mensaje de syslog, el S2 y el S3 utilizan la VLAN 1 como VLAN nativa predeterminada.

Si bien hay una incompatibilidad de VLAN nativa, los pings entre las computadoras de la misma VLAN ahora se realizan de forma correcta. ¿Por qué? Los pings se realizan correctamente porque los enlaces troncales se habilitaron en S1. El protocolo de enlace troncal dinámico (DTP) negoció automáticamente el otro lado de los enlaces troncales. En este caso, S2 y S3 ahora han configurado automáticamente los puertos conectados a S1 como puertos de enlaces troncales.

Paso 2: verificar que el enlace troncal esté habilitado en el S2 y el S3.

En el **S2** y el **S3**, emita el comando **show interface trunk** para confirmar que el DTP haya negociado de forma correcta el enlace troncal con el S1 en el S2 y el S3. El resultado también muestra información sobre las interfaces troncales en el S2 y el S3.

¿Qué VLAN activas se permiten a través del enlace troncal? 1, 10, 20, 30 y 99.

Paso 3: corregir la incompatibilidad de VLAN nativa en el S2 y el S3.

a. Configure la VLAN 99 como VLAN nativa para las interfaces apropiadas en el S2 y el S3.

b. Emita el comando **show interface trunk** para verificar que la configuración de la VLAN sea correcta.

Paso 4: verificar las configuraciones del S2 y el S3.

a. Emita el comando **show interface** *interfaz* **switchport** para verificar que la VLAN nativa ahora sea 99.

b. Emita el comando **show vlan** para mostrar información acerca de las VLAN configuradas. ¿Por qué el puerto G0/1 en el S2 ya no está asignado a la VLAN 1? El puerto G0/1 es un puerto de enlace troncal, y este tipo de puertos no se muestran.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 80 puntos. Las tres preguntas de los pasos 1, 2 y 4 valen 20 puntos.

Packet Tracer: resolución de problemas de implementación de VLAN, situación 1 (versión para el instructor)

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

Topología

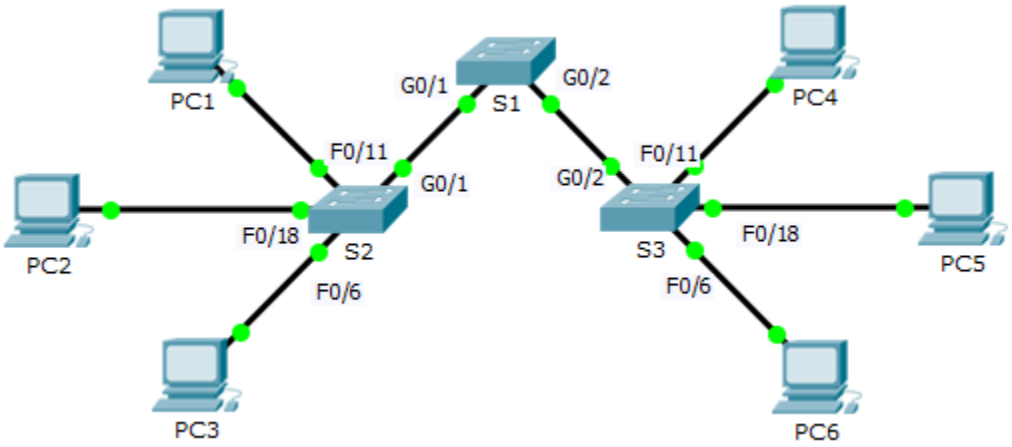


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Puerto del switch	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S1 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S1 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S1 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S2 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S2 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S2 F0/6	30

Objetivos

Parte 1: probar la conectividad entre las computadoras en la misma VLAN

Parte 2: investigar los problemas de conectividad por medio de la recopilación de datos

Parte 3: implementar la solución y probar la conectividad

Situación

En esta actividad, se efectúa la resolución de problemas de conectividad entre las PC de la misma VLAN. La actividad finaliza cuando las computadoras en la misma VLAN pueden hacer ping entre sí. Cualquier solución que implemente debe cumplir con la tabla de direccionamiento.

Parte 1: Probar la conectividad entre las PC de la misma VLAN

En el símbolo del sistema de cada computadora, haga ping entre las computadoras en la misma VLAN.

a. ¿Puede PC1 hacer ping a PC4? No

b. ¿Puede PC2 hacer ping a PC5? No

c. ¿Puede PC3 hacer ping a PC6? No

Parte 2: investigar los problemas de conectividad por medio de la recopilación de datos

Paso 1: verificar la configuración en las computadoras.

Verifique si las siguientes configuraciones para cada computadora son correctas.

- Dirección IP
- Máscara de subred

Paso 2: verificar la configuración en los switches.

Verifique si las siguientes configuraciones en los switches son correctas.

- Los puertos están asignados a las VLAN correctas.
- Los puertos se configuraron para el modo correcto.
- Los puertos están conectados a los dispositivos correctos.

Paso 3: registrar el problema y las soluciones.

Enumere los problemas y las soluciones que permitirán que estas computadoras hagan ping entre sí. Recuerde que podría haber más de un problema o más de una solución.

PC1 a PC4

a. Explique los problemas de conectividad entre la PC1 y la PC4. La PC1 está en la VLAN 30 en lugar de en la VLAN 10. El puerto G0/1 en el S1 está configurado como un puerto de acceso.

b. Registre las acciones necesarias para corregir los problemas. Emitir el comando **switchport access vlan 10** en la interfaz F0/11 del S2. Emitir el comando **switchport mode trunk** en la interfaz G0/1 del S1 y el S2.

PC2 a PC5

c. Explique los problemas de conectividad entre la PC2 y la PC5. La PC5 está conectada al puerto incorrecto, y F0/18 se asignó a la VLAN incorrecta.

d. Registre las acciones necesarias para corregir los problemas. Mover la PC5 de F0/17 a F0/18 en el S3 y asignar F0/18 a la VLAN 20. Emitir el comando **switchport mode trunk** en la interfaz G0/1 del S1 y el S2.

PC3 a PC6

e. ¿Cuáles son las razones por las que la conectividad falló entre las PC? La dirección IP de la PC6 está configurada de forma incorrecta. La interfaz G0/1 del S1 está configurada en modo de acceso. El puerto F0/6 en el S3 no está asignado a una VLAN.

f. Registre las acciones necesarias para corregir los problemas. Configurar la dirección IP de la PC6 para que sea 172.17.30.26. Emitir el comando **switchport mode trunk** en la interfaz G0/1 del S1 y el S2. Asignar el puerto F0/6 del S3 a la VLAN 30.

Parte 3: Implementar la solución y probar la conectividad

Verifique que las computadoras en la misma VLAN ahora puedan hacer ping entre sí. De lo contrario, continúe con el proceso de resolución de problemas.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 70 puntos. El registro realizado en el paso 2 de la parte 3 vale 30 puntos.

Packet Tracer: resolución de problemas de implementación de VLAN, situación 2 (versión para el instructor)

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

Topología

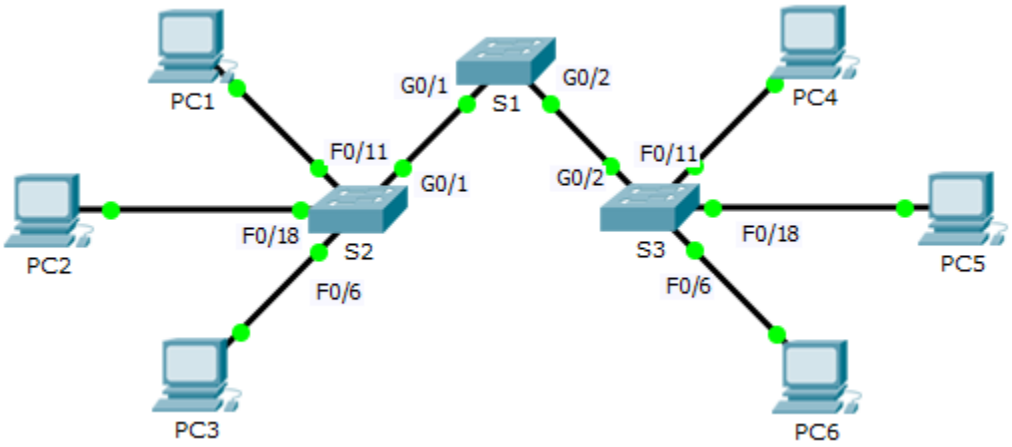


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
S1	VLAN 56	192.168.56.11	255.255.255.0	No aplicable
S2	VLAN 56	192.168.56.12	255.255.255.0	No aplicable
S3	VLAN 56	192.168.56.13	255.255.255.0	No aplicable
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

Asignación de VLAN y de puertos

Puertos	Número y nombre de VLAN	Red
F0/1–F0/5	VLAN 56 – Administración y Nativa	192.168.56.0/24
F0/6–F0/10	VLAN 30 – Invitado(Predeterminado)	192.168.30.0/24
F0/11–F0/17	VLAN 10 – Cuerpo docente/Personal	192.168.10.0/24

F0/18–F0/24	VLAN 20 – Students	192.168.20.0/24

Objetivos

Parte 1: identificar y corregir los errores de red

Parte 2: registrar las correcciones realizadas a la red

Parte 3: implementar soluciones y probar la conectividad

Información básica

En esta actividad, deberá llevar a cabo la resolución de problemas de un entorno VLAN mal configurado. La red inicial tiene errores. Su objetivo es localizar y corregir los errores en la configuración y establecer la conectividad de extremo a extremo. La configuración final debe coincidir con el diagrama de topología y con la tabla de direccionamiento. La VLAN nativa para esta topología es la VLAN 56.

Parte 1: detectar y registrar los problemas en la red

Utilice la topología, la tabla de direccionamiento, la tabla de asignación de VLAN y de puertos, y su conocimiento acerca de VLAN y enlaces troncales para detectar problemas en la red. Complete la tabla de **documentación** con los problemas que detectó y las posibles soluciones.

Documentación

Problemas	Soluciones
El puerto G0/1 en el S2 está configurado como puerto de acceso en lugar de como puerto de enlace troncal.	Implementar el comando **switchport mode trunk**.
El S1 no está configurado con ninguna VLAN, solo con enlaces troncales.	Utilizar los comandos necesarios en el S1 para configurar las VLAN y establecer la VLAN nativa en los enlaces troncales.
Los puertos del S3 no están asignados a una VLAN.	Emitir el comando **switchport access vlan #** según la tabla de asignación de puertos.
Hay una incompatibilidad de VLAN nativa.	Configurar los puertos de enlace troncal en el S1 en la VLAN 56 nativa.

Parte 2: Implementar la solución y probar la conectividad

Verifique que las computadoras en la misma VLAN ahora puedan hacer ping entre sí. De lo contrario, continúe con el proceso de resolución de problemas.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 70 puntos. El registro realizado en el paso 2 de la parte 3 vale 30 puntos.

```
!S1!!!!!!!!!!!!
en
conf t
vlan 56
name Management&Native
vlan 30
name Guest(Default)
vlan 10
name Faculty/Staff
vlan 20
name Students
int range g0/1 - 2
switchport trunk native vlan 56

!S2!!!!!!!!!!!!!!
en
conf t
int g0/1
switchport mode trunk

!S3!!!!!!!!!!!!!!!
en
conf t
int range fa0/1 - 5
switchport access vlan 56
int range fa0/6 - 10
switchport access vlan 30
int range fa0/11 - 17
switchport access vlan 10
int range fa0/18 - 24
switchport access vlan 20
```

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

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

Topología

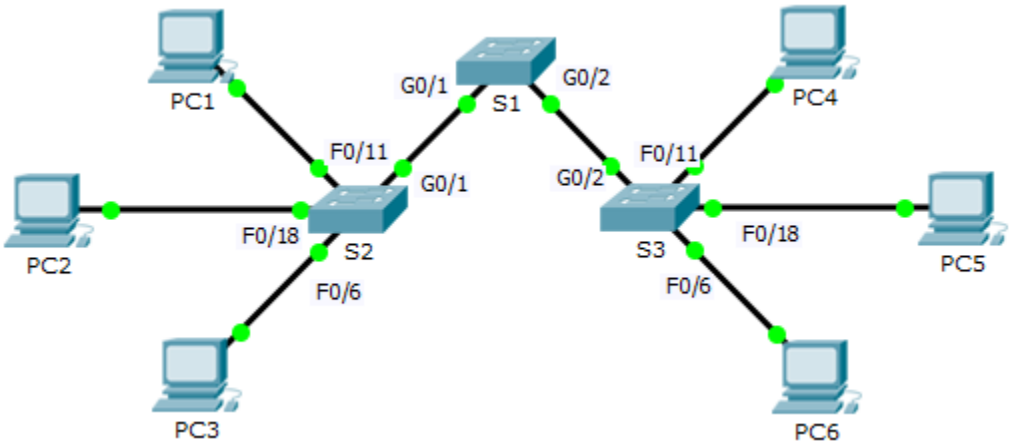


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 88	172.31.88.2	255.255.255.0	172.31.88.1
S2	VLAN 88	172.31.88.3	255.255.255.0	172.31.88.1
S3	VLAN 88	172.31.88.4	255.255.255.0	172.31.88.1
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.1
PC4	NIC	172.31.10.24	255.255.255.0	172.31.10.1
PC5	NIC	172.31.20.25	255.255.255.0	172.31.20.1
PC6	NIC	172.31.30.26	255.255.255.0	172.31.30.1

Tabla de asignación de VLAN y de puertos

Puertos	Asignaciones	Red
F0/7-12	VLAN 10: Ventas	172.31.10.0/24
F0/13-20	VLAN 20: Producción	172.31.20.0/24
F0/1-6	VLAN 30: Marketing	172.31.30.0/24
Interfaz VLAN 88	VLAN 88: Administración	172.31.88.0/24
Enlaces troncales	VLAN 99: Nativa	N/A

Situación

En esta actividad, hay dos switches completamente configurados. Usted es responsable de asignar el direccionamiento IP a una interfaz virtual de switch, configurar las VLAN, asignar las VLAN a las interfaces, configurar enlaces troncales e implementar medidas de seguridad básicas en un tercer switch.

Requisitos

El **S1** y **S2** están totalmente configurados. No puede acceder a esos switches. Usted es responsable de configurar el **S3** con los siguientes requisitos:

- Configure el direccionamiento IP y el gateway predeterminado según la **tabla de direccionamiento**.
- Cree, nombre y asigne las VLAN según la **tabla de asignación de VLAN y de puertos**.
- Asigne la VLAN 99 nativa al puerto de enlace troncal y deshabilite DTP.
- Restrinja el enlace troncal para que solo permita las VLAN 10, 20, 30, 88 y 99.
- Utilice la VLAN 99 como VLAN nativa en los puertos de enlace troncal.
- Configure la seguridad básica del switch en el S1.
  - Utilice la contraseña secreta cifrada **itsasecret.**
  - Utilice la contraseña de consola **letmein.**
  - Utilice la contraseña de VTY **c1$c0** (donde 0 es el número cero).
  - Cifre las contraseñas de texto no cifrado.
  - El mensaje MOTD debe tener el texto **Authorized Access Only!!** (¡Acceso autorizado únicamente!).
  - Deshabilitar los puertos que no se utilicen.
- Configure la seguridad de puertos en **F0/6**.
  - Solo dos dispositivos únicos tienen permitido acceder el puerto.
  - Las MAC detectadas se agregan a la configuración en ejecución.
  - Proteja la interfaz de manera que se envíe una notificación cuando se produzca una infracción, pero que el puerto no se deshabilite.
- Verifique que las computadoras en la misma VLAN ahora puedan hacer ping entre sí.

```
!S3!!!!!!!!!!!!!!
en
conf t
interface vlan 88
```



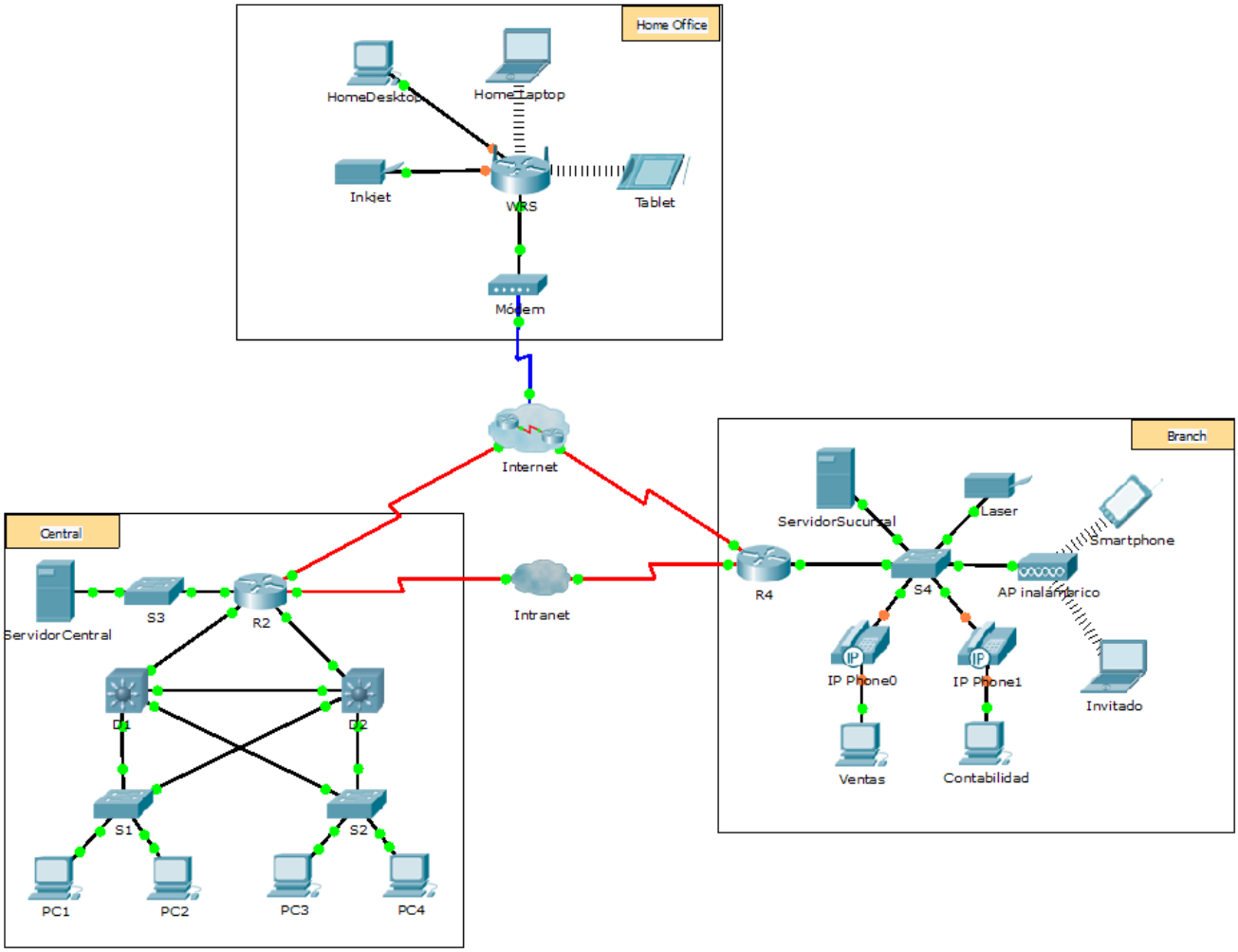
```
ip address 172.31.88.4 255.255.255.0
no shutdown
ip default-gateway 172.31.88.1
!VLAN names are accepted as long as the first 3 letters are correct
vlan 10
name Sales
vlan 20
name Production
vlan 30
name Marketing
vlan 88
name Management
vlan 99
name Native
!Ports Fa0/6, Fa0/11 and Fa0/18 are checked for VLAN assignment
interface range fa0/7 - 12
switchport mode access
switchport access vlan 10
interface range fa0/13 - 20
switchport mode access
switchport access vlan 20
interface range fa0/1 - 6
 switchport mode access
 switchport access vlan 30
interface g0/2
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,88,99
 switchport mode trunk
 switchport nonegotiate
enable secret itsasecret
line console 0
password letmein
login
line vty 0 15
password c1$c0
login
service password-encryption
!Only the first 3 letters of the word 'Access' in banner text are checked
banner motd $Authorized Access Only!!$
int fa0/6
```

```
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!Ports fa0/4, fa0/14 and fa0/24 are checked for shutdown
interface range fa0/1 - 5, fa0/7 - 10, fa0/12 - 17, fa0/19 - 24, g0/1
 shutdown
```

Packet Tracer: uso de traceroute para detectar la red (versión para el instructor)

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

Topología



Situación

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

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

Rastreo y registro de una ubicación remota

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

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

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

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

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

¿Qué dirección devolvió el comando para **b2server**? 128.107.64.254

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

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

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

```
PC> telnet 172.16.0.1
```

e. Ya está conectado al router **R4**. Emita el comando **traceroute** en el router con la dirección de b2server determinada en el punto b. ¿Qué diferencia hay entre el comando **traceroute** en el router y el comando **tracert** en la computadora? Hay un salto menos, dado que el comando se origina en el R4, y el orden de los campos en el resultado es diferente, ya que la dirección IP aparece en la primera columna.

¿Cuál es la importancia del **R4** para **Sales**? Es el gateway predeterminado de Sales.

f. Use el comando **show ip interface brief** para mostrar el estado de las interfaces en el **R4**. Según el resultado del comando, ¿qué interfaz se utiliza para llegar al siguiente dispositivo en la lista de resultados del comando **tracert**? La interfaz S0/0/0 está conectada a la red 64.100.150.0.

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

g. Acceda a la segunda dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. Puede utilizar el número en la columna del extremo izquierdo del resultado del comando **tracert** para seguir su recorrido por la lista. ¿Cuál es el nombre del dispositivo al que está conectado? Nivel3a

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

i. Según el resultado del comando **show ip route**, ¿cuál es la interfaz de salida de la siguiente dirección IP que se indica en el resultado original del comando **tracert**? GigabitEthernet0/0

j. Acceda a la tercera dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. ¿Cuál es el nombre de host del dispositivo actual? ISP-Nivel3b

Emita el comando **show ip route connected**. ¿Cuáles son las redes conectadas directamente a este router? 64.100.8.0/24, 64.104.222.0/30, 64.104.222.4/30, 128.107.46.0/24

Consulte la tabla de **registro del esquema de direccionamiento**. ¿Qué interfaces conectan los dispositivos entre trace route 2 y trace route 3? GigabitEthernet 0/0 para ISP-Nivel3a y GigabitEthernet0/1 para ISP-Nivel3B

k. Acceda a la cuarta dirección IP de la lista de **tracert** mediante Telnet e inicie sesión. ¿Cuál es el nombre del dispositivo? B2-R1

l. Emita un comando para determinar a qué interfaz está conectado **b2server.pt.pka**. El estudiante puede usar el comando show ip route, show ip interface brief o show run.

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

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

Registro del esquema de direccionamiento

ID de trace route	Dispositivo	Interfaz	Dirección	Máscara de subred
-	Ventas	NIC	172.16.0.x (DHCP)	255.255.255.0
1	R4	G0/0	172.16.0.1	255.255.255.0
		S0/0/0	64.100.150.1	255.255.255.252
		S0/0/1.1	64.100.200.1	255.255.255.252
2	ISP-Nivel3a	G0/0	64.104.222.1	255.255.255.252
		G0/1	64.104.223.1	255.255.255.252
		S0/0/0	64.100.100.2	255.255.255.252
		S0/1/0	64.100.150.2	255.255.255.252
3	ISP-Nivel3b	G0/1	64.104.222.2	255.255.255.252
		G0/2	64.100.8.1	255.255.255.0
		F0/1	128.107.46.1	255.255.255.0
		F/0/2	64.104.222.5	255.255.255.252
4	B2-R1	G0/0	64.104.222.6	255.255.255.252
		G0/1	128.107.64.1	255.255.255.0
5	b2server.pt.pka	NIC	128.107.64.254	255.255.255.0

Registro de la topología

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

Solo para el instructor: topología de Sucursal2

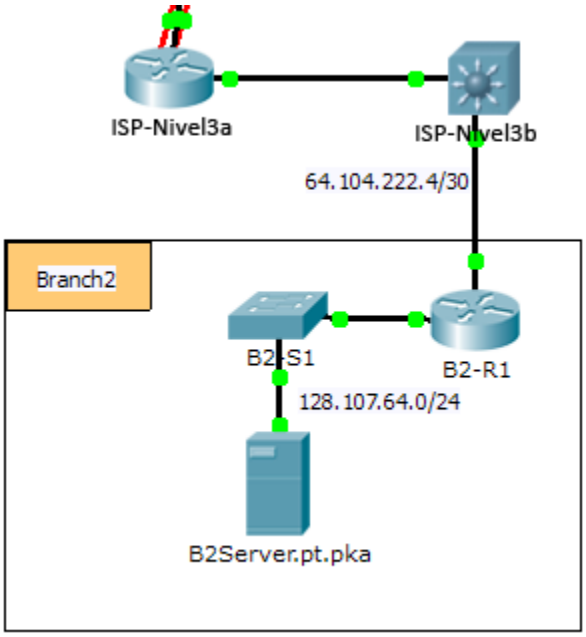


Tabla de calificación sugerida

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

Sugerencias: referencia resumida de comandos

Comandos de DOS

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

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

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

Sintaxis:

nslookup dns.name

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

Sintaxis:

tracert [NombreDestino/Dirección IP]

Comandos del IOS

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

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

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

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

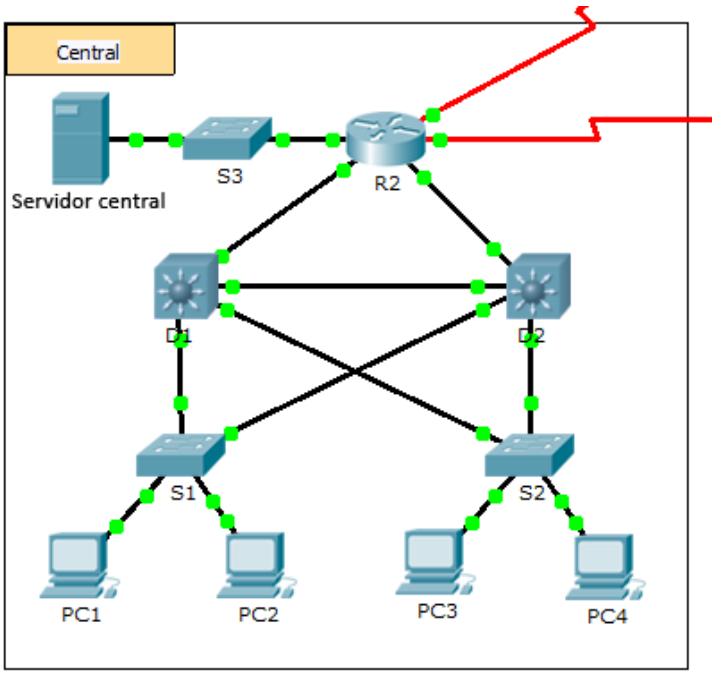
show running-config: el resultado de este comando muestra la configuración operativa actual.

traceroute: rastrea la ruta al destino.

Packet Tracer: registro de la red (versión para el instructor)

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

Topología



Información básica

En esta actividad, su trabajo es registrar el esquema de direccionamiento y las conexiones que se usan en la porción Central de la red. Debe utilizar una variedad de comandos para recopilar la información requerida.

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

Requisitos

- Acceda a la línea de comandos de los diversos dispositivos en la porción Central de la red.
- Utilice comandos para recopilar la información requerida en la tabla **Registro del esquema de direccionamiento y conexiones de dispositivos**.
- Si no recuerda los comandos necesarios, puede utilizar el sistema de ayuda incorporado del IOS.
- Si aún necesita más ayuda, consulte la página de **Sugerencias**. En Packet Tracer, haga clic en la flecha derecha (>) que se encuentra en el sector inferior derecho de la ventana de instrucciones. Si tiene una versión impresa de las instrucciones, la página de **Sugerencias** es la última.

Registro del esquema de direccionamiento y conexiones de dispositivos

Nombre del dispositivo	Interfaz	Dirección	Máscara de subred	Dispositivo de conexión	
				Nombre del dispositivo	Interfaz
R2	G0/0	10.255.255.245	255.255.255.252	D1	G0/1
	G0/1	10.255.255.249	255.255.255.252	D2	G0/1
	G0/2	10.10.10.1	255.255.255.0	S3	G0/1
	S0/0/0	64.100.100.1	255.255.255.252	Internet	N/A
	S0/0/1.1	64.100.200.2	255.255.255.252	Intranet	N/A
S3	VLAN 1	10.10.10.254	255.255.255.0	N/A	N/A
	F0/1	N/A	N/A	CentralServer	NIC
	G0/1	N/A	N/A	R2	G0/2
CentralServer	NIC	10.10.10.2	255.255.255.0	S3	F0/1
D1	VLAN2	10.2.0.1	255.255.255.0	N/A	N/A
	G0/1	10.255.255.246	255.255.255.252	R2	G0/0
	G0/2	10.255.255.254	255.255.255.252	D2	G0/2
	F0/23	N/A	N/A	S2	F0/23
	F0/24	N/A	N/A	S1	G0/1
S1	VLAN 2	10.2.0.2	255.255.255.0	N/A	N/A
	F0/23	N/A	N/A	D2	F0/23
	G0/1	N/A	N/A	D1	F0/24
D2	F0/23	N/A	N/A	S1	F0/23
	F0/24	10.3.0.1	255.255.255.0	S3	G0/1
	G0/1	10.255.255.250	255.255.255.252	R2	G0/1
	G0/2	10.255.255.253	255.255.255.252	D1	G0/2
S2	VLAN 1	10.3.0.2	255.255.255.0	N/A	N/A
	F0/23	N/A	N/A	D1	F0/23
	G0/1	N/A	N/A	D2	F0/24

Sugerencias

Utilice los siguientes comandos para recopilar la información que necesita para registrar la red:

```
show ip interface brief
show interfaces
show running-config
ipconfig
```

Packet Tracer: configuración de interfaces IPv4 e IPv6 (versión para el instructor)

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

Topología

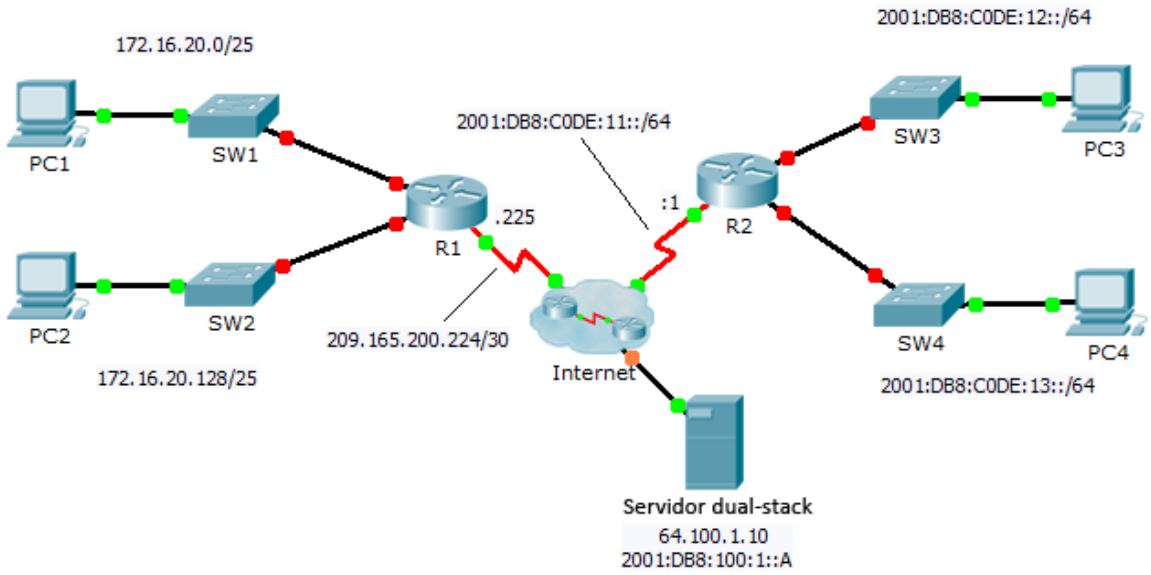


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	172.16.20.1	255.255.255.128	N/A
	G0/1	172.16.20.129	255.255.255.128	N/A
	S0/0/0	209.165.200.225	255.255.255.252	N/A
PC1	NIC	172.16.20.10	255.255.255.128	172.16.20.1
PC2	NIC	172.16.20.138	255.255.255.128	172.16.20.129
R2	G0/0	2001:DB8:C0DE:12::1/64		N/A
	G0/1	2001:DB8:C0DE:13::1/64		N/A
	S0/0/1	2001:DB8:C0DE:11::1/64		N/A
	Link-local	FE80::2		N/A
PC3	NIC	2001:DB8:C0DE:12::A/64		FE80::2
PC4	NIC	2001:DB8:C0DE:13::A/64		FE80::2

Objetivos

Parte 1: configurar el direccionamiento IPv4 y verificar la conectividad

Parte 2: configurar el direccionamiento IPv6 y verificar la conectividad

Información básica

Los routers R1 y R2 tienen dos LAN cada uno. Su tarea es configurar el direccionamiento adecuado en cada dispositivo y verificar la conectividad entre las LAN.

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

Parte 1: configurar el direccionamiento IPv4 y verificar la conectividad

Paso 1: asignar direcciones IPv4 al R1 y a los dispositivos en la LAN.

Consulte la **tabla de direccionamiento** para configurar el direccionamiento IP de las interfaces LAN del **R1**, la **PC1** y la **PC2**. La interfaz serial ya está configurada.

Paso 2: Verifique la conectividad.

La **PC1** y la **PC2** deberían poder hacer ping entre sí y al **servidor dual-stack**.

Parte 2: configurar el direccionamiento IPv6 y verificar la conectividad

Paso 1: asignar direcciones IPv6 al R2 y a los dispositivos en la LAN.

Consulte la **tabla de direccionamiento** para configurar el direccionamiento IP de las interfaces LAN del **R2**, la **PC3** y la **PC4**. La interfaz serial ya está configurada.

Paso 2: Verifique la conectividad.

La **PC3** y la **PC4** deberían poder hacer ping entre sí y al **servidor dual-stack**.

Packet Tracer: configuración y verificación de una red pequeña (versión para el instructor)

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

Topología

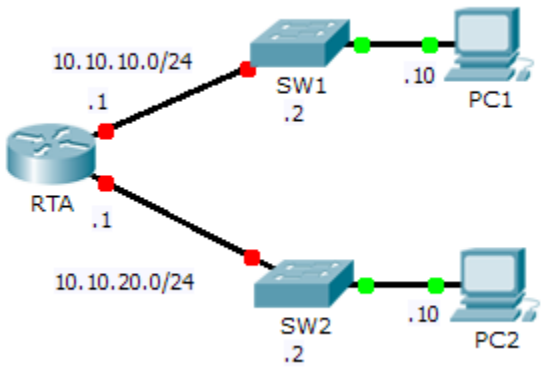


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
	G0/1	10.10.20.1	255.255.255.0	N/A
SW1	VLAN1	10.10.10.2	255.255.255.0	10.10.10.1
SW2	VLAN1	10.10.20.2	255.255.255.0	10.10.20.1
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC2	NIC	10.10.20.10	255.255.255.0	10.10.20.1

Objetivos

Parte 1: configurar los dispositivos y verificar la conectividad

Parte 2: recopilar información con los comandos show

Información básica

En esta actividad, configurará el **RTA** con los parámetros básicos, incluido el direccionamiento IP. También configurará el SW1 para la administración remota y configurará las computadoras. Una vez que verificó correctamente la conectividad, utilizará los comandos **show** para recopilar información acerca de la red.

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

Parte 1: Configurar dispositivos y verificar la conectividad

Paso 1: aplicar las configuraciones básicas al RTA.

a. Utilice la siguiente información y la **tabla de direccionamiento** para configurar el RTA:
   - Nombre de host y aviso
   - Contraseña de líneas **cisco**; contraseña cifrada **class**
   - Direccionamiento IP y descripciones en las interfaces LAN

b. Guarde la configuración.

Paso 2: configurar el direccionamiento en la PC1 y la PC2.

a. Utilice la **tabla de direccionamiento** para configurar el direccionamiento IP de la PC1 y la PC2.

b. Pruebe la conectividad entre la **PC1** y la **PC2**. Resuelva cualquier problema que se presente.

Paso 3: configurar el SW1 para la administración remota.

a. Utilice la **tabla de direccionamiento** para configurar la interfaz de administración del SW1.

b. Configure la dirección de gateway predeterminado.

c. Guarde la configuración.

Parte 2: recopilar información con los comandos show

Paso 1: recopilar la información del resultado del comando show interface.

Emita cada uno de los siguientes comandos y, a continuación, responda las preguntas relacionadas:

```
show ip interface brief
show interfaces
show ip interface
```

¿Qué comandos muestran el estado del puerto? show ip interface brief, show interfaces, show ip interface

¿Con qué comando se muestra solo la dirección IP (sin la máscara de subred ni el prefijo)? show ip interface brief

¿Con qué comando se muestra la descripción configurada en la interfaz? show interfaces

¿Con qué comando se muestra la dirección IP de difusión? show ip interface

¿Con qué comando se muestra la dirección MAC de la interfaz? show interfaces

Paso 2: recopilar la información del resultado del comando show ip route.

Emita cada uno de los siguientes comandos y, a continuación, responda las preguntas relacionadas:

```
show ip route
show ip route connected
```

¿Cuántas redes conoce el router según el resultado del comando **show ip route**? 2: 10.10.10.0/24 y 10.10.20.0/24

¿Qué representa la **L** al comienzo de las líneas dentro de la tabla de routing? Conexión local

¿Qué indica el prefijo /32 incluido en la tabla de rutas? La dirección host de la interfaz

Paso 3: recopilar información después de modificar el estado de una interfaz.

a. En el **RTA**, desactive la interfaz Gigabit Ethernet 0/0 y emita el comando **show ip route**. ¿Cuántas redes se muestran en la tabla de routing ahora? 1: 10.10.20.0/24

b. Intente hacer ping a la PC1. ¿Elping fue exitoso? No

c. Emita el comando **show ip interface brief**. ¿Cuál es el estado de la interfaz Gigabit Ethernet 0/0? administratively down

d. Reactive la interfaz Gigabit Ethernet 0/0. Emita el comando **show ip route**. ¿Se volvió a completar la tabla de routing? Sí

¿Qué se puede deducir sobre el estado de la interfaz de las rutas que aparecen en la tabla de routing? Las interfaces deben estar activas para que se indiquen en la tabla de routing.

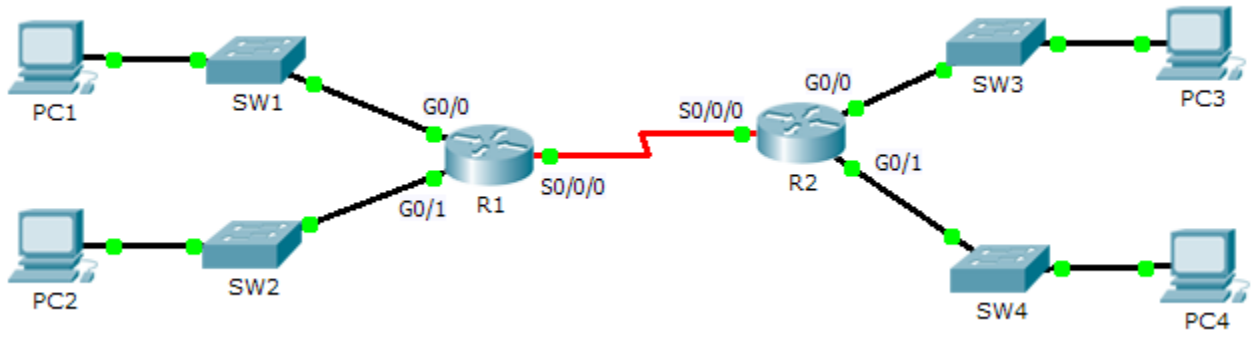
Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 2: recopilar información con los comandos show	Paso 1	15	
	Paso 2	10	
	Paso 3	15	
Total de la parte 2		**40**	
Puntuación de Packet Tracer		**60**	
Puntuación total		**100**	

Packet Tracer: investigación de rutas conectadas directamente (versión para el instructor)

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

Topología



Objetivos

Parte 1: investigar rutas IPv4 conectadas directamente

Parte 2: investigar rutas IPv6 conectadas directamente

Información básica

La red de la actividad ya está configurada. Iniciará sesión en los routers y utilizará los comandos **show** para detectar las rutas conectadas directamente y contestar las preguntas siguientes sobre estas.

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

Parte 1: investigar rutas IPv4 conectadas directamente

Paso 1: utilizar los comandos show para recopilar información sobre las redes IPv4 conectadas directamente.

Introduzca el siguiente comando en el **R1**:

```
R1> show ip route ?
```

a. ¿Qué opción sería la más ventajosa para determinar cuáles son las redes asignadas a las interfaces del router? Conectado

b. ¿Cuáles son las redes conectadas directamente en el **R1**? Sugerencia: utilice la opción indicada arriba.

```
C    172.31.20.0/23  is directly connected, GigabitEthernet0/0
C    172.31.22.0/23  is directly connected, GigabitEthernet0/1
C    209.165.200.224/30  is directly connected, Serial0/0/0
```

c. ¿Qué direcciones IP se asignaron a las interfaces LAN en el **R1**?

```
Interface              IP-Address      OK? Method Status                Protocol
 GigabitEthernet0/0     172.31.21.254   YES manual up                    up
 GigabitEthernet0/1     172.31.23.254   YES manual up                    up
```

d. Which networks are directly connected on **R2**?

```
C   172.31.24.0/24  is directly connected, GigabitEthernet0/0
C   172.31.25.0/24  is directly connected, GigabitEthernet0/1
C   209.165.200.224/30  is directly connected, Serial0/0/0
```

e. ¿Qué direcciones IP se asignaron a las interfaces LAN en el **R2**?

```
Interface              IP-Address      OK? Method Status                Protocol
 GigabitEthernet0/0     172.31.24.254   YES manual up                    up
 GigabitEthernet0/1     172.31.25.254   YES manual up                    up
```

Paso 2: verificar el direccionamiento de las computadoras y probar la conectividad.

a. Abra un símbolo del sistema en la **PC1**. Emita el comando para ver la configuración IP. Sobre la base del resultado, ¿cree que la **PC1** se podrá comunicar con todas las interfaces del router? Proporcione una respuesta breve que describa sus expectativas. La computadora tiene la dirección de gateway correcta, y el router enumera todas las redes conectadas en la tabla de routing.

b. Abra un símbolo del sistema en la **PC2**. Emita el comando para ver la configuración IP. Sobre la base del resultado, ¿cree que la **PC2** se podrá comunicar con la **PC1**? Verifique sus expectativas. El ping se realiza correctamente.

c. Determine las direcciones IP de la **PC3** y la **PC4**. Registre los resultados y determine si la **PC3** y la **PC4** se pueden comunicar. PC3: dirección IP 172.31.24.10, PC4: dirección IP 172.31.25.10.

d. Pruebe la conectividad de la **PC1** a la **PC3**. ¿La prueba se realizó correctamente? sí

e. **Pregunta adicional:** observe los resultados de las tablas de routing en el **R1** y el **R2**. ¿Qué elemento podría indicar el motivo por el cual la comunicación entre la **PC1** y la **PC3** se produce correctamente o no se produce? La ruta estática predeterminada 0.0.0.0/0.

Parte 2: investigar rutas IPv6 conectadas directamente

Paso 1: utilizar los comandos show para recopilar información sobre las redes IPv6 conectadas directamente.

a. ¿Qué redes IPv6 se encuentran disponibles en el **R1**?

```
C   2001:DB8:C001:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:C001:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:DB8:C001:2::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2001:DB8:C001:2::1/128 [0/0]
     via ::, GigabitEthernet0/1
C   2001:DB8:C001:ACE::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:C001:ACE::1/128 [0/0]
     via ::, Serial0/0/0
```

b. ¿Qué direcciones IPv6 de unidifusión se asignaron a las interfaces LAN en el **R1**?

```
L   2001:DB8:C001:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:C001:2::1/128 [0/0]
     via ::, GigabitEthernet0/1
```


c. ¿Qué redes IPv6 se encuentran disponibles en el R2?

```
C   2001:DB8:C001:3::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:C001:3::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:DB8:C001:4::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2001:DB8:C001:4::1/128 [0/0]
     via ::, GigabitEthernet0/1
C   2001:DB8:C001:ACE::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:C001:ACE::2/128 [0/0]
     via ::, Serial0/0/0
```

d. ¿Qué direcciones IPv6 se asignaron a las interfaces LAN en el **R2**?

```
L   2001:DB8:C001:3::1/128 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:C001:4::1/128 [0/0]
     via ::, GigabitEthernet0/1
```

Paso 2: verificar la configuración y la conectividad de la computadora.

a. Abra un símbolo del sistema en la **PC1**. Emita el comando para ver la configuración de IPv6. Sobre la base del resultado, ¿cree que la **PC1** se podrá comunicar con todas las interfaces del router? Proporcione una respuesta breve que describa sus expectativas. La computadora tiene la dirección de gateway correcta con la dirección link-local en el router, y este enumera todas las redes conectadas en la tabla de routing.

b. Abra un símbolo del sistema en la **PC2**. Emita el comando para ver la configuración de IPv6. Sobre la base del resultado, ¿cree que la **PC2** se podrá comunicar con la **PC1**? Verifique sus expectativas. El ping se realiza correctamente.

c. Determine las direcciones IPv6 de la **PC3** y la **PC4**. Registre los resultados y determine si la **PC3** y la **PC4** se pueden comunicar. PC3: dirección IP 2001:DB8:C001:3::10/64, PC4: dirección IP 2001:DB8:C001: 4::10/64

d. Pruebe la conectividad de la **PC1** a la **PC3**. ¿La prueba se realizó correctamente? sí

e. **Pregunta adicional:** ¿qué elemento podría indicar el motivo por el cual la comunicación entre la **PC1** y la **PC3** se produce correctamente o no se produce, luego de observar los resultados de las tablas de routing IPv6 en el **R1** y el **R2**? La ruta estática predeterminada IPv6.

```
S   ::/0 [1/0]
     via ::, Serial0/0/0
```


Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: investigar rutas IPv4 conectadas directamente	Paso 1	25	
	Paso 2	25	
Parte 2: investigar rutas IPv6 conectadas directamente	Paso 1	25	
	Paso 2	25	
	Puntuación total	**100**	

Packet Tracer: configuración de routing entre VLAN con router-on-a-stick (versión para el instructor)

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

Topología

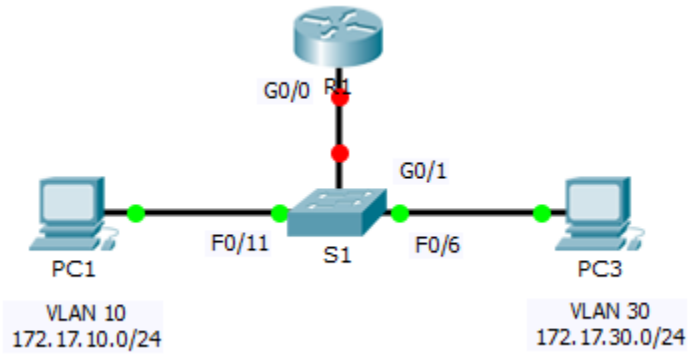


Tabla de direccionamiento

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

Objetivos

Parte 1: probar la conectividad sin routing entre VLAN

Parte 2: agregar VLAN a un switch

Parte 3: configurar subinterfaces

Parte 4: probar la conectividad con routing entre VLAN

Situación

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

Parte 1: Probar conectividad sin routing entre VLAN

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

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

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

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

b. Haga clic en **Capture/Forward** (Capturar/Adelantar) para ver los pasos que sigue el ping entre la **PC1** y la **PC3**. Observe que el ping nunca deja la **PC1**. ¿Qué proceso falló y por qué? Falló el proceso ARP porque la PC3 descartó la solicitud de ARP. La PC1 y la PC3 no están en la misma red, de modo que la PC1 nunca recibe la dirección MAC de la PC3. Sin una dirección MAC, la PC1 no puede crear una solicitud de eco ICMP.

Parte 2: agregar VLAN a un switch

Paso 1: crear VLAN en el S1.

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

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
```

Paso 2: Asignar VLAN a puertos.

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

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

```
S1(config-vlan)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# int fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 30
```

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

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active    Fa0/11
```



```
30   VLAN0030                         active    Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

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

En la **PC1**, haga ping a la **PC3**. Los pings deberían seguir fallando. ¿Por qué fallaron los pings? Cada VLAN es una red diferente y requiere un router o un switch de capa 3 que proporcione la comunicación entre ellas.

Parte 3: configurar subinterfaces

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

a. Cree la subinterfaz G0/0.10.

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

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

```
R1(config)# int g0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# int g0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
```

Paso 2: verificar la configuración.

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

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

Parte 4: probar la conectividad con routing entre VLAN

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

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

Paso 2: habilitar el enlace troncal.

a. En el **S1**, emita el comando **show vlan**. ¿A qué VLAN se asignó la interfaz G0/1? VLAN 1

b. Como el router se configuró con varias subinterfaces asignadas a diferentes VLAN, el puerto de switch que se conecta al router se debe configurar como enlace troncal. Habilite el enlace troncal en la interfaz G0/1.

```
S1(config-if)# int g0/1
S1(config-if)# switchport mode trunk
```


c. ¿Cómo puede determinar que la interfaz es un puerto de enlace troncal mediante el comando **show vlan**? La interfaz ya no figura en la VLAN 1.

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

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

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

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

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

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

Tabla de calificación sugerida

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

Packet Tracer: resolución de problemas de routing entre VLAN (versión para el instructor)

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

Topología

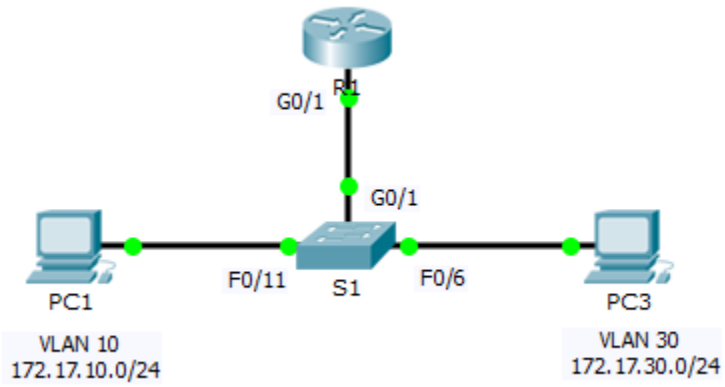


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	VLAN
R1	G0/1.10	172.17.10.1	255.255.255.0	N/A	VLAN 10
	G0/1.30	172.17.30.1	255.255.255.0	N/A	VLAN 30
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1	VLAN 10
PC3	NIC	172.17.30.10	255.255.255.0	172.17.30.1	VLAN 30

Objetivos

Parte 1: encontrar los problemas de red

Parte 2: implementar la solución

Parte 3: verificar la conectividad de red

Situación

En esta actividad, resolverá problemas de conectividad causados por configuraciones inadecuadas relacionadas con las VLAN y el routing entre VLAN.

Parte 1: encontrar los problemas de red

Examine la red y ubique el origen de cualquier problema de conectividad.

- Pruebe la conectividad y use los comandos **show** necesarios para verificar la configuración.
- Indique todos los problemas y las soluciones posibles en la **tabla de documentación**.

Tabla de documentación

Problemas	Soluciones
La interfaz física G0/1 está activa, pero la subinterfaz G0/1.10 está administrativamente inactiva.	Implementar el comando **no shutdown** para habilitar la subinterfaz G0/1.10.
La PC3 se configuró con la dirección de gateway predeterminado incorrecta.	Cambiar el gateway predeterminado en la PC3 de 172.17.10.1 a 172.17.30.1.
La interfaz G0/1 en el S1 se configuró como puerto de acceso en lugar de puerto de enlace troncal.	Utilizar el comando **switchport mode trunk** para que la interfaz pase del modo de acceso al modo de enlace troncal.
Se cambiaron las asignaciones de VLAN de las subinterfaces en el R1.	Emita el comando **no encapsulation dot1q** para eliminar la información incorrecta. Luego, configure las subinterfaces con el comando **encap dot1q <vlan>** correcto. Vuelva a introducir la información de dirección IP correcta.

Parte 2: implementar las soluciones

Realice cambios según las soluciones que recomendó.

Parte 3: Verificar la conectividad de la red

Verifique que las computadoras puedan hacer ping a las demás computadoras y al R1. Si no es así, continúe con la resolución de problemas hasta que los pings se realicen correctamente.

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 60 puntos. Completar la **tabla de documentación** vale 40 puntos.

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

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

Topología

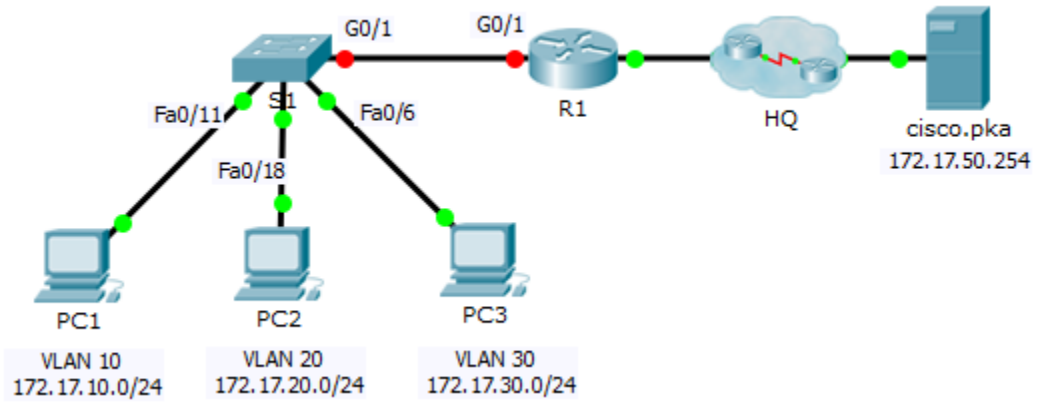


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.17.25.2	255.255.255.252	N/A
	G0/1.10	172.17.10.1	255.255.255.0	N/A
	G0/1.20	172.17.20.1	255.255.255.0	N/A
	G0/1.30	172.17.30.1	255.255.255.0	N/A
	G0/1.88	172.17.88.1	255.255.255.0	N/A
	G0/1.99	172.17.99.1	255.255.255.0	N/A
S1	VLAN 99	172.17.99.10	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

Tabla de asignación de VLAN y de puertos

VLAN	Nombre	Interfaz
10	Faculty/Staff	Fa0/11-17
20	Students	Fa0/18-24
30	Invitado (Predeterminada)	Fa0/6-10
88	Nativo	G0/1
99	Management	VLAN 99

Situación

En esta actividad, demostrará y reforzará su capacidad para implementar el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces.

Requisitos

- Asigne el direccionamiento IP al **R1** y al **S1** según la **tabla de direccionamiento**.
- Cree, nombre y asigne las VLAN en el **S1** según la **tabla de asignación de VLAN y de puertos**. Los puertos deben estar en modo de acceso.
- Configure el **S1** en modo de enlace troncal y permita solo las VLAN que figuran en la **tabla de asignación de VLAN y de puertos**.
- Configure el gateway predeterminado en el **S1**.
- Todos los puertos que no se asignen a una VLAN deben estar deshabilitados.
- Configure el routing entre VLAN en el **R1** según la **tabla de direccionamiento**.
- Verifique la conectividad. El **R1**, el **S1** y todas las computadoras deben poder hacer ping entre sí y al servidor **cisco.pka**.

```
!S1!!!!!!!!!!!!!!
en
config t
interface vlan 99
ip address 172.17.99.10 255.255.255.0
no shutdown
ip default-gateway 172.17.99.1
!Note: VLAN naming only requires the first letter be correct
vlan 10
name Faculty/Staff
vlan 20
name Students
vlan 30
name Guest(Default)
```

```
vlan 88
name Native
vlan 99
name Management
interface range fa0/11 - 17
switchport mode access
switchport access vlan 10
interface range fa0/18 - 24
switchport mode access
switchport access vlan 20
interface range fa0/6 - 10
switchport mode access
switchport access vlan 30
interface g0/1
switchport mode trunk
switchport trunk native vlan 99
interface range fa0/1 - 5 , g1/2
shutdown
do write

!R1!!!!!!!!!!!!!!!!!
ena
conf t
interface GigabitEthernet0/1
no shutdown
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.17.10.1 255.255.255.0
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.17.20.1 255.255.255.0
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.17.30.1 255.255.255.0
interface GigabitEthernet0/1.88
encapsulation dot1Q 88 native
ip address 172.17.88.1 255.255.255.0
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
```

```
ip address 172.17.99.1 255.255.255.0
do write
```

Packet Tracer: configuración de rutas estáticas y predeterminadas IPv4 (versión para el instructor)

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

Topología

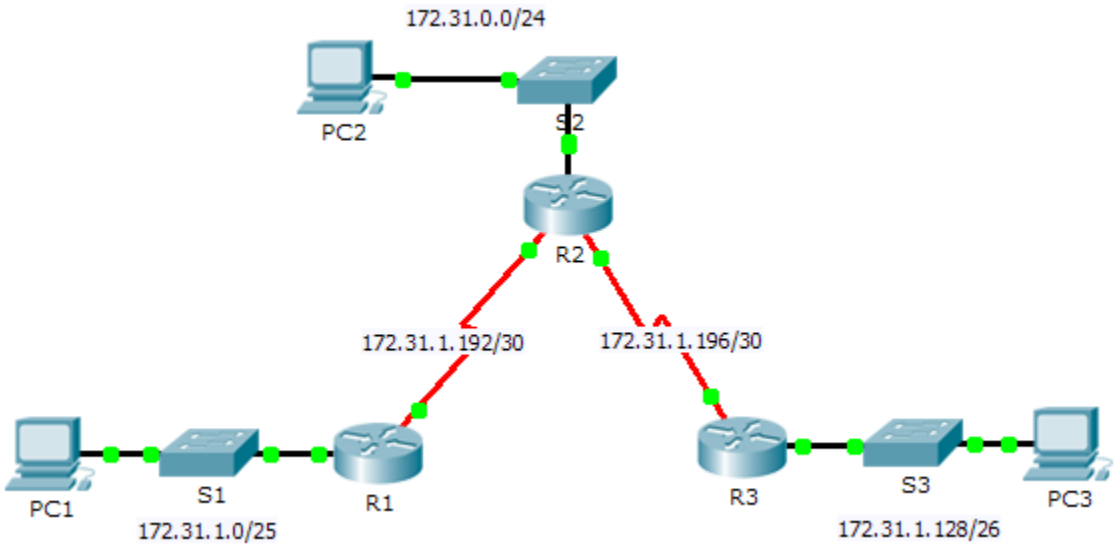


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar rutas estáticas y predeterminadas

Parte 3: verificar la conectividad

Información básica

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

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

a. Observe el diagrama de la topología. ¿Cuántas redes hay en total? 5

b. ¿Cuántas redes están conectadas directamente al R1, al R2 y al R3? El R1 tiene 2, el R2 tiene 3 y el R3 tiene 2.

c. ¿Cuántas rutas estáticas requiere cada router para llegar a las redes que no están conectadas directamente? El R1 necesita 3 rutas estáticas, el R2 necesita 2, y el R3 necesita 3.

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

¿Por qué no logró hacerlo? Porque no hay rutas a estas redes en el R1.

Parte 2: configurar rutas estáticas y predeterminadas

Paso 1: configurar rutas estáticas recursivas en el R1.

a. ¿Qué es una ruta estática recursiva? Una ruta estática recursiva depende del router de siguiente salto para que los paquetes se envíen a su destino. Una ruta estática recursiva requiere dos búsquedas en la tabla de routing.

b. ¿Por qué una ruta estática recursiva requiere dos búsquedas en la tabla de routing? Primero debe buscar la red de destino en la tabla de routing y, luego, debe buscar la interfaz de salida y el sentido de la red para el router de siguiente salto.

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

```
ip route 172.31.0.0 255.255.255.0 172.31.1.193
ip route 172.31.1.196 255.255.255.252 172.31.1.193
ip route 172.31.1.128 255.255.255.192 172.31.1.193
```

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

¿Por qué no logró hacerlo? El R1 tiene una ruta a las LAN del R2 y el R3, pero estos no tienen rutas al R1.

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

a. ¿En qué se diferencia una ruta estática conectada directamente de una ruta estática recursiva? Una ruta estática conectada directamente depende de su interfaz de salida para que los paquetes se envíen a su destino, mientras que una ruta estática recursiva utiliza la dirección IP del router de siguiente salto.

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

```
ip route 172.31.1.0 255.255.255.128 Serial0/0/0
ip route 172.31.1.128 255.255.255.192 Serial0/0/1
```

c. ¿Con qué comando se muestran solo las redes conectadas directamente? `show ip route connected`

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

e. Al ver la tabla de routing completa, ¿cómo se puede distinguir entre una ruta estática conectada directamente y una red conectada directamente? La ruta estática tiene una S, y las redes conectadas directamente tienen una C.

Paso 3: configurar una ruta predeterminada en el R3.

a. ¿En qué se diferencia una ruta predeterminada de una ruta estática común? Una ruta predeterminada, también conocida como “gateway de último recurso”, es la ruta de red que usa un router cuando no existe ninguna otra ruta conocida para una red de destino. Una ruta estática se utiliza para enrutar el tráfico a una red específica.

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

```
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

c. ¿Cómo se muestra una ruta estática en la tabla de routing? S* 0.0.0.0/0

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

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

a. Explique qué es una ruta completamente especificada. Una ruta completamente especificada es una ruta estática que se configura con una interfaz de salida y la dirección de siguiente salto.

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

```
R3(config)# ip route 172.31.0.0 255.255.255.0 s0/0/1 172.31.1.197
```

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

```
R3(config)# ip route 172.31.1.192 255.255.255.252 s0/0/1 172.31.1.197
```

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

```
R3(config)# ip route 172.31.1.0 255.255.255.128 s0/0/1 172.31.1.197
```


Paso 5: verificar la configuración de las rutas estáticas.

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

¿Qué comandos **show** puede utilizar para verificar que las rutas estáticas se hayan configurado correctamente? show ip route, show ip route static y los comandos show ip route [red]

Parte 3: Verificar la conectividad

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

Tabla de calificación sugerida

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

Packet Tracer: configuración de rutas estáticas y predeterminadas IPv6 (versión para el instructor)

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

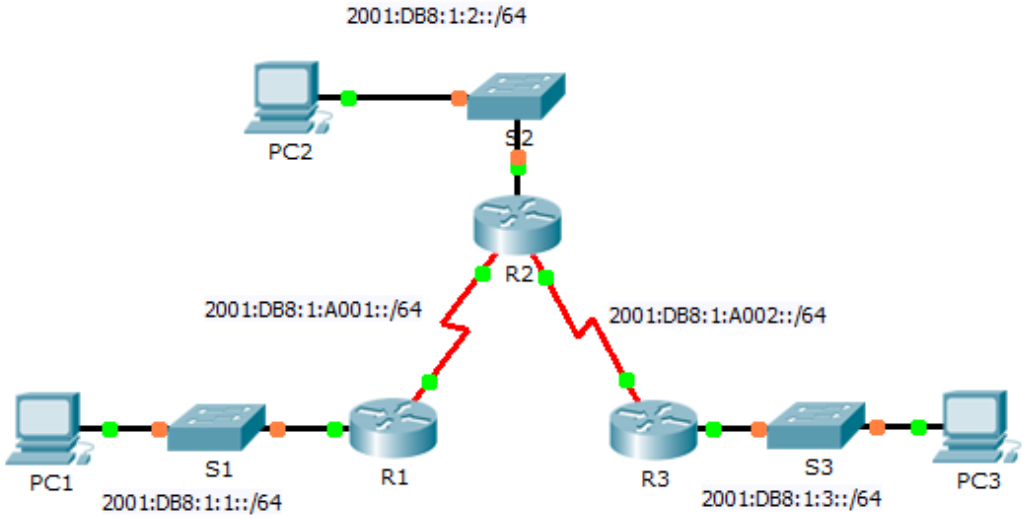


Tabla de direccionamiento IPv6

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

Objetivos

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

Parte 2: configurar rutas estáticas y predeterminadas IPv6

Parte 3: verificar la conectividad

Información básica

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

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

a. Observe el diagrama de la topología. ¿Cuántas redes hay en total? 5

b. ¿Cuántas redes están conectadas directamente al R1, al R2 y al R3? El R1 tiene 2, el R2 tiene 3 y el R3 tiene 2.

c. ¿Cuántas rutas estáticas requiere cada router para llegar a las redes que no están conectadas directamente? El R1 necesita configurar 3 rutas estáticas, el R2, 2 y el R3, 3.

d. ¿Qué comando se utiliza para configurar las rutas estáticas IPv6? `ipv6 route [network/prefix] [exit interface/next hop address]`

Parte 2: configurar rutas estáticas y predeterminadas IPv6

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

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

¿Qué comando permite lograr este resultado? `ipv6 unicast-routing`

Introduzca este comando en cada router.

Paso 2: configurar rutas estáticas recursivas en el R1.

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

```
ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:A001::2
ipv6 route 2001:DB8:1:A002::/64 2001:DB8:1:A001::2
ipv6 route 2001:DB8:1:3::/64 2001:DB8:1:A001::2
```

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

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

```
ipv6 route 2001:DB8:1:1::/64 Serial0/0/0
```

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

```
ipv6 route 2001:DB8:1:3::/64 Serial0/0/1 2001:DB8:1:A002::2
```

Paso 4: configurar una ruta predeterminada en el R3.

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

```
ipv6 route ::/0 2001:DB8:1:A002::1
```


Paso 5: verificar la configuración de las rutas estáticas.

a. ¿Qué comando se utiliza para verificar la configuración de IPv6 en una computadora desde el símbolo del sistema? `ipv6config`

b. ¿Con qué comando se muestran las direcciones IPv6 configuradas en la interfaz de un router? `show ipv6 interface brief`

c. ¿Con qué comando se muestra el contenido de la tabla de routing IPv6? `show ipv6 route`

Parte 3: Verificar la conectividad de la red

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

Tabla de calificación sugerida

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

Packet Tracer: diseño e implementación de un esquema de direccionamiento VLSM (versión para el instructor)

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

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0	[[R1G0Add]]	[[R1G0Sub]]	No aplicable
	G0/1	[[R1G1Add]]	[[R1G1Sub]]	No aplicable
	S0/0/0	[[R1S0Add]]	[[R1S0Sub]]	No aplicable
[[R2Name]]	G0/0	[[R2G0Add]]	[[R2G0Sub]]	No aplicable
	G0/1	[[R2G1Add]]	[[R2G1Sub]]	No aplicable
	S0/0/0	[[R2S0Add]]	[[R2S0Sub]]	No aplicable
[[S1Name]]	VLAN 1	[[S1Add]]	[[S1Sub]]	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	[[S2Sub]]	[[R1G1Add]]
[[S3Name]]	VLAN 1	[[S3Add]]	[[S3Sub]]	[[R2G0Add]]
[[S4Name]]	VLAN 1	[[S4Add]]	[[S4Sub]]	[[R2G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	[[PC1Sub]]	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	[[PC2Sub]]	[[R1G1Add]]
[[PC3Name]]	NIC	[[PC3Add]]	[[PC3Sub]]	[[R2G0Add]]
[[PC4Name]]	NIC	[[PC4Add]]	[[PC4Sub]]	[[R2G1Add]]

Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direccionamiento VLSM

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

Información básica

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

Parte 1: examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias.

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

- La LAN de **[[S1Name]]** requerirá **[[HostReg1]]** direcciones IP host.
- La LAN de **[[S2Name]]** requerirá **[[HostReg2]]** direcciones IP host.
- La LAN de **[[S3Name]]** requerirá **[[HostReg3]]** direcciones IP host.
- La LAN de **[[S4Name]]** requerirá **[[HostReg4]]** direcciones IP host.

¿Cuántas subredes se necesitan en la topología de la red? 5

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

a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requerida para **[[S1Name]]**?

   ¿Cuántas direcciones host utilizables admitirá esta subred?

b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S2Name]]**?

   ¿Cuántas direcciones host utilizables admitirá esta subred?

c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S3Name]]**?

   ¿Cuántas direcciones host utilizables admitirá esta subred?

d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **[[S4Name]]**?

   ¿Cuántas direcciones host utilizables admitirá esta subred?

e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requerida para la conexión entre **[[R1Name]]** y **[[R2Name]]**?

Parte 2: diseñar el esquema de direccionamiento VLSM

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

a. Utilice la primera subred para admitir la LAN más grande.

b. Utilice la segunda subred para admitir la segunda LAN más grande.

c. Utilice la tercera subred para admitir la tercera LAN más grande.

d. Utilice la cuarta subred para admitir la cuarta LAN más grande.

e. Utilice la quinta subred para admitir la conexión entre **[[R1Name]]** y **[[R2Name]]**.

Paso 2: registrar las subredes VLSM.

Complete la **tabla de subredes** con las descripciones de las subredes (p. ej., LAN de [[S1Name]]), la cantidad de hosts necesarios, la dirección de red para la subred, la primera dirección host utilizable y la dirección de difusión. Repita hasta que aparezcan todas las direcciones.

Tabla de subredes

Nota: las respuestas correctas para esta tabla pueden variar según la situación recibida. Consulte las notas para el instructor al final de estas instrucciones para obtener más información. Este formato coincide con lo que utilizó el estudiante en **Diseño e implementación de un esquema de direccionamiento VLSM**.

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

Paso 3: Documente el esquema de direccionamiento.

a. Asigne las primeras direcciones IP utilizables a **[[R1Name]]** para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables a **[[R2Name]]** para los dos enlaces LAN. Asigne la última dirección IP utilizable al enlace WAN.

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

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

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

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

Paso 1: configurar el direccionamiento IP en las interfaces LAN de [[R1Name]].

Paso 2: configurar el direccionamiento IP en [[S3Name]], incluido el gateway predeterminado.

Paso 3: configurar el direccionamiento IP en [[PC4Name]], incluido el gateway predeterminado.

Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde [[R1Name]], [[S3Name]] y [[PC4Name]]. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan al diseño y al registro del esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

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

ID:[[indexAdds]][[indexNames]][[indexTopos]]

Notas para el instructor:

Las tablas de direccionamiento que figuran a continuación representan las tres situaciones de direccionamiento posibles que el estudiante puede recibir. Observe que la columna Dispositivo es independiente del esquema de direccionamiento. Por ejemplo, un estudiante podría recibir los nombres de los dispositivos de la situación 1 y el esquema de direccionamiento de la situación 3. Además, las tres topologías posibles también son independientes de los nombres de los dispositivos y del esquema de direccionamiento (haga clic en Restablecer en la actividad para ver las diferentes topologías). Por lo tanto, esta actividad utiliza tres variables independientes con tres valores posibles cada una, lo que hace a un total de 27 combinaciones posibles (3 nombres de dispositivos x 3 esquemas de direccionamiento x 3 topologías = 27 isomorfos).

Situación 1: dirección de red 10.11.48.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección host utilizable	Última dirección host utilizable	Dirección de difusión
LAN del Host-D	60	10.11.48.0/26	10.11.48.1	10.11.48.62	10.11.48.63
LAN del Host-B	30	10.11.48.64/27	10.11.48.65	10.11.48.94	10.11.48.95
LAN del Host-A	14	10.11.48.96/28	10.11.48.97	10.11.48.110	10.11.48.111
LAN del Host-C	6	10.11.48.112/29	10.11.48.113	10.11.48.118	10.11.48.119
Enlace WAN	2	10.11.48.120/30	10.11.48.121	10.11.48.122	10.11.48.123

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Edificio1	G0/0	10.11.48.97	255.255.255.240	N/A
	G0/1	10.11.48.65	255.255.255.224	N/A
	S0/0/0	10.11.48.121	255.255.255.252	N/A
Edificio2	G0/0	10.11.48.113	255.255.255.248	N/A
	G0/1	10.11.48.1	255.255.255.192	N/A
	S0/0/0	10.11.48.122	255.255.255.252	N/A
ASW1	VLAN 1	10.11.48.98	255.255.255.240	10.11.48.97
ASW2	VLAN 1	10.11.48.66	255.255.255.224	10.11.48.65
ASW3	VLAN 1	10.11.48.114	255.255.255.248	10.11.48.113
ASW4	VLAN 1	10.11.48.2	255.255.255.192	10.11.48.1
Host A	NIC	10.11.48.110	255.255.255.240	10.11.48.97
Host B	NIC	10.11.48.94	255.255.255.224	10.11.48.65
Host-C	NIC	10.11.48.118	255.255.255.248	10.11.48.113
Host-D	NIC	10.11.48.62	255.255.255.192	10.11.48.1

Edificio 1

```
en
conf t
int g0/0
ip add 10.11.48.97 255.255.255.240
no shut
int g0/1
ip add 10.11.48.65 255.255.255.224
no shut
```

ASW3

```
en
conf t
int vlan 1
ip add 10.11.48.114 255.255.255.248
no shut
ip def 10.11.48.113
```

Situación 2: dirección de red 172.31.103.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección host utilizable	Última dirección host utilizable	Dirección de difusión
LAN de la PC-A	27	172.31.103.0/27	172.31.103.1	172.31.103.30	172.31.103.31
LAN de la PC-B	25	172.31.103.32/27	172.31.103.33	172.31.103.62	172.31.103.63
LAN de la PC-C	14	172.31.103.64/28	172.31.103.65	172.31.103.78	172.31.103.79
LAN de la PC-D	8	172.31.103.80/28	172.31.103.81	172.31.103.94	172.31.103.95
Enlace WAN	2	172.31.103.96/30	172.31.103.97	172.31.103.98	172.31.103.99

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Branch1	G0/0	172.31.103.1	255.255.255.224	N/A
	G0/1	172.31.103.33	255.255.255.224	N/A
	S0/0/0	172.31.103.97	255.255.255.252	N/A
Branch2	G0/0	172.31.103.65	255.255.255.240	N/A
	G0/1	172.31.103.81	255.255.255.240	N/A
	S0/0/0	172.31.103.98	255.255.255.252	N/A
Sala-114	VLAN 1	172.31.103.2	255.255.255.224	172.31.103.1
Sala-279	VLAN 1	172.31.103.34	255.255.255.224	172.31.103.33
Sala-312	VLAN 1	172.31.103.66	255.255.255.240	172.31.103.65
Sala-407	VLAN 1	172.31.103.82	255.255.255.240	172.31.103.81
PC-A	NIC	172.31.103.30	255.255.255.224	172.31.103.1
PC-B	NIC	172.31.103.62	255.255.255.224	172.31.103.33
PC-C	NIC	172.31.103.78	255.255.255.240	172.31.103.65
PC-D	NIC	172.31.103.94	255.255.255.240	172.31.103.81

Sucursal 1

```
en
conf t
int g0/0
ip add 172.31.103.1 255.255.255.224
no shut
int g0/1
ip add 172.31.103.33 255.255.255.224
no shut
```

Sala-312

```
en
conf t
int vlan 1
ip add 172.31.103.66 255.255.255.240
no shut
ip def 172.31.103.65
```

Situación 3: dirección de red 192.168.72.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección host utilizable	Última dirección host utilizable	Dirección de difusión
LAN del usuario-4	58	192.168.72.0/26	192.168.72.1	192.168.72.62	192.168.72.63
LAN del usuario-3	29	192.168.72.64/27	192.168.72.65	192.168.72.94	192.168.72.95
LAN del usuario-2	15	192.168.72.96/27	192.168.72.97	192.168.72.126	192.168.72.127
LAN del usuario-1	7	192.168.72.128/28	192.168.72.129	192.168.72.142	192.168.72.143
Enlace WAN	2	192.168.72.144/30	192.168.72.145	192.168.72.146	192.168.72.147

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Sitio-remoto1	G0/0	192.168.72.129	255.255.255.240	N/A
	G0/1	192.168.72.97	255.255.255.224	N/A
	S0/0/0	192.168.72.145	255.255.255.252	N/A
Sitio-remoto2	G0/0	192.168.72.65	255.255.255.224	N/A
	G0/1	192.168.72.1	255.255.255.192	N/A
	S0/0/0	192.168.72.146	255.255.255.252	N/A
Sw1	VLAN 1	192.168.72.130	255.255.255.240	192.168.72.129
Sw2	VLAN 1	192.168.72.98	255.255.255.224	192.168.72.97
Sw3	VLAN 1	192.168.72.66	255.255.255.224	192.168.72.65
Sw4	VLAN 1	192.168.72.2	255.255.255.192	192.168.72.1
Usuario-1	NIC	192.168.72.142	255.255.255.240	192.168.72.129
Usuario-2	NIC	192.168.72.126	255.255.255.224	192.168.72.97
Usuario-3	NIC	192.168.72.94	255.255.255.224	192.168.72.65
Usuario-4	NIC	192.168.72.62	255.255.255.192	192.168.72.1

Sitio-remoto1

```
en
conf t
int g0/0
ip add 192.168.72.129 255.255.255.240
no shut
int g0/1
ip add 192.168.72.97 255.255.255.224
no shut
```

Sw-3

```
en
conf t
int vlan 1
ip add 192.168.72.66 255.255.255.224
no shut
ip def 192.168.72.65
```

Packet Tracer: configuración de sumarización de ruta IPv4, situación 1 (versión para el instructor)

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

Topología

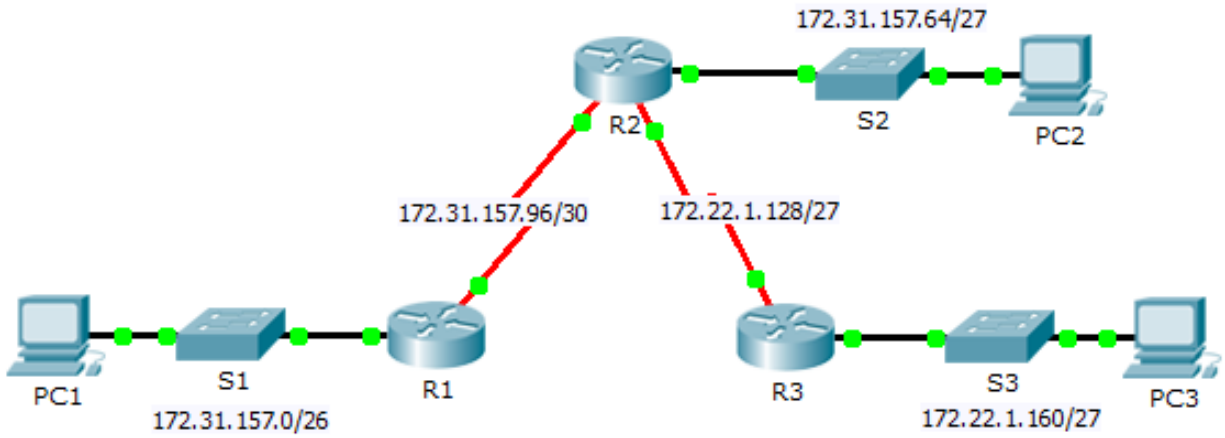


Tabla de direccionamiento

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

Objetivos

Parte 1: calcular rutas resumidas

Parte 2: configurar rutas resumidas

Parte 3: verificar la conectividad

Información básica

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

Parte 1: calcular rutas resumidas

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

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

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

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

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

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

```
10101100.00010110.00000001.10000000
```

d. ¿Cuál es la dirección de red resumida y la máscara de subred? 172.22.1.128 255.255.255.192

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

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

```
10101100.00011111.10011101.00000000
10101100.00011111.10011101.01000000
10101100.00011111.10011101.01100000
```

b. ¿Cuál es la dirección de red resumida y la máscara de subred? 172.31.157.0 255.255.255.128

Parte 2: configurar rutas resumidas

Paso 1: configurar una ruta resumida para el R1.

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

```
R1(config)# ip route 172.22.1.128 255.255.255.192 172.31.157.98
```

Paso 2: configurar una ruta resumida para el R3.

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

```
R3(config)# ip route 172.31.157.0 255.255.255.128 serial 0/0/1
```

Parte 3: Verificar la conectividad

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

Packet Tracer: configuración de la sumarización de ruta IPv4, situación 2 (versión para el instructor)

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

Topología

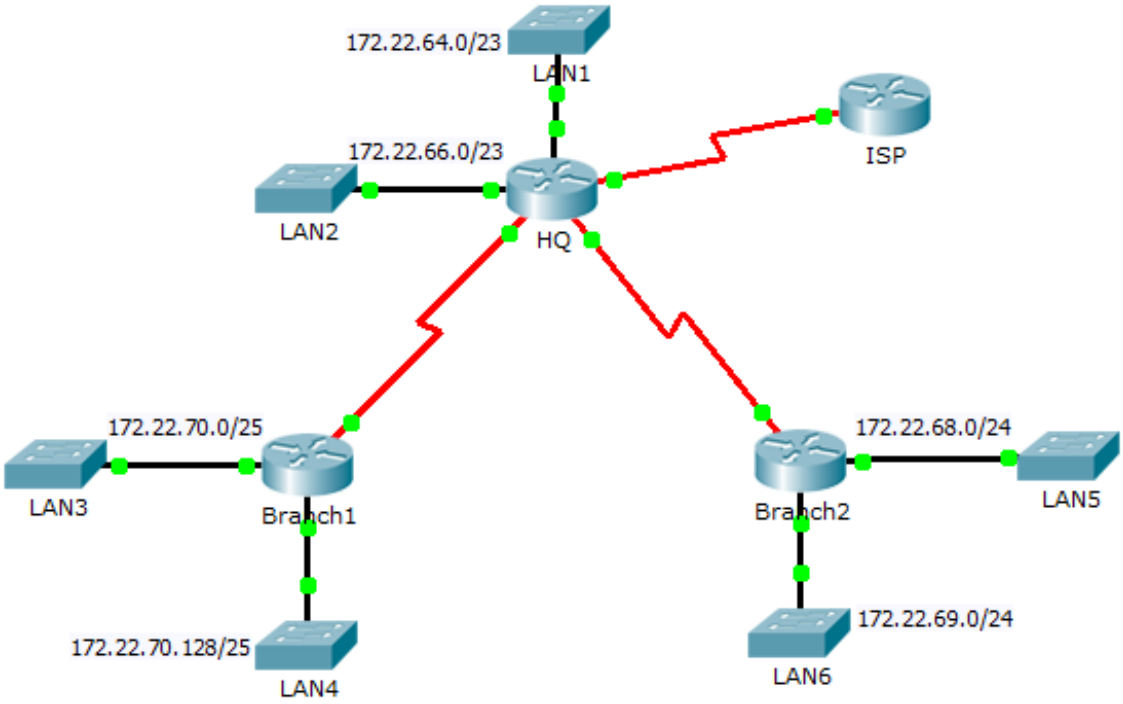


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
ISP	S0/0/1	198.0.0.1	255.255.255.252	N/A
HQ	G0/0	172.22.64.1	255.255.254.0	N/A
	G0/1	172.22.66.1	255.255.254.0	N/A
	S0/0/0	172.22.71.1	255.255.255.252	N/A
	S0/0/1	172.22.71.5	255.255.255.252	N/A
	S0/1/0	198.0.0.2	255.255.255.252	N/A
Branch1	G0/0	172.22.70.1	255.255.255.128	N/A
	G0/1	172.22.70.129	255.255.255.128	N/A
	S0/0/0	172.22.71.2	255.255.255.252	N/A
Branch2	G0/0	172.22.68.1	255.255.255.0	N/A
	G0/1	172.22.69.1	255.255.255.0	N/A
	S0/0/1	172.22.71.6	255.255.255.252	N/A
LAN1	VLAN 1	172.22.64.2	255.255.254.0	172.22.64.1
LAN2	VLAN 1	172.22.66.2	255.255.254.0	172.22.66.1
LAN3	VLAN 1	172.22.70.2	255.255.255.128	172.22.70.1
LAN4	VLAN 1	172.22.70.130	255.255.255.128	172.22.70.129
LAN5	VLAN 1	172.22.68.2	255.255.255.0	172.22.68.1
LAN6	VLAN 1	172.22.69.2	255.255.255.0	172.22.69.1

Objetivos

Parte 1: calcular rutas resumidas

Parte 2: configurar rutas resumidas

Parte 3: verificar la conectividad

Información básica

En esta actividad, calculará y configurará rutas resumidas. La sumarización de ruta, también conocida como “agregación de rutas”, es el proceso de anunciar un conjunto de direcciones contiguas como una única dirección. Después de calcular las rutas resumidas para cada LAN, debe resumir una ruta que incluya todas las redes en la topología para que el ISP alcance cada LAN.

Parte 1: calcular rutas resumidas

a. ¿Cuál es la ruta resumida para llegar a las LAN de HQ? 172.22.64.0 255.255.252.0

b. ¿Cuál es la ruta resumida para llegar a las LAN de Sucursal1? 172.22.70.0 255.255.255.0

c. ¿Cuál es la ruta resumida para llegar a las LAN de Sucursal2? 172.22.68.0 255.255.254.0

d. ¿Cuál es la ruta resumida del router ISP para llegar a todas las LAN? 172.22.64.0 255.255.248.0

Parte 2: configurar rutas resumidas

Paso 1: configurar las rutas resumidas del router HQ a otras redes.

a. Configure una ruta resumida conectada directamente en **HQ** para que llegue a las LAN de **Sucursal1**.

```
HQ(config)# ip route 172.22.70.0 255.255.255.0 s0/0/0
```

b. Configure una ruta resumida recursiva en **HQ** para que llegue a las LAN de **Sucursal2**.

```
HQ(config)# ip route 172.22.68.0 255.255.254.0 172.22.71.6
```

Paso 2: configurar las rutas resumidas del router de Sucursal1 a otras redes.

a. Configure una ruta resumida recursiva en **Sucursal1** para que llegue a las LAN de **HQ**.

```
Branch1(config)# ip route 172.22.64.0 255.255.252.0 172.22.71.1
```

b. Configure una ruta resumida recursiva en **Sucursal1** para que llegue a las LAN de **Sucursal2**.

```
Branch1(config)# ip route 172.22.68.0 255.255.254.0 172.22.71.1
```

Paso 3: configurar las rutas resumidas del router Sucursal2 a otras redes.

a. Configure una ruta resumida conectada directamente en **Sucursal2** para que llegue a las LAN de **Sucursal1**.

```
Branch2(config)# ip route 172.22.70.0 255.255.255.0 s0/0/1
```

b. Configure una ruta resumida recursiva en **Sucursal2** para que llegue a las LAN de **HQ**.

```
Branch2(config)# ip route 172.22.64.0 255.255.252.0 172.22.71.5
```

Paso 4: configurar una ruta resumida en ISP para que llegue a todas las redes.

```
ISP(config)# ip route 172.22.64.0 255.255.248.0 s0/0/1
```

Parte 3: Verificar la conectividad

Verifique que todos los switches y routers puedan hacer ping a los otros dispositivos en la topología. De lo contrario, resuelva y corrija los problemas de las rutas resumidas.

Packet Tracer: cálculo y configuración de la sumarización de ruta IPv6 (versión para el instructor)

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

Topología

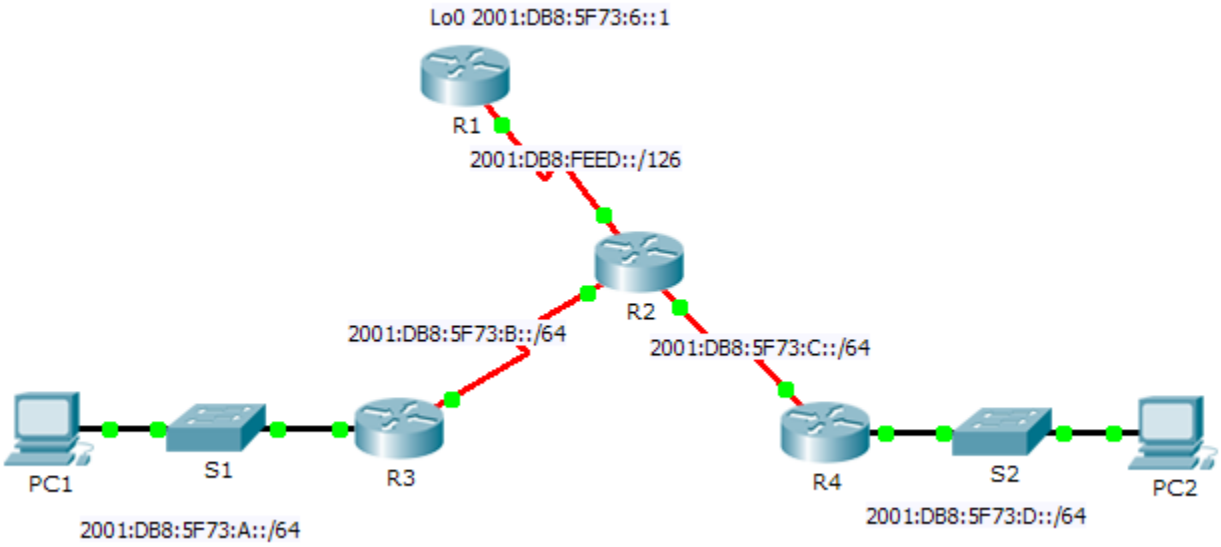


Tabla de direccionamiento

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

Objetivos

Parte 1: calcular una ruta resumida para el R1

Parte 2: configurar la ruta resumida y verificar la conectividad

Información básica

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

Parte 1: configurar una ruta resumida para el R1

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

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

2001:DB8:5F73:0000000000001010

2001:DB8:5F73:0000000000001011

2001:DB8:5F73:0000000000001100

2001:DB8:5F73:0000000000001101

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

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

Parte 2: configurar la ruta resumida y verificar la conectividad

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

```
ipv6 route 2001:DB8:5F73:8::/61 Serial0/0/0
```

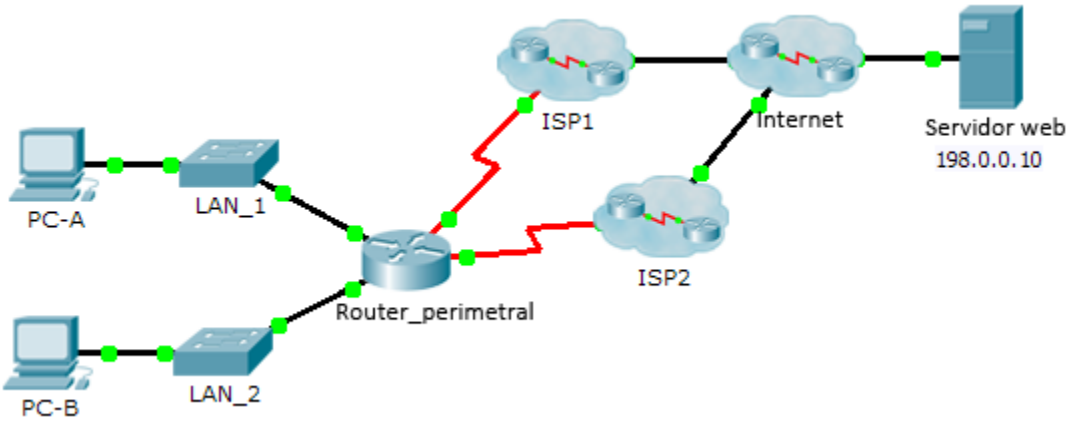
b. La PC1 debe poder hacer ping a la PC2.

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

Packet Tracer: configuración de una ruta estática flotante (versión para el instructor)

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

Topología



Objetivos

Parte 1: configurar una ruta estática flotante

Parte 2: probar la conmutación por falla a la ruta de respaldo

Información básica

En esta actividad, configurará una ruta estática flotante que se utiliza como ruta de respaldo. Esta ruta tiene una distancia administrativa configurada manualmente mayor que la de la ruta principal y, por lo tanto, no aparece en la tabla de routing hasta que la ruta principal falla. Deberá probar la conmutación por falla a la ruta de respaldo y, luego, restaurar la conectividad a la ruta principal.

Parte 1: configurar una ruta estática flotante

Paso 1: configurar una ruta estática predeterminada conectada directamente.

a. Configure una ruta estática predeterminada conectada directamente del **Router_perimetral** a Internet. La ruta predeterminada principal debe ser a través de **ISP1**.

```
Edge_Router(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
```

b. Muestre el contenido de la tabla de routing. Verifique que la ruta predeterminada se visualice en la tabla de routing.

```
Edge_Router# show ip route

<output omitted>
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

c. ¿Qué comando se utiliza para rastrear una ruta desde una computadora hasta un destino? `tracert`

Desde la **PC-A**, rastree la ruta hacia el **servidor web**. La ruta debe comenzar en el gateway predeterminado 192.168.10.1 y pasar por la dirección 10.10.10.1. Si no es así, revise la configuración de la ruta estática predeterminada.

```
PC> tracert 198.0.0.10

Tracing route to 198.0.0.10 over a maximum of 30 hops:

  1    3 ms       0 ms       0 ms       192.168.10.1
  2    0 ms       1 ms       0 ms       10.10.10.1
  3    1 ms       2 ms       0 ms       198.0.0.10

Trace complete.
```

Paso 2: configurar una ruta estática flotante.

a. ¿Cuál es la distancia administrativa de una ruta estática? La distancia es 0 para redes conectadas directamente y 1 para redes recurrentes.

b. Configure una ruta estática flotante predeterminada conectada directamente con una distancia administrativa de 5. La ruta debe dirigirse al **ISP2**.

```
Edge_Router(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1 5
```

c. Vea la configuración en ejecución y verifique que aparezca la ruta estática flotante predeterminada y la ruta estática predeterminada.

```
Edge_Router# show run
Building configuration...

Current configuration : 781 bytes
!
<output omitted>
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 0.0.0.0 0.0.0.0 Serial0/0/1 5
!
```

d. Muestre el contenido de la tabla de routing. ¿Es posible ver la ruta estática flotante en la tabla de routing? ¿Por qué o por qué no? N.º No se puede visualizar, porque no es la ruta principal. Los routers solo colocan la mejor ruta en la tabla de routing, y dado que esta es la ruta de respaldo, solo estará visible en la tabla de routing cuando la ruta principal esté inactiva.

Parte 2: probar la conmutación por falla a la ruta de respaldo

a. En el **Router_perimetral**, deshabilite administrativamente la interfaz de salida de la ruta principal.

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

b. Verifique que la ruta de respaldo se visualice ahora en la tabla de routing.

```
Edge_Router# show ip route

<output omitted>
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```


c. Rastree la ruta desde la **PC-A** hasta el **servidor web**.

```
PC> tracert 198.0.0.10

Tracing route to 198.0.0.10 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       192.168.10.1
  2    0 ms       0 ms       2 ms       10.10.10.5
  3    0 ms       2 ms       0 ms       198.0.0.10

Trace complete.
```

¿Funcionó la ruta de respaldo? Si no es así, espere unos segundos para que se logre la convergencia y luego vuelva a hacer la prueba. Si la ruta de respaldo aún no funciona, investigue la configuración de la ruta estática flotante.

d. Restaure la conectividad a la ruta principal.

```
Edge_Router(config)# interface s0/0/0
Edge_Router(config-if)# no shutdown
```

e. Rastree la ruta desde la **PC-A** hacia el **servidor web** para verificar que se haya restaurado la ruta principal.

```
PC> tracert 198.0.0.10

Tracing route to 198.0.0.10 over a maximum of 30 hops:

  1    3 ms       0 ms       0 ms       192.168.10.1
  2    0 ms       1 ms       0 ms       10.10.10.1
  3    1 ms       2 ms       0 ms       198.0.0.10

Trace complete.
```

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: configurar una ruta estática flotante	Paso 1c	2	
	Paso 2a	3	
	Paso 2d	5	
Total de la parte 1		**10**	
Puntuación de Packet Tracer		**90**	
Puntuación total		**100**	

Packet Tracer: resolución de problemas de rutas estáticas (versión para el instructor)

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

Topología

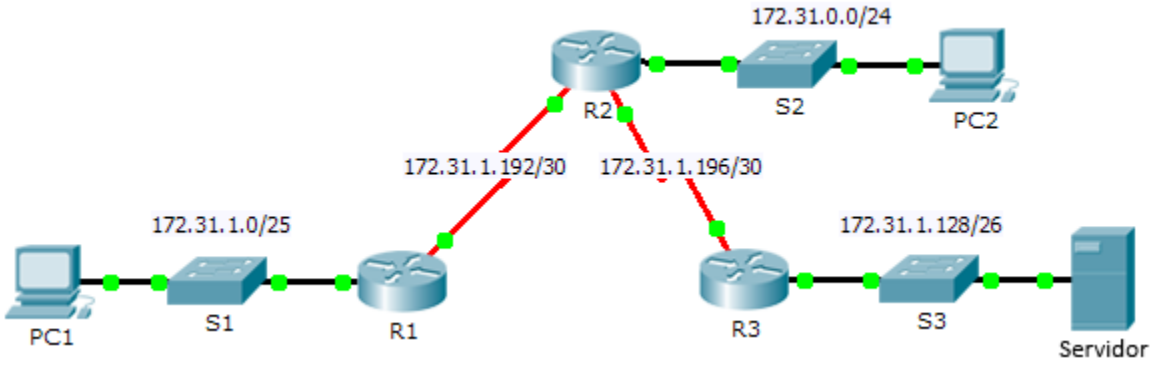


Tabla de direccionamiento

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

Objetivos

Parte 1: encontrar el problema

Parte 2: determinar la solución

Parte 3: implementar la solución

Parte 4: verificar que el problema esté resuelto

Información básica

En esta actividad, la PC1 informa que no se puede acceder a los recursos en el servidor. Encuentre el problema, determine una solución apropiada y resuélvalo.

Parte 1: encontrar el problema

La PC1 no puede acceder a los archivos en el servidor. De los comandos que aprendió en los capítulos anteriores, utilice los comandos **show** apropiados en todos los routers y los comandos para la resolución de problemas en las computadoras, a fin de encontrar el problema.

¿Cuáles son algunos de los comandos para la resolución de problemas en los routers y las computadoras que se pueden utilizar para identificar el origen del problema? show ip route, show run, traceroute, tracert y ping.

Parte 2: determinar la solución

Una vez ubicado el problema que evita que la PC1 acceda a los archivos en el servidor, rellene la siguiente tabla.

Problema	Solución
Ambas rutas estáticas en el R2 utilizan la dirección de siguiente salto incorrecta.	Eliminar las rutas estáticas y reemplazarlas con la dirección del router de siguiente salto correcta.
No se indica ninguna ruta en el R3 para la LAN del R1.	Agregar una ruta estática en el R3 hacia la LAN del R1.

Parte 3: Implemente la solución

a. Si hay rutas estáticas mal configuradas, debe quitarlas para poder agregar las rutas correctas a la configuración.

```
R2(config)# no ip route 172.31.1.0 255.255.255.128 172.31.1.198
R2(config)# no ip route 172.31.1.128 255.255.255.192 172.31.1.194
R2(config)# ip route 172.31.1.0 255.255.255.128 172.31.1.194
R2(config)# ip route 172.31.1.128 255.255.255.192 172.31.1.198
```

b. Para agregar las rutas estáticas faltantes, configure las rutas conectadas directamente.

```
R3(config)# ip route 172.31.1.0 255.255.255.128 s0/0/1
```

Parte 4: verificar que el problema esté resuelto

a. Haga ping de la PC1 al servidor.

b. Establezca una conexión web al servidor. Después de identificar el problema correctamente e implementar la solución adecuada, recibirá un mensaje en el navegador web cuando se conecte al servidor.

Tabla de calificación sugerida

Sección de la actividad	Puntos posibles	Puntos obtenidos
Parte 1: encontrar el problema	**2**	
Parte 2: determinar la solución	**8**	
Puntuación de Packet Tracer	**90**	
Puntuación total	**100**	

Packet Tracer: resolución de problemas de sumarización de ruta y VLSM (versión para el instructor)

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

Topología

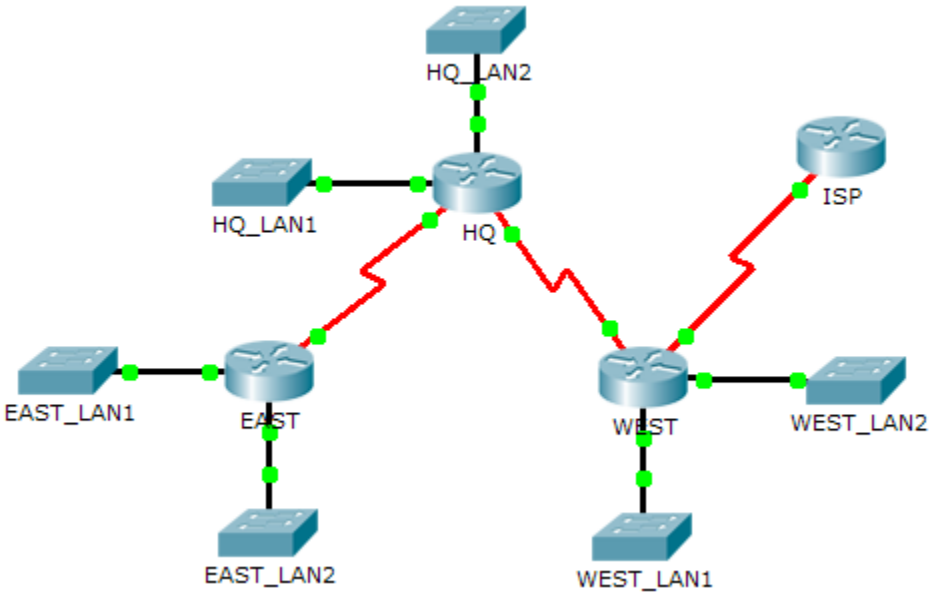


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
HQ	G0/0	172.16.40.1	255.255.254.0	N/A
	G0/1	172.16.32.1	255.255.252.0	N/A
	S0/0/0	10.10.10.2	255.255.255.252	N/A
	S0/0/1	10.10.10.5	255.255.255.252	N/A
EAST	G0/0	172.16.52.1	255.255.252.0	N/A
	G0/1	172.16.48.1	255.255.252.0	N/A
	S0/0/0	10.10.10.1	255.255.255.252	N/A
WEST	G0/0	172.16.58.1	255.255.255.0	N/A
	G0/1	172.16.56.1	255.255.254.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
	S0/0/1	10.10.10.9	255.255.255.252	N/A
HQ_LAN1	VLAN 1	172.16.32.2	255.255.252.0	172.16.32.1
HQ_LAN2	VLAN 1	172.16.40.2	255.255.254.0	172.16.40.1
EAST_LAN1	VLAN 1	172.16.48.2	255.255.252.0	172.16.48.1
EAST_LAN2	VLAN 1	172.16.52.2	255.255.252.0	172.16.52.1
WEST_LAN1	VLAN 1	172.16.58.2	255.255.255.0	172.16.58.1
WEST_LAN2	VLAN 1	172.16.56.2	255.255.254.0	172.16.56.1

Objetivos

Parte 1: encontrar el problema

Parte 2: determinar la solución

Parte 3: implementar la solución

Parte 4: verificar que los problemas estén resueltos

Información básica/situación

En esta actividad, la red ya se direccionó mediante VLSM y se configuró con rutas estáticas, pero hay un problema. Encuentre los problemas, determine la mejor solución, impleméntela y verifique que los problemas se resuelvan.

Parte 1: encontrar el problema

a. Investigue el dispositivo y registre el esquema de direccionamiento actual en la tabla de direccionamiento.

b. Utilice el gráfico de hosts que se muestra a continuación para determinar si el direccionamiento en cada interfaz LAN tiene la máscara de subred correcta según la cantidad de hosts necesarios para esa LAN.

Gráfico de hosts

LAN	Interfaz	Cantidad de hosts
LAN 1 de HQ	G0/1	1500
LAN 2 de HQ	G0/0	1000
LAN 1 ESTE	G0/1	900
LAN 2 ESTE	G0/0	900
LAN 1 OESTE	G0/0	250
LAN 2 OESTE	G0/1	500

Parte 2: determinar la solución

a. Determine la solución para los errores de direccionamiento y corrija el registro en la tabla de direccionamiento.

b. Una vez corregido el esquema de direccionamiento, analice las rutas resumidas para ver si existen errores. Debe haber una ruta resumida para ambas LAN de cada router.

c. En la siguiente tabla Registro de resolución de problemas, registre los errores y la solución para cada problema que se encuentre.

Registro de resolución de problemas

Problema	Solución
La máscara de subred de la interfaz G0/0 de HQ es incorrecta.	La máscara de subred correcta debe ser 255.255.252.0.
La máscara de subred de la interfaz G0/1 de HQ es incorrecta.	La máscara de subred correcta debe ser 255.255.248.0.
La máscara de subred de la LAN 1 de HQ es incorrecta.	La máscara de subred correcta debe ser 255.255.248.0.
La máscara de subred de la LAN 2 de HQ es incorrecta.	La máscara de subred correcta debe ser 255.255.252.0.
La ruta resumida de las LAN de HQ en el router ESTE es incorrecta.	La ruta resumida correcta debe ser ip route 172.16.32.0 255.255.240.0 10.10.10.5.
La ruta resumida de las LAN de HQ en el router OESTE es incorrecta.	La ruta resumida correcta debe ser ip route 172.16.32.0 255.255.240.0 10.10.10.2.

Parte 3: Implemente la solución

a. Corrija los errores de direccionamiento.

```
HQ(config)# interface g0/0
HQ(config-if)# ip address 172.16.40.1 255.255.252.0
HQ(config-if)# interface g0/1
HQ(config-if)# ip address 172.16.32.1 255.255.248.0
```

```
HQ_LAN1(config)# interface vlan 1
HQ_LAN1(config-if)# ip address 172.16.32.2 255.255.248.0
HQ_LAN2(config)# interface vlan 1
HQ_LAN2(config-if)# ip address 172.16.40.2 255.255.252.0
```

b. Corrija los errores de rutas resumidas.

```
EAST(config)# no ip route 172.16.32.0 255.255.248.0 10.10.10.2
EAST(config)# ip route 172.16.32.0 255.255.240.0 10.10.10.2
WEST(config)# no ip route 172.16.32.0 255.255.248.0 10.10.10.5
WEST(config)# ip route 172.16.32.0 255.255.240.0 10.10.10.5
```

Parte 4: verificar que los problemas estén resueltos

Haga ping a cada switch desde LAN1_ESTE. Si falla, vuelva a revisar las configuraciones de las rutas resumidas y el esquema de direccionamiento.

Tabla de calificación sugerida

Sección de la actividad	Puntos posibles	Puntos obtenidos
Tabla de direccionamiento	**25**	
Registro de resolución de problemas	**25**	
Puntuación de Packet Tracer	**50**	
Puntuación total	**100**	

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

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

Topología

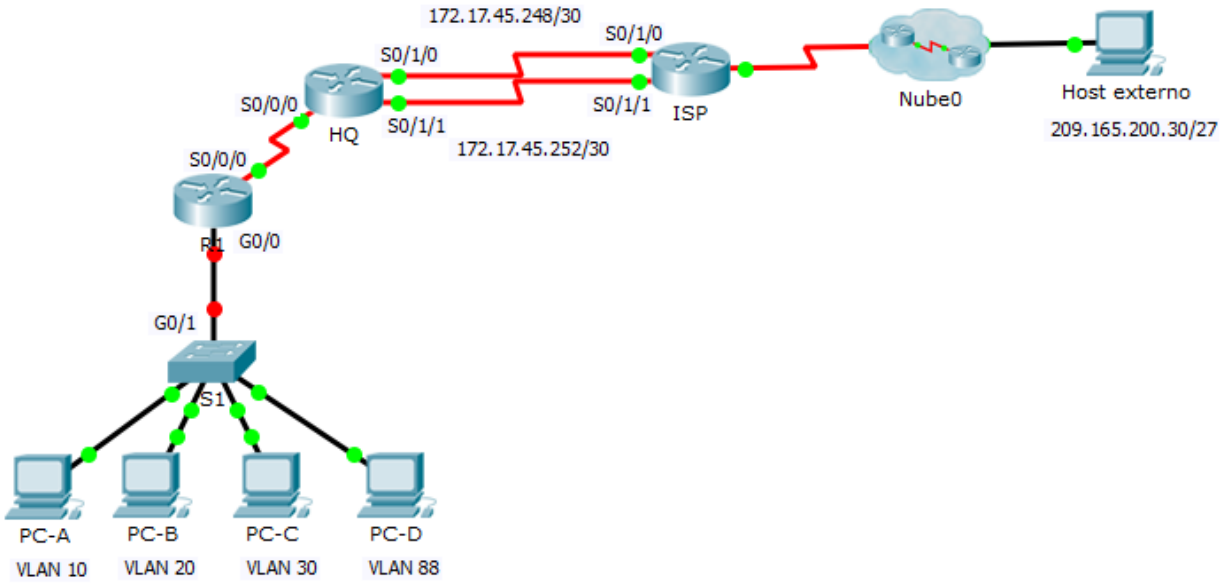


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	VLAN
R1	S0/0/0	172.31.1.1	255.255.255.0	N/A	N/A
	G0/0.10	172.31.10.1	255.255.255.0	N/A	10
	G0/0.20	172.31.20.1	255.255.255.0	N/A	20
	G0/0.30	172.31.30.1	255.255.255.0	N/A	30
	G0/0.88	172.31.88.1	255.255.255.0	N/A	88
	G0/0.99	172.31.99.1	255.255.255.0	N/A	99
S1	VLAN 88	172.31.88.33	255.255.255.0	172.17.88.1	88
PC-A	NIC	172.31.10.21	255.255.255.0	172.17.10.1	10
PC-B	NIC	172.31.20.22	255.255.255.0	172.17.20.1	20
PC-C	NIC	172.31.30.23	255.255.255.0	172.17.30.1	30
PC-D	NIC	172.31.88.24	255.255.255.0	172.31.88.1	88

Tabla de VLAN

VLAN	Nombre	Interfaces
10	Ventas	F0/11-15
20	Producción	F0/16-20
30	Marketing	F0/5-10
88	Management	F0/21-24
99	Nativo	G0/1

Situación

En esta actividad, demostrará y reforzará su habilidad para configurar routers destinados a la comunicación entre VLAN, al igual que rutas estáticas para llegar a destinos fuera de su red. Entre las habilidades que demostrará se incluye la configuración de routing entre VLAN y de rutas estáticas y predeterminadas.

Requisitos

- Configure el routing entre VLAN en el **R1** según la **tabla de direccionamiento**.
- Configure el enlace troncal en el **S1**.
- Configure cuatro rutas estáticas conectadas directamente en **HQ** para llegar a las VLAN 10, 20, 30 y 88.
- Configure las rutas estáticas conectadas directamente en **HQ** para llegar al **host externo**.
  - Configure la ruta principal a través de la interfaz Serial 0/1/0.
  - Configure la ruta de respaldo a través de la interfaz Serial 0/1/1 con una AD de 10.

- Configure la ruta principal conectada directamente y la ruta de respaldo resumida en el **ISP** para todo el espacio de direcciones 172.31.0.0/17.
  - Configure la ruta principal a través de la interfaz Serial 0/1/1.
  - Configure la ruta de respaldo a través de la interfaz Serial 0/1/0 con una AD de 25.
- Configure una ruta predeterminada conectada directamente en el **R1**.
- Verifique la conectividad asegurándose de que todas las computadoras puedan hacer ping al **host externo**.

Modelos de respuestas

```
!R1!!!!!!!!!!!!!!!!!!
en
config t
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.10
 description Sales VLAN
 encapsulation dot1Q 10
 ip address 172.31.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 description Production VLAN
 encapsulation dot1Q 20
 ip address 172.31.20.1 255.255.255.0
!
interface GigabitEthernet0/0.30
 description Marketing VLAN
 encapsulation dot1Q 30
 ip address 172.31.30.1 255.255.255.0
!
interface GigabitEthernet0/0.88
 description Management VLAN
 encapsulation dot1Q 88
 ip address 172.31.88.1 255.255.255.0
!
interface GigabitEthernet0/0.99
 description Native VLAN
 encapsulation dot1Q 99 native
 ip address 172.31.99.1 255.255.255.0
!
```



```
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
end

!S1!!!!!!!!!!!!!!!!!!!!!!!!!
en
config t
int g0/1
switchport mode trunk
switchport trunk native vlan 99
end
wr

!HQ!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip route 172.31.10.0 255.255.255.0 Serial0/0/0
ip route 172.31.20.0 255.255.255.0 Serial0/0/0
ip route 172.31.30.0 255.255.255.0 Serial0/0/0
ip route 172.31.88.0 255.255.255.0 Serial0/0/0
ip route 209.165.200.0 255.255.255.224 Serial0/1/0
ip route 209.165.200.0 255.255.255.224 Serial0/1/1 10
end
wr

!ISP!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip route 172.31.0.0 255.255.128.0 Serial0/1/1
ip route 172.31.0.0 255.255.128.0 Serial0/1/0 25
end
wr
```

Packet Tracer: investigación de la convergencia (versión para el instructor)

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

Topología

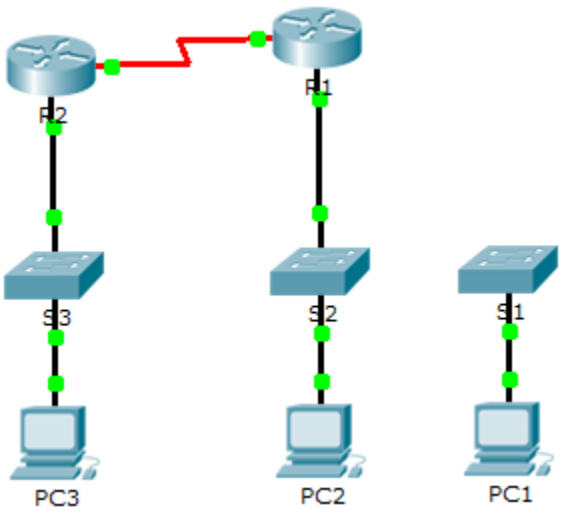


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	209.165.0.1	255.255.255.0	N/A
	G0/1	64.100.0.1	255.0.0.0	N/A
	S0/0/0	192.168.1.2	255.255.255.0	N/A
R2	G0/0	10.0.0.1	255.0.0.0	N/A
	S0/0/0	192.168.1.1	255.255.255.0	N/A
PC1	NIC	64.100.0.2	255.0.0.0	64.100.0.1
PC2	NIC	209.165.0.2	255.255.255.0	209.165.0.1
PC3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objetivos

Parte 1: ver la tabla de routing de una red convergente

Parte 2: agregar una nueva LAN a la topología

Parte 3: observar la convergencia de la red

Información básica

Esta actividad lo ayudará a identificar información importante en las tablas de routing y a observar el proceso de convergencia de la red.

Parte 1: ver la tabla de routing de una red convergente

Paso 1: utilizar comandos show e interpretar el resultado.

a. Muestre las redes conectadas directamente del **R1**. ¿Cuántas rutas se conectan al **R1**? 2

```
R1# show ip route connected
```

b. Muestre la configuración en ejecución del **R1**. ¿Qué protocolo de routing está en uso? RIP

c. En la configuración que anuncia RIP, ¿las direcciones IP son las mismas que las de las redes que están conectadas? Sí

d. Estas direcciones IP ¿son asignables, de red o de difusión? Red

e. Muestre las redes del **R1** descubiertas mediante RIP. ¿Cuántas rutas hay? 1

```
R1# show ip route rip
```

f. Muestre todas las redes que tiene el **R1** en su tabla de routing. ¿Qué significan las letras iniciales?

C = conectada, R = RIP, L = local

```
R1# show ip route
```

g. Repita el paso 1, del punto a al f en el **R2**. Compare el resultado de los dos routers.

Paso 2: verificar el estado de la topología.

a. Haga ping de la **PC2** a la **PC3**. El ping debería realizarse correctamente.

b. Muestre el estado de las interfaces en el **R2**. Dos interfaces deben tener direcciones asignadas. Cada dirección corresponde a una red conectada.

```
R2# show ip interface brief
```

c. Muestre el estado de las interfaces en el **R1**. ¿Cuántas interfaces tienen redes asignadas? 3

```
R1# show ip interface brief
```

Parte 2: agregar una nueva LAN a la topología

Paso 1: agregar un cable Ethernet.

a. Conecte el cable Ethernet correcto del **S1** al puerto correspondiente en el **R1**.

b. Haga ping de la **PC1** a la **PC2** una vez que el puerto afectado del **S1** se torne de color verde. ¿Elping fue exitoso? Sí

c. Haga ping de la **PC1** a la **PC3**. ¿Elping fue exitoso? ¿Por qué?

No, el R1 no está anuncia la red 64.0.0.0 al R2, el cual no podía devolver los paquetes.

Paso 2: configurar una ruta.

a. Cambie del Modo de tiempo real al Modo de simulación.

b. Introduzca una nueva ruta en el **R1** para la red 64.0.0.0.

```
R1(config)# router rip
R1(config-router)# network 64.0.0.0
```

c. Examine las PDU que salen del **R1**. ¿De qué tipo son? RIPv1

Parte 3: observar la convergencia de la red

Paso 1: utilizar comandos debug.

a. Habilite la depuración en el **R2**.

```
R2# debug ip rip
R2# debug ip routing
```

b. Como referencia, muestre la tabla de routing del **R2** como en el paso 1f.

c. Haga clic en **Capture/Forward** (Capturar/Adelantar) en el modo de simulación. ¿Qué notificación apareció en la terminal del **R2**?

Hubo una actualización de RIPv1 desde el R1.

d. Según el resultado de la depuración, ¿a cuántos saltos del R2 está 64.0.0.0? Un salto.

e. ¿Qué interfaz utiliza el **R2** para enviar los paquetes destinados a la red 64.0.0.0? S0/0/0

f. Muestre la tabla de routing del **R2**. Registre la nueva entrada.

R 64.0.0.0/8 [120/1] via 192.168.1.2, 00:00:00, Serial0/0/0

Paso 2: verificar el estado de la topología.

Haga ping de la **PC1** a la **PC3**. ¿Elping fue exitoso? ¿Por qué?

Sí, el R1 anunció la red 64.0.0.0 al R2 que pudo devolver los paquetes.

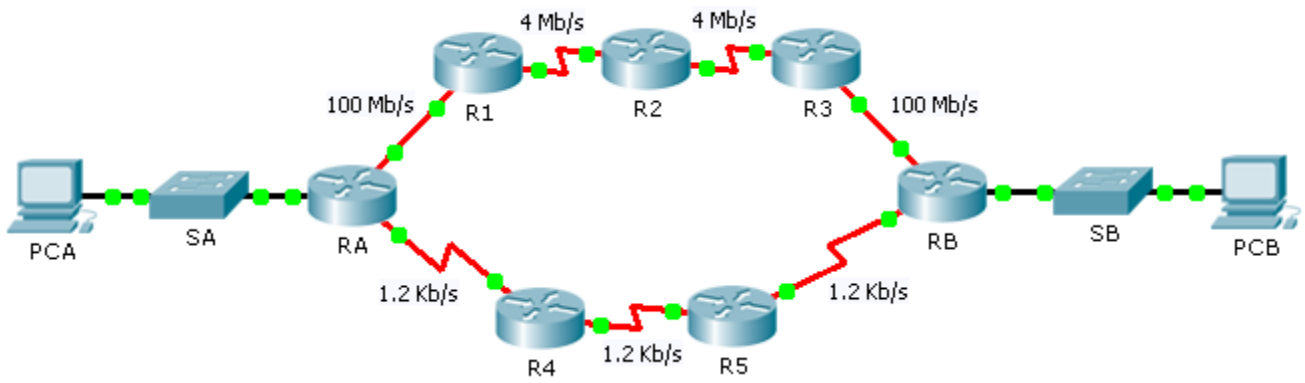
Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: ver la tabla de routing de una red convergente	Paso 1-a	6	
	Paso 1-b	6	
	Paso 1-c	6	
	Paso 1-d	6	
	Paso 1-e	6	
	Paso 1-f	6	
	Paso 2-c	6	
Total de la parte 1		**42**	
Parte 2: agregar una nueva LAN a la topología	Paso 1-b	6	
	Paso 1-c	6	
	Paso 2-c	6	
Total de la parte 2		**18**	
Parte 3: observar la convergencia de la red	Paso 1-c	6	
	Paso 1-d	6	
	Paso 1-e	6	
	Paso 1-f	6	
	Paso 2-a	6	
Total de la parte 3		**30**	
Puntuación de Packet Tracer		**10**	
Puntuación total		**100**	

Packet Tracer: comparación de la selección de rutas RIP y EIGRP (versión para el instructor)

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

Topología



Objetivos

Parte 1: predecir la ruta

Parte 2: rastrear la ruta

Parte 3: preguntas de reflexión

Situación

La **PCA** y la **PCB** necesitan comunicarse. La ruta que toman los datos entre estas terminales puede recorrer el **R1**, el **R2** y el **R3**, o bien el **R4** y el **R5**. El proceso por el cual los routers seleccionan la mejor ruta depende del protocolo de routing. Examinaremos el comportamiento de dos protocolos de routing vector distancia: el protocolo de routing de gateway interior mejorado (EIGRP) y el protocolo de información de routing versión 2 (RIPv2).

Parte 1: predecir la ruta

Las métricas son factores que se pueden medir. En el diseño de cada protocolo de routing se tienen en cuenta las diferentes métricas en el momento de considerar cuál es la mejor ruta para enviar datos. Estas métricas incluyen el conteo de saltos, el ancho de banda, el retraso, la confiabilidad y el costo de la ruta, entre otros factores.

Parte 1: considerar las métricas de EIGRP.

a. El EIGRP puede considerar muchas métricas. Sin embargo, las métricas que utiliza de manera predeterminada para determinar la selección de la mejor ruta son el ancho de banda y el retraso.

b. Sobre la base de las métricas, ¿qué ruta cree que seguirán los datos desde la **PCA** hasta la **PCB**? PCA, RA, R1, R2, R3, RB, PCB

Parte 2: considerar las métricas de RIP.

a. ¿Qué métricas utiliza el protocolo RIP? Conteo de saltos

b. Sobre la base de las métricas, ¿qué ruta cree que seguirán los datos desde la **PCA** hasta la **PCB**? PCA, RA, R4, R5, RB, PCB

Parte 2: rastrear la ruta

Parte 1: examinar la ruta EIGRP.

a. En el **RA**, utilice el comando adecuado para ver la tabla de routing. ¿Qué códigos de protocolo se indican en la tabla y qué protocolos representan? C = conectado y D = EIGRP

b. Rastree la ruta de la **PCA** a la **PCB**.

¿Qué ruta siguen los datos? 64.100.0.254, 64.101.0.2, 64.101.0.6, 64.101.0.10, 64.101.0.14

¿A cuántos saltos está el destino? 5 saltos

¿Cuál es el ancho de banda mínimo en la ruta? 4 Mb/s

Parte 2: examinar la ruta RIPv2.

Es posible que haya advertido que, mientras se configura RIPv2, los routers omiten las rutas que genera, porque prefieren el EIGRP. Los routers Cisco utilizan una escala llamada “distancia administrativa”, y es necesario cambiar ese número para que RIPv2 en el **RA** haga que el router prefiera el protocolo.

a. Para fines de referencia, utilice el comando adecuado para mostrar la tabla de routing del **RA**. ¿Cuál es el primer número entre corchetes de cada entrada de ruta EIGRP? 90

b. Establezca la distancia administrativa de RIPv2 con los siguientes comandos. Esto hace que el **RA** elija las rutas RIP por sobre las rutas EIGRP.

```
RA(config)# router rip
RA(config-router)# distance 89
```

c. Espere un minuto y muestre la tabla de routing nuevamente. ¿Qué códigos de protocolo se indican en la tabla y qué protocolos representan? C = conectado y R = RIP

d. Rastree la ruta de la **PCA** a la **PCB**.

¿Qué ruta siguen los datos? 64.100.0.254, 64.102.0.2, 64.102.0.6, 64.102.0.14

¿A cuántos saltos está el destino? 4 saltos

¿Cuál es el ancho de banda mínimo en la ruta? 1,2 Kb/s

e. ¿Cuál es el primer número entre corchetes de cada entrada de ruta RIP? 89

Parte 3: Preguntas de reflexión

1. ¿Qué métricas omite el protocolo de routing RIPv2? Todas menos los saltos.

   ¿Cómo podría afectar su rendimiento? La respuesta variará. RIP omitirá la ruta con el ancho de banda más rápido.

2. ¿Qué métricas omite el protocolo de routing EIGRP? Los saltos.

   ¿Cómo podría afectar su rendimiento? La respuesta varía. Es posible que un paquete se descarte si pasa por más saltos que los que permite su valor de TTL.

3. Para acceder a Internet, ¿prefiere menos saltos o más ancho de banda? Respuesta abierta.
4. ¿Es adecuado un solo protocolo de routing para todas las aplicaciones? ¿Por qué? Respuesta abierta.

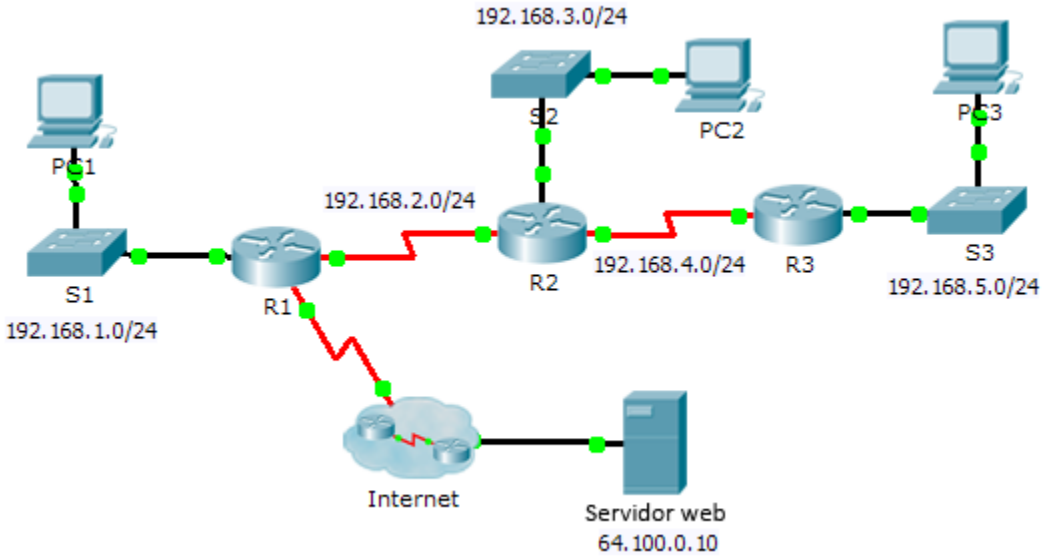
Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: predecir la ruta	Paso 1-b	8	
	Paso 2-a	8	
	Paso 2-b	8	
	Total de la parte 1	24	
Parte 2: rastrear la ruta	Paso 1-a	8	
	Paso 1-b	8	
	Paso 2-a	8	
	Paso 2-c	8	
	Paso 2-d	8	
	Paso 2-e	8	
	Total de la parte 2	48	
Parte 3: preguntas de reflexión	1	7	
	2	7	
	3	7	
	4	7	
	Total de la parte 3	28	
	Puntuación total	100	

Packet Tracer: configuración de RIPv2 (versión para el instructor)

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

Topología



Objetivos

Parte 1: configurar RIPv2

Parte 2: verificar las configuraciones

Información básica

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

Parte 1: Configurar RIPv2

Paso 1: configurar RIPv2 en el R1.

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

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

b. Ingrese al modo de configuración del protocolo RIP.

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

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

```
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

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

```
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
```

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

```
R1(config-router)# passive-interface gig 0/0
```

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

```
R1(config-router)# default-information originate
```

g. Guarde la configuración.

Paso 2: configurar RIPv2 en el R2.

a. Ingrese al modo de configuración del protocolo RIP.

```
R2(config)# router rip
```

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

```
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

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

```
R2(config-router)# network 192.168.2.0
R2(config-router)# network 192.168.3.0
R2(config-router)# network 192.168.4.0
```

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

```
R2(config-router)# passive-interface gig 0/0
```

e. Guarde la configuración.

Paso 3: configurar RIPv2 en el R3.

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

```
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# no auto-summary
R3(config-router)# network 192.168.4.0
R3(config-router)# network 192.168.5.0
R3(config-router)# passive-interface gig 0/0
```

Parte 2: verificar las configuraciones

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

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

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

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

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

Packet Tracer: configuración de RIPng (versión para el instructor)

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

Topología

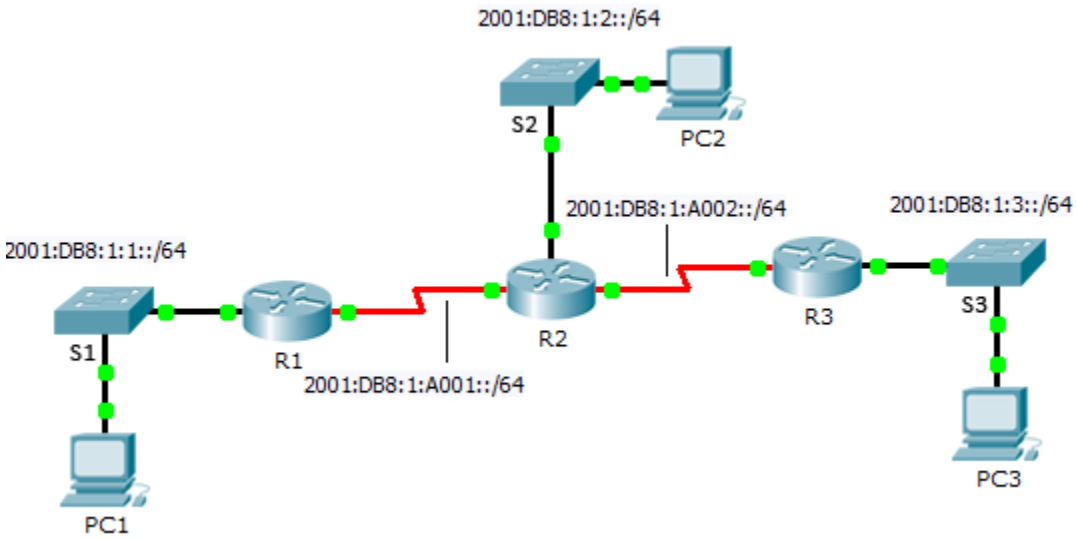


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar RIPng

Parte 2: verificar las configuraciones y la conectividad

Información básica

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

Parte 1: configurar RIPng

Paso 1: configurar RIPng en el R1.

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

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

b. Ingrese al modo de configuración del protocolo RIPng.

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

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

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

d. Guarde la configuración.

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

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

```
!R2
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router rip CISCO
R2(config-rtr)# int g0/0
R2(config-if)# ipv6 rip CISCO enable
R2(config-if)# int s0/0/0
R2(config-if)# ipv6 rip CISCO enable
R2(config-if)# int s0/0/1
R2(config-if)# ipv6 rip CISCO enable
!R3
R3(config)# ipv6 unicast-routing
R3(config)# ipv6 router rip CISCO
R3(config-rtr)# int g0/0
R3(config-if)# ipv6 rip CISCO enable
R3(config-if)# int s0/0/1
R3(config-if)# ipv6 rip CISCO enable
```

Parte 2: verificar las configuraciones y la conectividad

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

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

b. Verifique que las interfaces adecuadas utilicen RIPng.

```
R1# show ipv6 protocols
```

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

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

Paso 2: verificar la plena conectividad.

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

Packet Tracer: configuración de OSPFv2 en un área única (versión para el instructor)

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

Topología

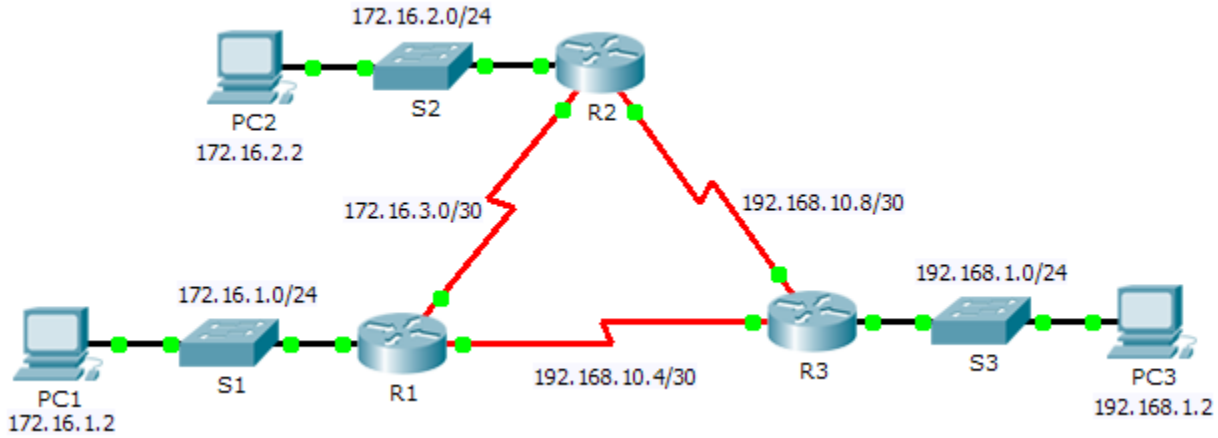


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar el routing OSPFv2

Parte 2: verificar las configuraciones

Información básica

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

Nota: la topología es la misma que se utilizó en los ejemplos del capítulo. Además, el estudiante practicó la configuración de esta topología en las actividades del verificador de sintaxis. Por lo tanto, el estudiante debe poder completar esta actividad con ayuda mínima.

Parte 1: configurar el routing OSPFv2

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

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

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

Paso 2: verificar que el routing OSPF funcione.

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

Parte 2: Verificación de las configuraciones

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

```
!--------------------------
!R1
!--------------------------
ena
conf t
!
router ospf 10
 router-id 1.1.1.1
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.3 area 0
 network 192.168.10.4 0.0.0.3 area 0
 passive-interface GigabitEthernet0/0
!
end

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

```
!R2
!-------------------------
ena
conf t
!
router ospf 10
 router-id 2.2.2.2
 network 172.16.2.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.3 area 0
 network 192.168.10.8 0.0.0.3 area 0
 passive-interface GigabitEthernet0/0
!
end

!-------------------------
!R3
!-------------------------
ena
conf t
!
router ospf 10
 router-id 3.3.3.3
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.10.4 0.0.0.3 area 0
 network 192.168.10.8 0.0.0.3 area 0
 passive-interface GigabitEthernet0/0
!
end
```

Packet Tracer: configuración de OSPFv3 básico en un área única (versión para el instructor)

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

Topología

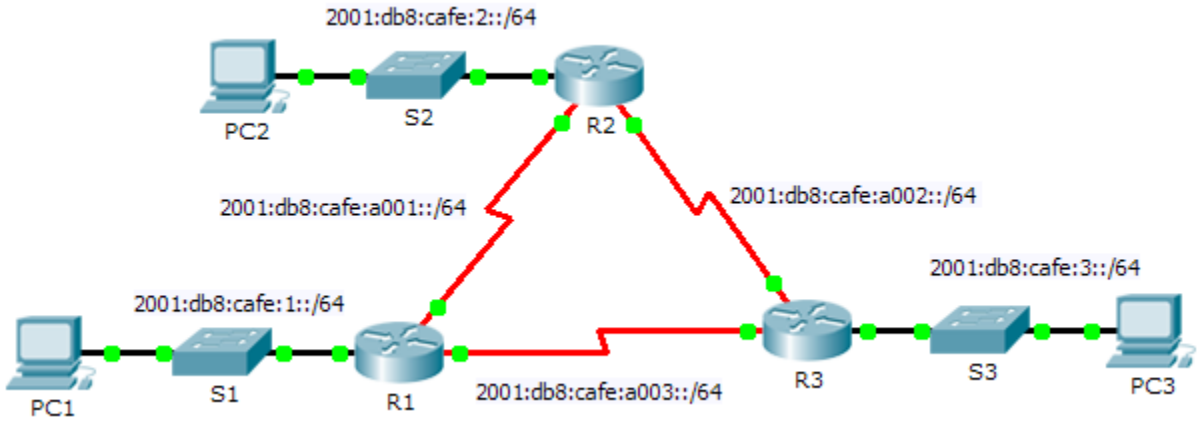


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar el routing OSPFv3

Parte 2: verificar la conectividad

Información básica

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

Nota: la topología es la misma que se utilizó en los ejemplos del capítulo. Además, el estudiante practicó la configuración de esta topología en las actividades del verificador de sintaxis. Por lo tanto, el estudiante debe poder completar esta actividad con ayuda mínima.

Parte 1: configurar el routing OSPFv3

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

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

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

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

Paso 2: verificar que el routing OSPF funcione.

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

Parte 2: Verificar la conectividad

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

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

```
!--------------------------
!R1
!--------------------------
ena
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 1.1.1.1
end
```

```
clear ipv6 ospf process
y

conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end

!--------------------------
!R2
!--------------------------
ena
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 2.2.2.2
end
clear ipv6 ospf process
y

conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
```

```
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end


!--------------------------
!R3
!--------------------------
ena
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 3.3.3.3
end
clear ipv6 ospf process
y

conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end
```

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

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

Topología

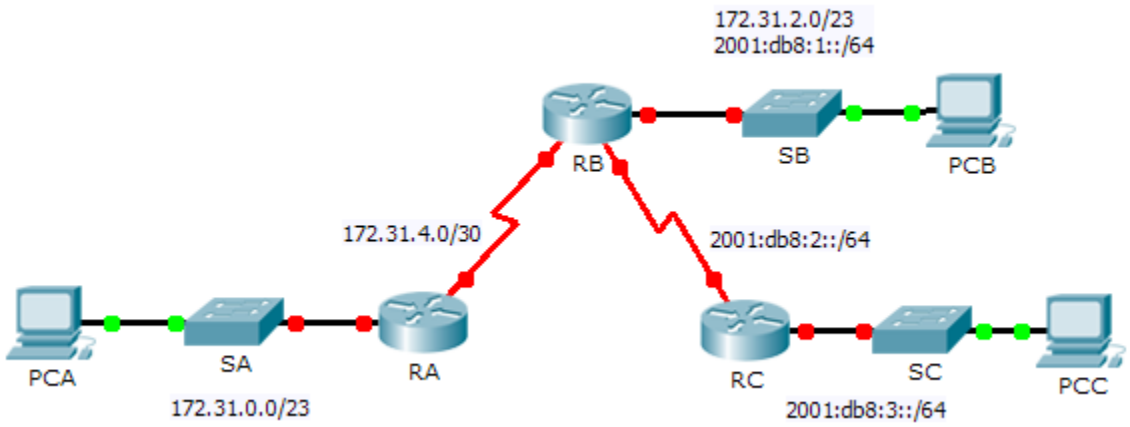


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4 / Dirección/Prefijo IPv6	Máscara de subred	Gateway predeterminado
RA	G0/0	172.31.0.1	255.255.254.0	N/A
	S0/1/0	172.31.4.1	255.255.255.252	N/A
RB	G0/0	172.31.2.1	255.255.254.0	N/A
		2001:DB8:1::1/64		N/A
	S0/0/0	172.31.4.2	255.255.255.252	N/A
	S0/0/1	2001:DB8:2::1/64		N/A
RC	G0/0	2001:DB8:3::1/64		N/A
	S0/0/1	2001:DB8:2::2/64		N/A
PC-A	NIC	172.31.1.254	255.255.254.0	172.31.0.1
PC-B	NIC	172.31.3.254	255.255.254.0	172.31.2.1
		2001:DB8:1::2/64		FE80::1
PC-C	NIC	2001:DB8:3::2/64		FE80::3

Información básica

En este desafío de integración de habilidades, debe concentrarse en la configuración de OSPFv2 y OSPFv3. Configurará el direccionamiento IP para todos los dispositivos. A continuación, configurará el routing OSPFv2 para la porción IPv4 de la red y el routing OSPFv3 para la porción IPv6 de la red. Se configurará un router con IPv4 e IPv6. Por último, verificará las configuraciones y probará la conectividad entre las terminales.

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

Requisitos

- Utilice los siguientes requisitos para configurar el direccionamiento del **RA** y el routing OSPFv2:
  - Direccionamiento IPv4 según la tabla de direccionamiento
  - ID de proceso 1
  - ID del router 1.1.1.1
  - Dirección de red de cada interfaz
  - Interfaz LAN configurada como pasiva (no utilice la palabra clave **default**)
- Utilice los siguientes requisitos para configurar el direccionamiento del **RB**, el routing OSPFv2 y el routing OSPFv3:
  - Direccionamiento IPv4 e IPv6 según la tabla de direccionamiento
    - Dirección link-local de Gigabit Ethernet 0/0 establecida en FE80::1
  - Requisitos de routing OSPFv2:
    - ID de proceso 1
    - ID del router 2.2.2.2
    - Dirección de red de cada interfaz
    - Interfaz LAN configurada como pasiva (no utilice la palabra clave **default**)
  - Requisitos de routing OSPFv3:
    - Habilitación del routing IPv6
    - ID de proceso 1
    - ID del router 2.2.2.2
    - Habilitación de OSPFv3 en cada interfaz
- Utilice los siguientes requisitos para configurar el direccionamiento del **RC** y el routing OSPFv3:
  - Direccionamiento IPv6 según la tabla de direccionamiento
    - Dirección link-local de Gigabit Ethernet 0/0 establecida en FE80::3
  - Requisitos de routing OSPFv3:
    - Habilitación del routing IPv6
    - ID de proceso 1
    - ID del router 3.3.3.3
    - Habilitación de OSPFv3 en cada interfaz

- Configure las computadoras con el direccionamiento adecuado.
  - El direccionamiento IPv6 de la **PCB** y la **PCC** debe utilizar la dirección link-local FE80 como gateway predeterminado.
  - Finalice el registro de la tabla de direccionamiento.
- Verifique las configuraciones y pruebe la conectividad.
  - Deben haberse establecido los vecinos OSPF, y las tablas de routing deben estar completas.
  - Los pings de la PCA a la PCB deben ejecutarse de forma correcta.
  - Los pings de la PCB a la PCC deben ejecutarse de forma correcta.

    Nota: si no hubo convergencia de OSPFv3, revise el estado de interfaces mediante el comando **show ip ospf interface**. Es posible que, en ocasiones, sea necesario eliminar y volver a aplicar el proceso OSPFv3 para forzar la convergencia.

```
!----------------------------
!RA
!----------------------------
ena
config t
!
hostname RA
!
interface GigabitEthernet0/0
 ip address 172.31.0.1 255.255.254.0
 no shut
!
interface Serial0/0/0
 ip address 172.31.4.1 255.255.255.252
 no shut
!
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
 network 172.31.0.0 0.0.1.255 area 0
 network 172.31.4.0 0.0.0.3 area 0
!
end

!----------------------------
!RB
!----------------------------
ena
conf t
```



```
hostname RB
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 ip address 172.31.2.1 255.255.254.0
 ipv6 address 2001:DB8:1::1/64
 ipv6 address FE80::1 link-local
 ipv6 ospf 1 area 0
 no shut
!
interface Serial0/0/1
 no ip address
 ipv6 address 2001:DB8:2::1/64
 ipv6 ospf 1 area 0
 no shut
!
interface Serial0/0/0
 ip address 172.31.4.2 255.255.255.252
 no shut
!
router ospf 1
 router-id 2.2.2.2
 passive-interface GigabitEthernet0/0
 network 172.31.2.0 0.0.1.255 area 0
 network 172.31.4.0 0.0.0.3 area 0
!
ipv6 router ospf 1
router-id 2.2.2.2
end
clear ipv6 ospf process
y
!
!NOTE: If OSPFv3 does not converge, enter the following:
int g0/0
no ipv6 ospf 1 area 0
ipv6 ospf 1 area 0

!----------------------------
!RC
```

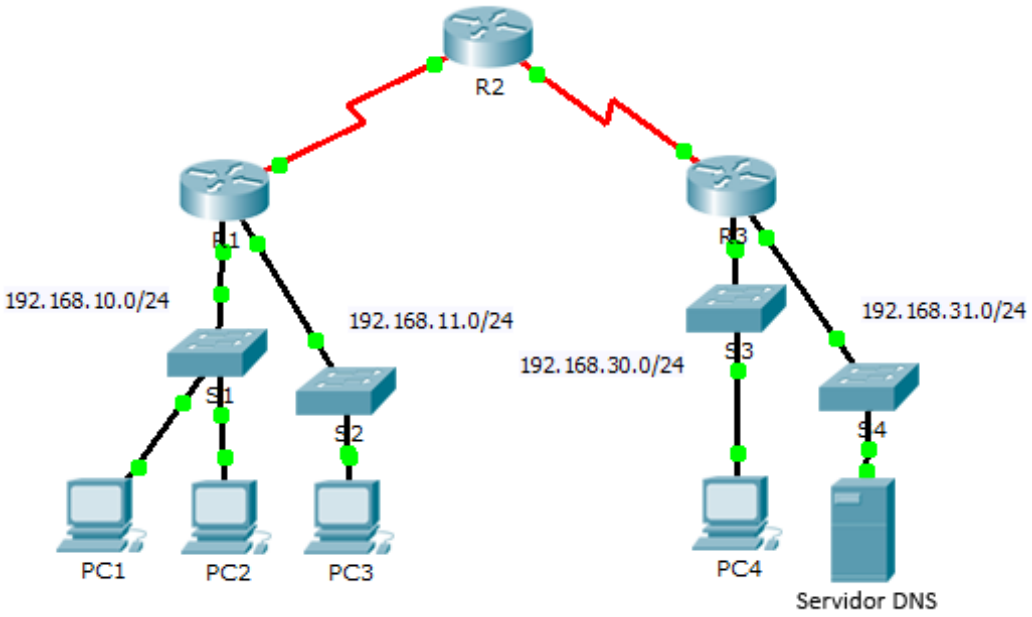


```
!----------------------------
ena
conf t
hostname RC
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:3::1/64
 ipv6 address FE80::3 link-local
 ipv6 ospf 1 area 0
 no shut
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:DB8:2::2/64
 ipv6 ospf 1 area 0
 no shut
!
ipv6 router ospf 1
router-id 3.3.3.3
end
clear ipv6 ospf process
y
!
```

Packet Tracer: demostración de listas de control de acceso (versión para el instructor)

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

Topología



Objetivos

Parte 1: verificar la conectividad local y probar la lista de control de acceso

Parte 2: eliminar la lista de control de acceso y repetir la prueba

Información básica

En esta actividad, observará cómo se puede utilizar una lista de control de acceso (ACL) para evitar que un ping llegue a hosts en redes remotas. Después de eliminar la ACL de la configuración, los pings se realizarán correctamente.

Parte 1: verificar la conectividad local y probar la lista de control de acceso

Paso 1: hacer ping a los dispositivos de la red local para verificar la conectividad.

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC2**.

b. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC3**.

¿Por qué se realizaron de forma correcta los pings? Por que las capas 1 a 3 funcionan correctamente y no existe una política que filtre los mensajes ICMP entre las dos redes locales.

Paso 2: hacer ping a los dispositivos en las redes remotas para probar la funcionalidad de la ACL.

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC4**.

b. Desde el símbolo del sistema de la **PC1**, haga ping al **servidor DNS**.

¿Por qué fallaron los pings? (Sugerencia: utilice el modo de simulación o vea las configuraciones del router para investigar). Los pings fallaron porque el R1 está configurado con una ACL que deniega la salida de cualquier ping por la interfaz serial 0/0/0.

Parte 2: eliminar la ACL y repetir la prueba

Paso 1: utilizar el comando show para investigar la configuración de la ACL.

a. Utilice los comandos **show run** y **show access-lists** para ver las ACL configuradas actualmente. Para obtener una vista rápida de las ACL vigentes, utilice **show access-lists**. Introduzca el comando **show access-lists** seguido de un espacio y un signo de interrogación (?) para ver las opciones disponibles:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Si conoce el número o el nombre de la ACL, puede filtrar aún más el resultado del comando **show**. Sin embargo, el **R1** tiene solo una ACL, por lo que basta con el comando **show access-lists**.

```
R1#show access-lists
Extended IP access list 101
    deny icmp any any echo
    permit ip any any
```

La primera línea de la ACL impide los ecos del protocolo de mensajes de control de Internet (ICMP) (es decir, las solicitudes de ping) desde **cualquier (any)** origen hasta **cualquier (any)** destino. La segunda línea de la ACL permite el resto del tráfico **ip** desde **cualquier (any)** origen hasta **cualquier (any)** destino.

b. Para que una ACL afecte el funcionamiento del router, debe aplicarse en algún lugar. En esta situación, la ACL se utiliza para filtrar el tráfico en una interfaz. Aunque pueda ver la información de IP con el comando **show ip interface**, en algunos casos puede ser más eficaz utilizar solo el comando **show run**. Al usar uno o ambos comandos, ¿a qué interfaz se aplica la ACL? Serial 0/0/0

Paso 2: eliminar la lista de acceso 101 de la configuración.

Es posible eliminar las ACL de la configuración por medio de la emisión del comando **no access list** *[número de ACL]*. El comando **no access-list** elimina todas las ACL configuradas en el router. El comando **no access-list** [*número de ACL*] solo elimina una ACL específica.

a. En el modo de configuración global, elimine la ACL por medio del siguiente comando:

```
R1(config)# no access-list 101
```

b. Verifique que la **PC1** ahora pueda hacer ping al **servidor DNS**.

Tabla de calificación sugerida

Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1, paso 1 b.	50	
Parte 1, paso 2 b.	40	
Parte 2, paso 2 b.	10	
Puntuación total	**100**	

Packet Tracer: configuración de ACL estándar (versión para el instructor)

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

Topología

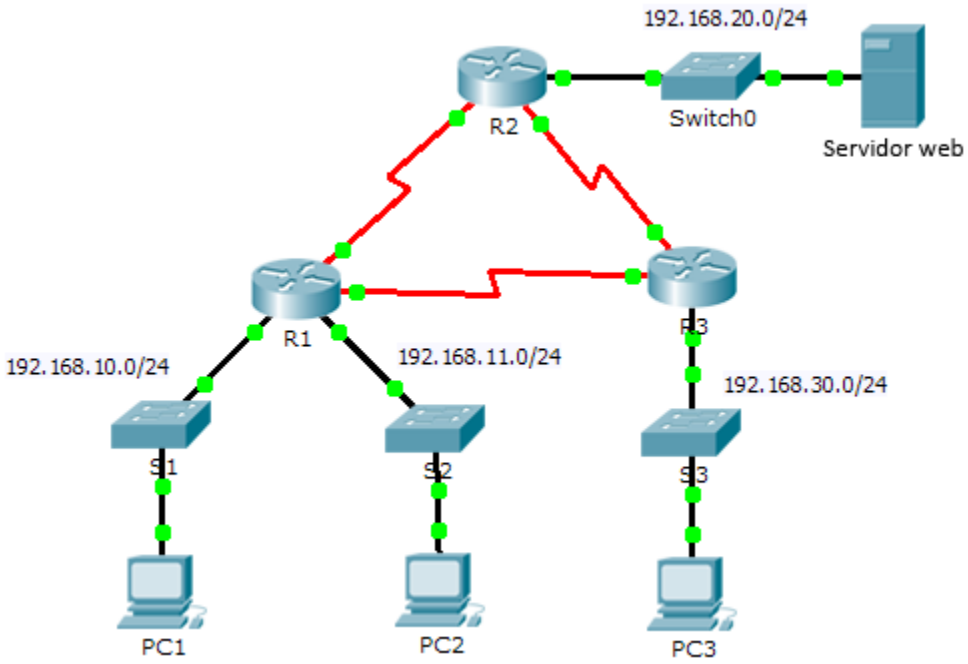


Tabla de direccionamiento

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

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Información básica/situación

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

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

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

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

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

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

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

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

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

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

Parte 2: configurar, aplicar y verificar una ACL estándar

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Packet Tracer: configuración de ACL estándar con nombre (versión para el instructor)

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

Topología

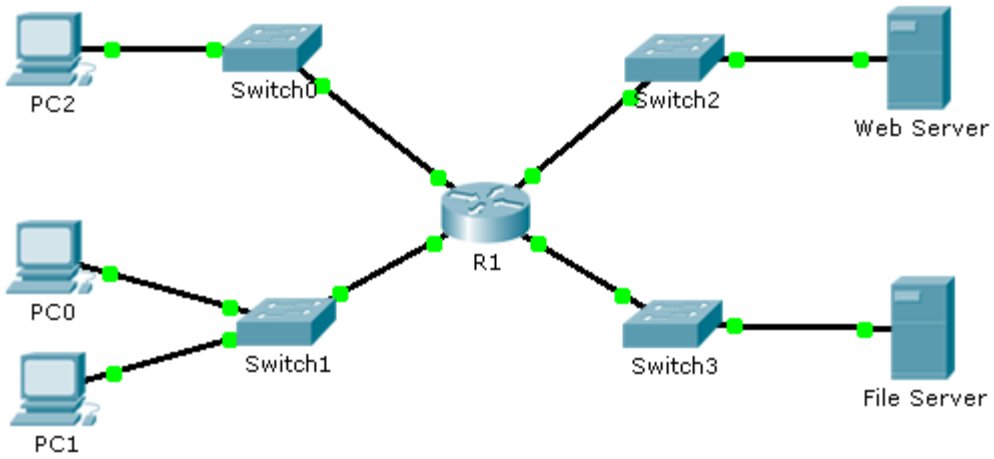


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar y aplicar una ACL estándar con nombre

Parte 2: verificar la implementación de la ACL

Información básica/situación

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

Parte 1: configurar y aplicar una ACL estándar con nombre

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

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

Paso 2: configurar una ACL estándar con nombre.

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

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

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

Paso 3: aplicar la ACL con nombre.

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

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

b. Guarde la configuración.

Parte 2: verificar la implementación de la ACL

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

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

Paso 2: verificar que la ACL funcione correctamente.

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

Packet Tracer: configuración de una ACL en líneas VTY (versión para el instructor)

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

Topología

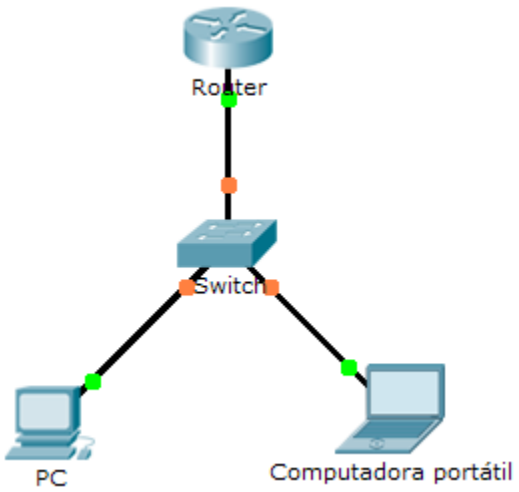


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Computadora portátil	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objetivos

Parte 1: configurar y aplicar una ACL a las líneas VTY

Parte 2: verificar la implementación de la ACL

Información básica

Como administrador de red, debe tener acceso remoto al router. Este acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permita el acceso de una computadora (**PC**) a las líneas Telnet, pero que deniegue el resto de las direcciones IP de origen.

Parte 1: configurar y aplicar una ACL a las líneas VTY

Paso 1: verificar el acceso por Telnet antes de configurar la ACL.

Ambas computadoras deben poder acceder al **Router** mediante Telnet. La contraseña es **cisco**.

Paso 2: configurar una ACL estándar numerada.

Configure la siguiente ACL numerada en el **Router**.

```
Router(config)# access-list 99 permit host 10.0.0.1
```

Ya que no deseamos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita de la lista de acceso cumple nuestros requisitos.

Paso 3: colocar una ACL estándar con nombre en el router.

Se debe permitir el acceso a las interfaces del **Router** y se debe restringir el acceso por Telnet. Por lo tanto, debemos colocar la ACL en las líneas Telnet que van de 0 a 4. Desde la petición de entrada de configuración del **Router**, acceda al modo de configuración de línea de las líneas 0 a 4 y utilice el comando **access-class** para aplicar la ACL a todas las líneas VTY:

```
Router(config)# line vty 0 4
Router(config-line)# access-class 99 in
```

Parte 2: verificar la implementación de la ACL

Paso 1: verificar la configuración de la ACL y su aplicación a las líneas VTY.

Utilice el comando **show access-lists** para verificar la configuración de la ACL. Utilice el comando **show run** para verificar que la ACL esté aplicada a las líneas VTY.

Paso 2: verificar que la ACL funcione correctamente.

Ambas computadoras deben poder hacer ping al **Router**, pero solo la computadora **PC** debería poder acceder al Router mediante Telnet.

Packet Tracer: configuración de ACL extendidas, situación 1 (versión para el instructor)

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

Topología

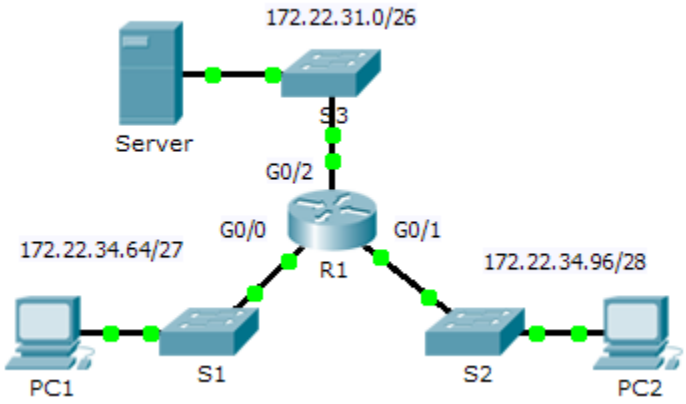


Tabla de direccionamiento

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

Objetivos

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

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

Información básica/situación

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

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

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

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

```
R1(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

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

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

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

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

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

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

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

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

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

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

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

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D  Destination address
  any      Any destination host
```



```
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

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

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

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

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

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

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

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

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

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

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


Paso 3: verificar la implementación de la ACL.

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

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

```
PC> ftp 172.22.34.62
```

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

```
ftp> quit
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Paso 3: verificar la implementación de la ACL.

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

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

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

Packet Tracer: configuración de ACL extendidas, situación 2 (versión para el instructor)

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

Topología

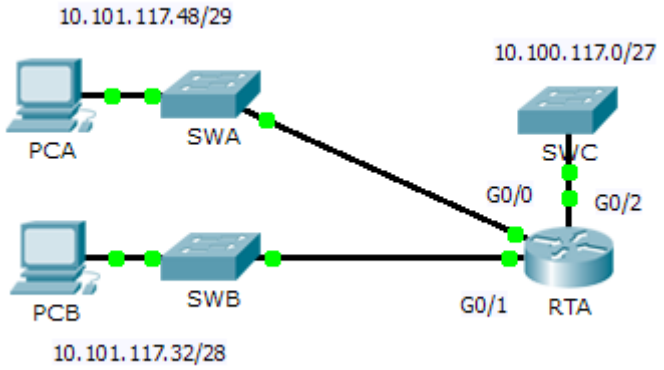


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RTA	G0/0	10.101.117.49	255.255.255.248	N/A
	G0/1	10.101.117.33	255.255.255.240	N/A
	G0/2	10.101.117.1	255.255.255.224	N/A
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWC	VLAN1	10.101.117.2	255.255.255.224	10.101.117.1

Objetivos

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

Parte 2: preguntas de reflexión

Información básica/situación

En esta situación, los dispositivos de una LAN pueden acceder de forma remota a los dispositivos de otra LAN mediante el protocolo Telnet. Aparte de ICMP, se deniega todo el tráfico de otras redes.

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

Configure, aplique y verifique una ACL para que cumpla con la siguiente política:

- Se permite el tráfico de Telnet desde los dispositivos de la red 10.101.117.32/28 hasta los dispositivos en las redes 10.100.117.0/27.
- Se permite el tráfico ICMP desde cualquier origen hasta cualquier destino.
- El tráfico restante está bloqueado.

Paso 1: configurar la ACL extendida.

a. Desde el modo de configuración adecuado en el **RTA**, utilice el último número válido de lista de acceso extendida para configurar la ACL. Utilice los siguientes pasos para crear la primera instrucción de ACL:

1) El último número de lista para ACL extendidas es 199.

2) El protocolo es TCP.

3) La red de origen es 10.101.117.32.

4) La máscara wildcard se puede determinar si se resta 255.255.255.240 a 255.255.255.255.

5) La red de destino es 10.101.117.0.

6) La máscara wildcard se puede determinar si se resta 255.255.255.224 a 255.255.255.255.

7) El protocolo es Telnet.

¿Cuál es la primera instrucción de ACL?

```
access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq telnet.
```

b. Se permite ICMP, y se necesita una segunda instrucción de ACL. Utilice el mismo número de lista de acceso para permitir todo el tráfico ICMP, independientemente de la dirección de origen o de destino. ¿Cuál es la segunda instrucción de ACL? (Sugerencia: utilice las palabras clave any).

```
access-list 199 permit icmp any any
```

c. El resto del tráfico IP se deniega de manera predeterminada.

Paso 2: aplicar el ACL extendida.

La regla general es colocar las ACL extendidas cerca del origen. Sin embargo, debido a que la lista de acceso 199 afecta al tráfico que se origina en las redes 10.101.117.48/29 y 10.101.117.32/28, la mejor ubicación para esta ACL puede ser la interfaz Gigabit Ethernet 0/2, en sentido de salida. ¿Cuál es el comando para aplicar la ACL 199 a la interfaz Gigabit Ethernet 0/2?

```
 ip access-group 199 out
```

Paso 3: verificar la implementación de la ACL extendida.

a. Haga ping de la **PCB** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

b. Desde la **PCB**, acceda al **SWC** mediante Telnet. La contraseña es **cisco**.

c. Salga del servicio de Telnet del **SWC**.

d. Haga ping de la **PCA** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

e. Desde la **PCA**, acceda al **SWC** mediante Telnet. La lista de acceso ocasiona que el router rechace la conexión.

f. Desde la **PCA**, acceda al **SWB** mediante Telnet. La lista de acceso está colocada en **G0/2** y no afecta esta conexión.

g. Una vez que inicie sesión en el **SWB**, no salga. Acceda al **SWC** mediante Telnet.

Parte 2: Preguntas de reflexión

1. ¿Cómo pudo la PCA omitir la lista de acceso 199 y acceder al SWC mediante Telnet? Se siguieron dos pasos: primero, la PCA utilizó Telnet para acceder al SWB. Desde el SWB, pudo acceder al SWC mediante Telnet.
2. ¿Qué se podría haber hecho para evitar que la PCA acceda indirectamente al SWC y, al mismo tiempo, permitir el acceso de la PCB al SWC por Telnet? La lista de acceso 199 debería haberse escrito para denegar el tráfico de Telnet de la red 10.101.117.48 /29 y permitir ICMP al mismo tiempo. Debería haberse colocado en G0/0 del RTA.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: configurar, aplicar y verificar una ACL extendida numerada	Paso 1a	4	
	Paso 1b	4	
	Paso 2	4	
Total de la parte 1		**12**	
Parte 2: preguntas de reflexión	Pregunta 1	4	
	Pregunta 2	4	
Total de la parte 2		**8**	
Puntuación de Packet Tracer		**80**	
Puntuación total		**100**	

Packet Tracer: configuración de ACL extendidas, situación 3 (versión para el instructor)

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

Topología

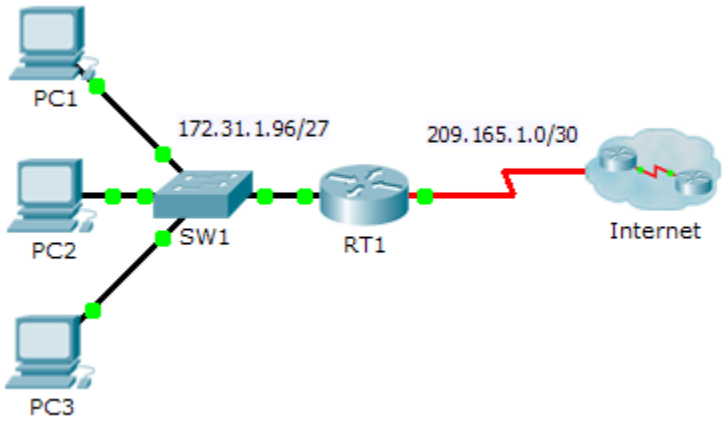


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254	255.254.0.0	64.100.1.1
Server2	NIC	64.103.255.254	255.254.0.0	64.102.1.1

Objetivos

Parte 1: configurar una ACL extendida con nombre

Parte 2: aplicar y verificar la ACL extendida

Información básica/situación

En esta situación, se permite que determinados dispositivos de la LAN tengan acceso a varios servicios en servidores ubicados en Internet.

Parte 1: Configurar una ACL extendida y nombrada

Utilice una ACL con nombre para implementar la política siguiente:

- Bloquee el acceso HTTP y HTTPS desde la **PC1** hasta el **Servidor1** y el **Servidor2** .Los servidores están dentro de la nube, y solo conoce sus direcciones IP.
- Bloquee el acceso FTP desde la **PC2** hasta el **Servidor1** y el **Servidor2.**
- Bloquee el acceso ICMP desde la **PC3** hasta el **Servidor1** y el **Servidor2.**

Nota: a los fines de la puntuación, las instrucciones se deben configurar en el orden que se especifica en los siguientes pasos.

Paso 1: denegar a la PC1 el acceso a los servicios HTTP y HTTPS en el Servidor1 y el Servidor2.

a. Cree una ACL de IP extendida con nombre que le deniegue a la **PC1** el acceso a los servicios HTTP y HTTPS del **Servidor1** y el **Servidor2**. Ya que no es posible observar directamente la subred de servidores en Internet, se necesitan cuatro reglas.

¿Cuál es el comando para iniciar la ACL con nombre?

```
ip access-list extended ACL
```

b. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTP (puerto 80).

```
deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
```

c. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTPS (puerto 443).

```
deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
```

d. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTP.

```
deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
```

e. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTPS.

```
deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Paso 2: denegar a la PC2 el acceso a los servicios FTP en el Servidor1 y el Servidor2.

a. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor1** solo para FTP (puerto 21 únicamente).

```
deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
```

b. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor2** solo para FTP (puerto 21 únicamente).

```
deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```

Paso 3: denegar a la PC3 que haga ping al Servidor1 y al Servidor2.

a. Registre la instrucción que deniega el acceso ICMP de la **PC3** al **Servidor1**.

```
deny icmp host 172.31.1.103 host 64.101.255.254
```

b. Registre la instrucción que deniega el acceso ICMP de la **PC3** al **Servidor2**.

```
deny icmp host 172.31.1.103 host 64.103.255.254
```

Paso 4: permitir todo el tráfico IP restante.

De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con alguna regla de la lista. ¿Qué comando permite el resto del tráfico?

```
permit ip any any
```

Parte 2: aplicar y verificar la ACL extendida

El tráfico que se filtrará proviene de la red 172.31.1.96/27 y tiene como destino las redes remotas. La ubicación adecuada de la ACL también depende de la relación del tráfico con respecto al **RT1**.

Paso 1: aplicar la ACL a la interfaz apropiada en el sentido correcto.

a. ¿Cuáles son los comandos que necesita para aplicar la ACL a la interfaz apropiada en el sentido correcto?

```
interface g0/0
 ip access-group ACL in
```

Paso 2: probar el acceso de cada computadora.

a. Acceda a los sitios web del **Servidor1** y **Servidor2** mediante el navegador web de la **PC1** con los protocolos HTTP y HTTPS.

b. Acceda al **Servidor1** y el **Servidor2** mediante FTP con la **PC1**. El nombre de usuario y la contraseña es "**cisco**".

c. Haga ping al **Servidor1** y al **Servidor2** desde la **PC1**.

d. Repita los pasos 2a hasta 2c con la **PC2** y la **PC3** para verificar que el funcionamiento de la lista de acceso sea correcto.

Packet Tracer: resolución de problemas de las ACL (versión para el instructor)

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

Topología

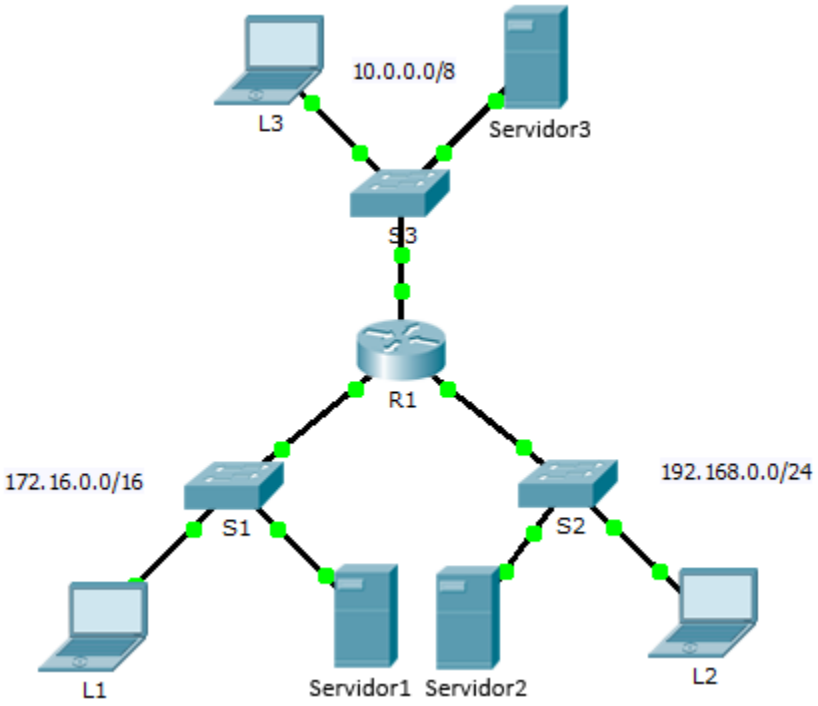


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
Server2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
Server3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objetivos

Parte 1: resolver el problema 1 de la ACL

Parte 2: resolver el problema 2 de la ACL

Parte 3: resolver el problema 3 de la ACL

Situación

En esta red, deberían estar implementadas las tres políticas siguientes:

- Los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del **Servidor3**.
- Los hosts de la red 10.0.0.0/8 no pueden acceder al servicio HTTP del **Servidor1**.
- Los hosts de la red 172.16.0.0/16 no pueden acceder al servicio FTP del **Servidor2**.

Nota: todos los nombres de usuario y las contraseñas del FTP son "**cisco**".

No debe haber otras restricciones. Lamentablemente, las reglas implementadas no funcionan de manera correcta. Su tarea es buscar y corregir los errores relacionados con las listas de acceso en el **R1**.

Parte 1: resolver el problema 1 de la ACL

Los hosts de la red 192.168.0.0/24 no pueden acceder (intencionalmente) a ningún servicio TCP del **Servidor3**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L2**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L2**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Desde la **L2**, haga ping a **G0/2** del **R1**.

d. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **192_to_10** y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

e. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **192_to_10** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

No llega tráfico debido a la instrucción deny any implícita. Se agregó una instrucción **permit ip any any** a la ACL.

Parte 2: resolver el problema 2 de la ACL

Los hosts de la red 10.0.0.0/8 no pueden acceder (intencionalmente) al servicio HTTP del **Servidor1**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L3**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L3**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **10_to_172** y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

d. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **10_to_172** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

Había una ACL aplicada en sentido de salida en G0/0. Se eliminó en sentido de salida y se aplicó en sentido de entrada en G0/0.

Parte 3: resolver el problema 3 de la ACL

Los hosts de la red 172.16.0.0/16 no pueden acceder (intencionalmente) al servicio FTP del **Servidor2**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L1**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L1**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **172_to_192** y su ubicación en las interfaces. ¿La lista de acceso se colocó en el puerto apropiado y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

d. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **172_to_192** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

Se permite todo el tráfico porque el orden de las instrucciones es incorrecto. Se deben reordenar las instrucciones de moto que **permit ip any any** sea la segunda instrucción.

Tabla de calificación sugerida

Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Puntuación del registro	10	
Puntuación de Packet Tracer	90	
Puntuación total	100	

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

Topología

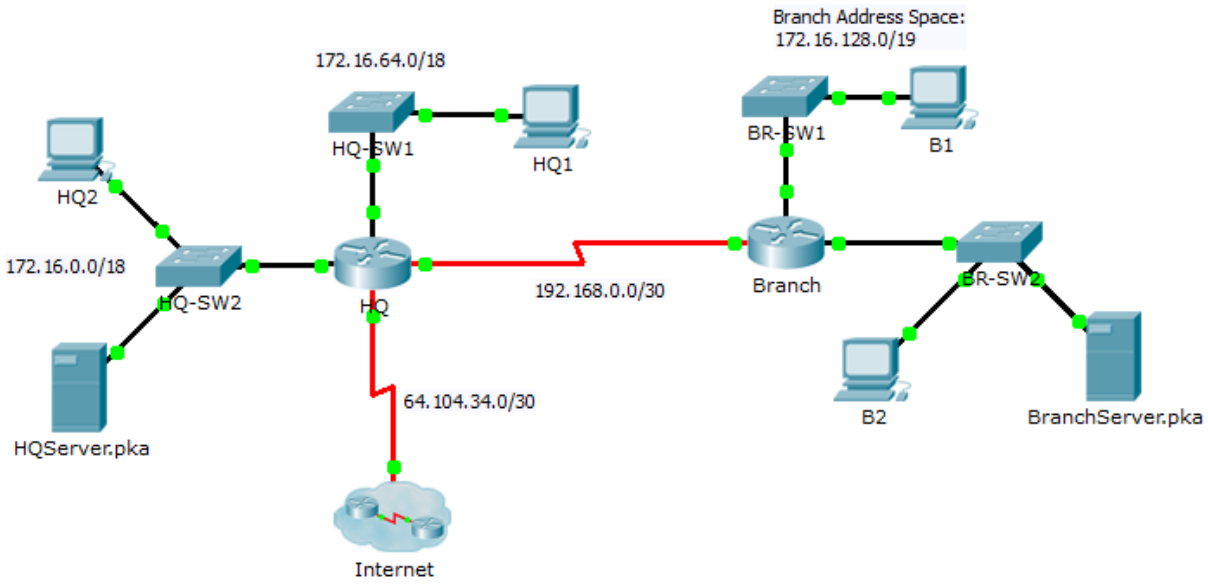


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
HQ	G0/0	172.16.127.254	255.255.192.0	N/A
	G0/1	172.16.63.254	255.255.192.0	N/A
	S0/0/0	192.168.0.1	255.255.255.252	N/A
	S0/0/1	64.104.34.2	255.255.255.252	64.104.34.1
Sucursal	G0/0	172.16.159.254	255.255.240.0	N/A
	G0/1	172.16.143.254	255.255.240.0	N/A
	S0/0/0	192.168.0.2	255.255.255.252	N/A
Oficina central 1	NIC	172.16.64.1	255.255.192.0	172.16.127.254
Oficina central 2	NIC	172.16.0.2	255.255.192.0	172.16.63.254
HQServer.pka	NIC	172.16.0.1	255.255.192.0	172.16.63.254
B1	NIC	172.16.144.1	255.255.240.0	172.16.159.254
B2	NIC	172.16.128.2	255.255.240.0	172.16.143.254
BranchServer.pka	NIC	172.16.128.1	255.255.240.0	172.16.143.254

Situación

En esta actividad del desafío, terminará el esquema de direccionamiento, configurará el routing e implementará listas de control de acceso con nombre.

Requisitos

a. Divida la red 172.16.128.0/19 en dos subredes iguales para utilizarse en **Sucursal**.
   1) Asigne la última dirección utilizable de la segunda subred a la interfaz Gigabit Ethernet 0/0.
   2) Asigne la última dirección utilizable de la primera subred a la interfaz Gigabit Ethernet 0/1.
   3) Registre el direccionamiento en la tabla de direccionamiento.
   4) Configure **Sucursal** con el direccionamiento adecuado.

b. Para configurar **B1** con el direccionamiento adecuado, utilice la primera dirección disponible de la red a la cual está conectada. Registre el direccionamiento en la tabla de direccionamiento.

c. Configure **Sucursal** con el protocolo de routing de gateway interior mejorado (EIGRP) según los criterios siguientes:
   - Anunciar las tres redes conectadas.
   - Asignar el número 1 a AS.
   - Desactivar la sumarización automática.
   - Configurar las interfaces adecuadas como pasivas.
   - Resumir 172.16.128.0/19 en la interfaz Serial 0/0/0 con una distancia administrativa de 5.

d. Establezca una ruta predeterminada en **HQ** que dirija el tráfico a la interfaz S0/0/1. Redistribuya la ruta a **Sucursal**.

e. Resuma las subredes LAN de **HQ** en la interfaz Serial 0/0/0 con una distancia administrativa de 5.

f. Diseñe la lista de acceso con nombre **HQServer** para evitar que cualquier computadora conectada a la interfaz Gigabit Ethernet 0/0 del router **Sucursal** acceda a **HQServer.pka.** Se permite todo el tráfico restante. Configure la lista de acceso en el router adecuado y aplíquela a la interfaz apropiada en el sentido correcto.

g. Diseñe la lista de acceso con nombre **BranchServer** para evitar que cualquier computadora conectada a la interfaz Gigabit Ethernet 0/0 del router **HQ** acceda a los servicios HTTP y HTTPS en el servidor de **Sucursal.** Se permite todo el tráfico restante. Configure la lista de acceso en el router adecuado y aplíquela a la interfaz apropiada en el sentido correcto.

```
Configuración de Sucursal

hostname Branch
!
interface GigabitEthernet0/0
 ip address 172.16.159.254 255.255.240.0
 ip access-group HQServer in
 no shut
!
interface GigabitEthernet0/1
 ip address 172.16.143.254 255.255.240.0
 no shut
```



```
!
interface Serial0/0/0
 ip address 192.168.0.2 255.255.255.252
 ip summary-address eigrp 1 172.16.128.0 255.255.224.0 5
no shut
!
router eigrp 1
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 172.16.128.0 0.0.15.255
 network 172.16.144.0 0.0.15.255
 network 192.168.0.0 0.0.0.3
 no auto-summary
!
ip access-list extended HQServer
 deny ip any host 172.16.0.1
 permit ip any any


HQ Configuration

hostname HQ
!
interface GigabitEthernet0/0
 ip address 172.16.127.254 255.255.192.0
 ip access-group BranchServer in
no shut
!
interface GigabitEthernet0/1
 ip address 172.16.63.254 255.255.192.0
no shut
!
interface Serial0/0/0
 ip address 192.168.0.1 255.255.255.252
 ip summary-address eigrp 1 172.16.0.0 255.255.128.0 5
no shut
!
interface Serial0/0/1
 ip address 64.104.34.2 255.255.255.252
no shut
!
router eigrp 1
 redistribute static
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 passive-interface Serial0/0/1
 network 172.16.64.0 0.0.63.255
 network 172.16.0.0 0.0.63.255
 network 192.168.0.0 0.0.0.3
```

```
 network 64.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip access-list extended BranchServer
 deny tcp any host 172.16.128.1 eq www
 deny tcp any host 172.16.128.1 eq 443
 permit ip any any
```

Packet Tracer: configuración de ACL de IPv6 (versión para el instructor)

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

Topología

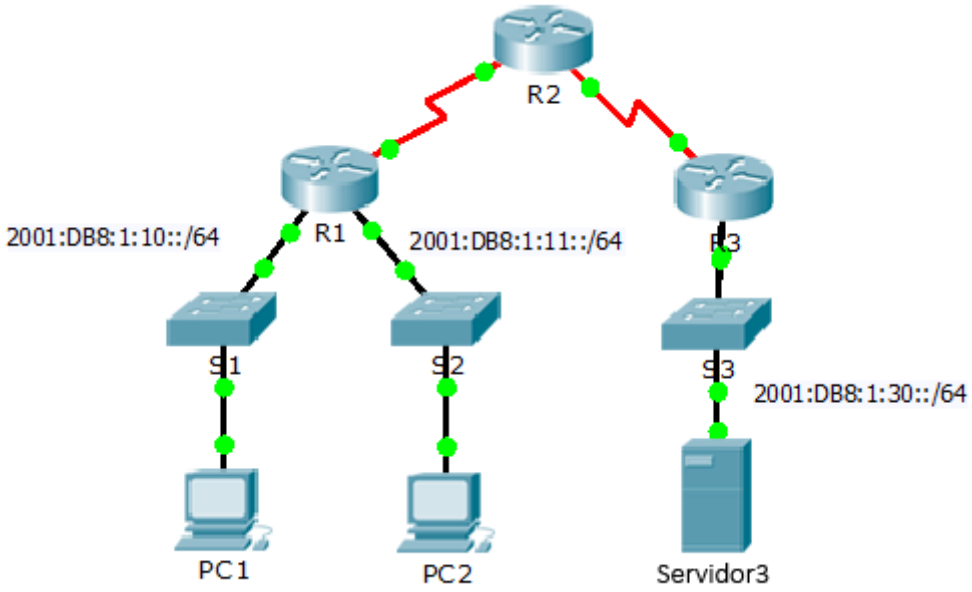


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
Servidor3	NIC	2001:DB8:1:30::30/64	FE80::30

Objetivos

Parte 1: configurar, aplicar y verificar una ACL de IPv6

Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Parte 1: configurar, aplicar y verificar una ACL de IPv6

Según los registros, una computadora en la red 2001:DB8:1:11::0/64 actualiza repetidamente su página web, lo que ocasiona un ataque por denegación de servicio (DoS) contra el **Servidor3**. Hasta que se pueda identificar y limpiar el cliente, debe bloquear el acceso HTTP y HTTPS a esa red mediante una lista de acceso.

Paso 1: configurar una ACL que bloquee el acceso HTTP y HTTPS.

Configure una ACL con el nombre **BLOCK_HTTP** en el **R1** con las siguientes instrucciones.

a. Bloquear el tráfico HTTP y HTTPS para que no llegue al **Servidor3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Permitir el paso del resto del tráfico IPv6.

```
R1(config)# permit ipv6 any any
```

Paso 2: aplicar la ACL a la interfaz correcta.

Aplique la ACL a la interfaz más cercana al origen del tráfico que se desea bloquear.

```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Paso 3: verificar la implementación de la ACL.

Realice las siguientes pruebas para verificar que la ACL funcione de manera correcta:

- Abra el **navegador web** de la **PC1** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. Debería aparecer el sitio web.
- Abra el **navegador web** de la **PC2** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. El sitio web debería estar bloqueado.
- Haga ping de la **PC2** a 2001:DB8:1:30::30. El ping debería realizarse correctamente.

Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Ahora, en los registros se indica que su servidor recibe pings de diversas direcciones IPv6 en un ataque por denegación de servicio distribuido (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

Paso 1: crear una lista de acceso para bloquear ICMP.

Configure una ACL con el nombre **BLOCK_ICMP** en el **R3** con las siguientes instrucciones:

a. Bloquear todo el tráfico ICMP desde cualquier host hasta cualquier destino.

```
R3(config)# deny icmp any any
```

b. Permitir el paso del resto del tráfico IPv6.

```
R3(config)# permit ipv6 any any
```

Paso 2: aplicar la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier origen. Para asegurar que el tráfico ICMP esté bloqueado, independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL lo más carca posible del destino.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out
```

Paso 3: verificar que la lista de acceso adecuada funcione.

a. Haga ping de la **PC2** a 2001:DB8:1:30::30. El ping debe fallar.

b. Haga ping de la **PC1** a 2001:DB8:1:30::30. El ping debe fallar.

   Abra el **navegador web** de la **PC1** con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. Debería aparecer el sitio web.

Packet Tracer: configuración de DHCP mediante el IOS de Cisco (versión para el instructor)

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

Topología

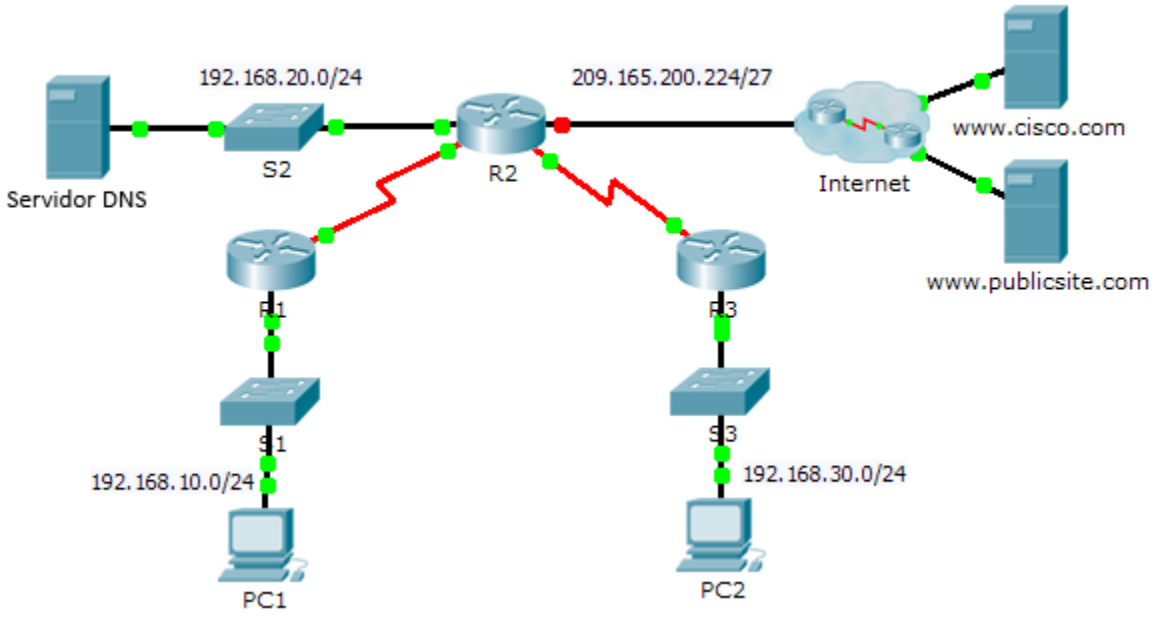


Tabla de direccionamiento

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

Objetivos

Parte 1: configurar un router como servidor de DHCP

Parte 2: configurar la retransmisión de DHCP

Parte 3: configurar un router como cliente DHCP

Parte 4: verificar DHCP y la conectividad

Situación

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

Parte 1: configurar un router como servidor de DHCP

Paso 1: configurar las direcciones IPv4 excluidas.

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

```
R2(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.10
```

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

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

```
R2(config)# ip dhcp pool R1-LAN
```

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

```
R2(dhcp-config)# network 192.168.10.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.10.1
R2(dhcp-config)# dns-server 192.168.20.254
```

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

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

```
R2(config)# ip dh pool R3-LAN
```

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

```
R2(dhcp-config)# network 192.168.30.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.30.1
R2(dhcp-config)# dns-server 192.168.20.254
```


Parte 2: configurar la retransmisión de DHCP

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

```
!R1
R1(config)# interface g0/0
R1(config-if)# ip helper-address 10.1.1.2
!R3
R3(config)# interface g0/0
R3(config-if)# ip helper-address 10.2.2.2
```

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

Parte 3: configurar el R2 como cliente DHCP

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

```
R2(config)# interface g0/1
R2(config-if)# ip address dhcp
R2(config-if)# no shutdown
```

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

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

Parte 4: verificar la conectividad y DHCP

Paso 1: verificar las asignaciones de DHCP.

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

Paso 2: verificar las configuraciones.

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

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

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

Topología

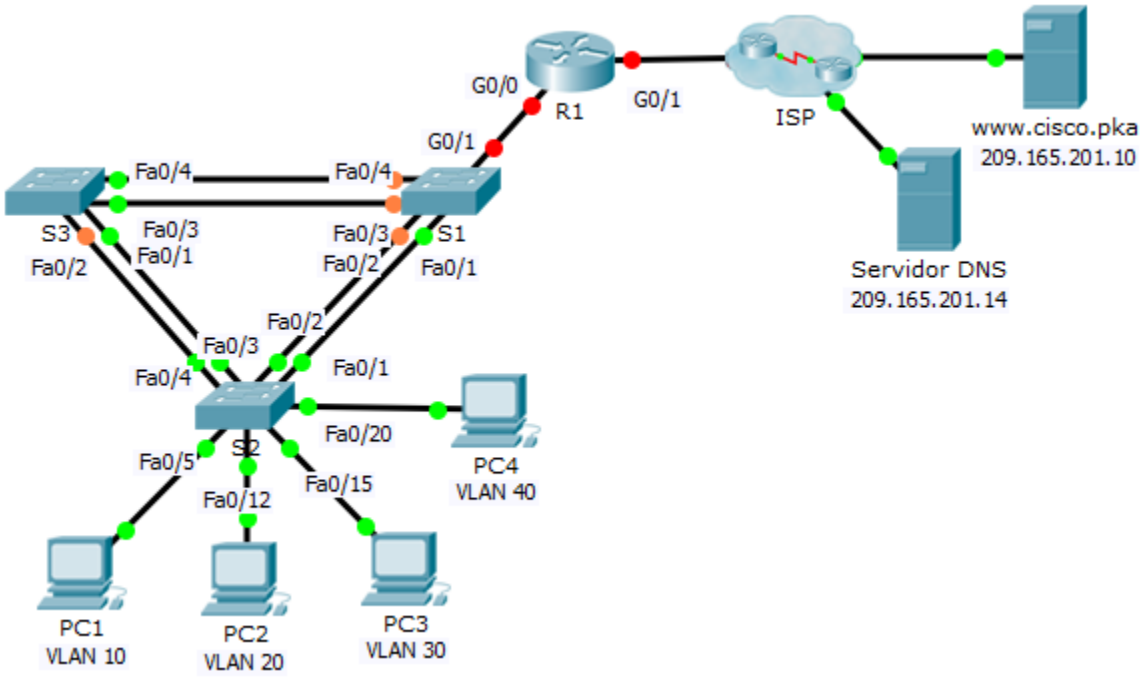


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0.10	172.31.10.1	255.255.255.224	No aplicable
	G0/0.20	172.31.20.1	255.255.255.240	No aplicable
	G0/0.30	172.31.30.1	255.255.255.128	No aplicable
	G0/0.40	172.31.40.1	255.255.255.192	No aplicable
	G0/1	DHCP asignado	DHCP asignado	No aplicable
PC1	NIC	DHCP asignado	DHCP asignado	DHCP asignado
PC2	NIC	DHCP asignado	DHCP asignado	DHCP asignado
PC3	NIC	DHCP asignado	DHCP asignado	DHCP asignado
PC4	NIC	DHCP asignado	DHCP asignado	DHCP asignado

Asignaciones de puertos de VLAN e información de DHCP

Puertos	Número y nombre de VLAN	Nombre del conjunto DHCP	Red
Fa0/5-0/9	VLAN 10: Ventas	VLAN_10	172.31.10.0/27
Fa0/10-Fa0/14	VLAN 20: Producción	VLAN_20	172.31.20.0/28
Fa0/15-Fa0/19	VLAN 30: Marketing	VLAN_30	172.31.30.0/25
Fa0/20-Fa0/24	VLAN 40: RR. HH.	VLAN_40	172.31.40.0/26

Situación

En esta actividad de culminación, configurará VLAN, enlaces troncales, Easy IP de DHCP, agentes de retransmisión DHCP y un router como cliente DHCP.

Requisitos

A partir de la información de las tablas anteriores, implemente los siguientes requisitos:

- Cree las VLAN en el **S2** y asígnelas a los puertos correspondientes. Los nombres distinguen mayúsculas de minúsculas.
- Configure los puertos del **S2** para el uso de enlaces troncales.
- Configure los puertos que se no usarán para enlaces troncales en el **S2** como puertos de acceso.
- Configure el **R1** para el routing entre las VLAN. Los nombres de subinterfaz deben coincidir con el número de VLAN.
- Configure el **R1** para que actúe como servidor de DHCP para las VLAN conectadas al S2.
  - Cree un pool de DHCP para cada VLAN. Los nombres distinguen mayúsculas de minúsculas.
  - Asigne las direcciones apropiadas a cada pool.
  - Configure DHCP para proporcionar una dirección de gateway predeterminado.
  - Configure el servidor DNS 209.165.201.14 para cada pool.
  - Evite que se distribuyan las primeras 10 direcciones de cada pool a las terminales.
- Verifique que cada computadora tenga una dirección asignada del pool de DHCP correcto.

  Nota: la asignación de direcciones DHCP puede tomar tiempo. Haga clic en **Fast Forward Time (Adelantar el tiempo)** para acelerar el proceso.
- Configure el **R1** como cliente DHCP para que reciba una dirección IP de la red del ISP.
- Verifique que ahora todos los dispositivos puedan hacer ping entre sí y a **www.cisco.pka.**

```
!R1!!!!!!!!!!!!!!!!!
enable
config t
!
ip dhcp excluded-address 172.31.10.1 172.31.10.10
ip dhcp excluded-address 172.31.20.1 172.31.20.10
ip dhcp excluded-address 172.31.30.1 172.31.30.10
```

```
ip dhcp excluded-address 172.31.40.1 172.31.40.10
!
ip dhcp pool VLAN_10
 network 172.31.10.0 255.255.255.224
 default-router 172.31.10.1
 dns-server 209.165.201.14
ip dhcp pool VLAN_20
 network 172.31.20.0 255.255.255.240
 default-router 172.31.20.1
 dns-server 209.165.201.14
ip dhcp pool VLAN_30
 network 172.31.30.0 255.255.255.128
 default-router 172.31.30.1
 dns-server 209.165.201.14
ip dhcp pool VLAN_40
 network 172.31.40.0 255.255.255.192
 default-router 172.31.40.1
 dns-server 209.165.201.14
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.31.10.1 255.255.255.224
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.31.20.1 255.255.255.240
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.31.30.1 255.255.255.128
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.31.40.1 255.255.255.192
!
interface GigabitEthernet0/1
 ip address dhcp
```

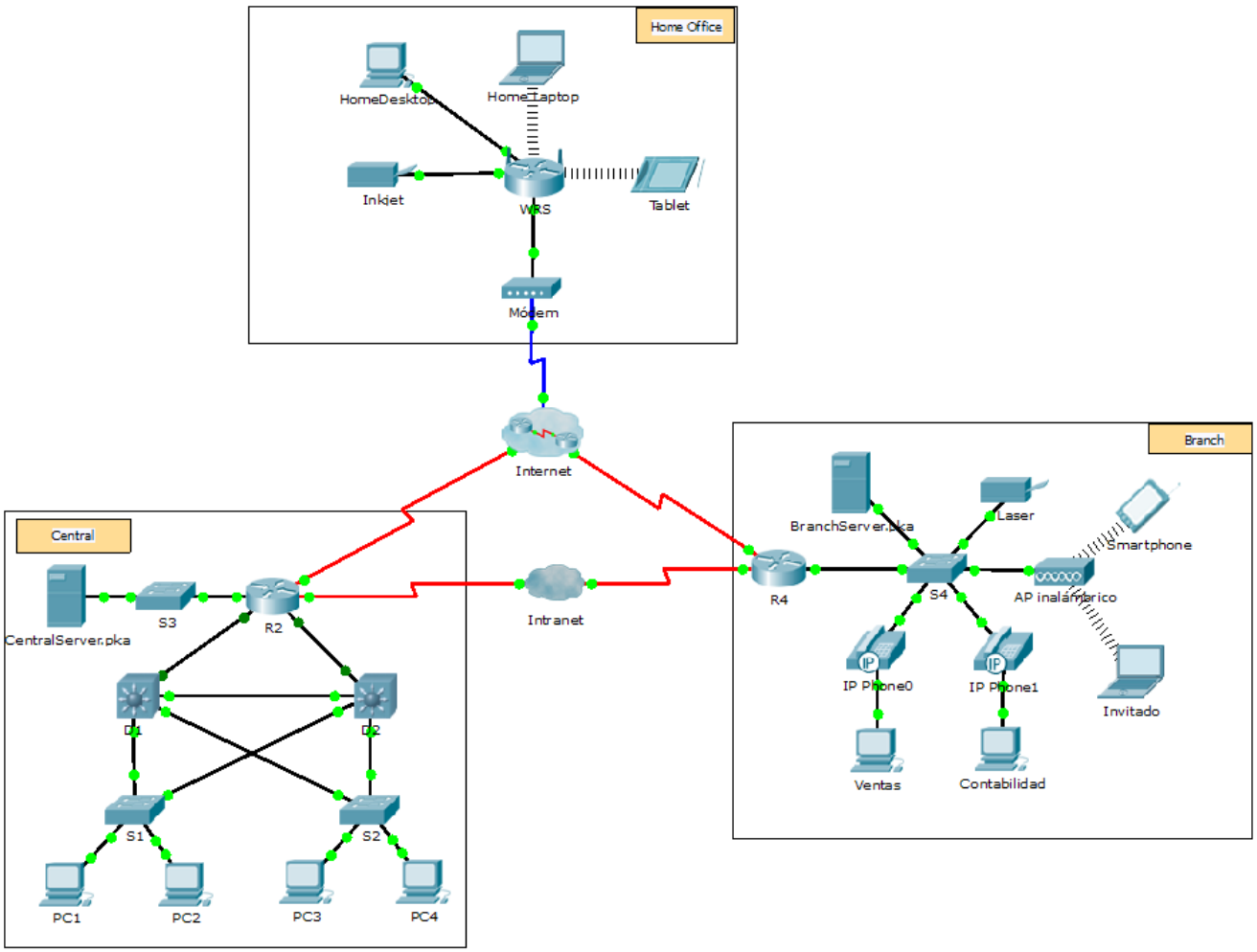
```
 no shutdown
!
end

!S2!!!!!!!!!!!!!!!!!!!!!!!!!!!!
enable
config t
!
interface range fa0/1 - 4
 switchport mode trunk
!
vlan 10
name Sales
vlan 20
name Production
vlan 30
name Marketing
vlan 40
name HR
!
interface range fa0/5 - 24
 switchport mode access
!
interface fa0/5
switchport access vlan 10
interface fa0/12
switchport access vlan 20
interface fa0/15
switchport access vlan 30
interface fa0/20
switchport access vlan 40
!
end
```

Packet Tracer: investigación del funcionamiento de NAT (versión para el instructor)

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

Topología



Objetivos

Parte 1: investigar el funcionamiento de NAT a través de la intranet

Parte 2: investigar el funcionamiento de la NAT a través de Internet

Parte 3: profundizar la investigación

Situación

A medida que una trama se desplaza a través de una red, las direcciones MAC pueden cambiar. Las direcciones IP también pueden cambiar cuando un dispositivo configurado con NAT reenvía un paquete. En esta actividad, investigaremos qué sucede con las direcciones IP durante el proceso de NAT.

Parte 1: investigar el funcionamiento de NAT a través de la intranet

Paso 1: esperar a que la red converja.

La convergencia de todos los elementos de la red puede tomar unos minutos. Para acelerar el proceso, haga clic en Fast Forward Time (Adelantar el tiempo).

Paso 2: generar una solicitud HTTP desde cualquier computadora en el dominio Central.

a. Abra el navegador web desde cualquier computadora en el dominio **Central** y escriba lo siguiente sin presionar la tecla Enter ni hacer clic en **Ir**: **http://branchserver.pka**.

b. Pase al modo **Simulation (Simulación)** y edite los filtros para que solo se muestren las solicitudes HTTP.

c. Haga clic en **Ir** en el navegador; se mostrará un sobre de PDU.

d. Haga clic en **Capture/Forward (Capturar/Adelantar)** hasta que la PDU llegue a **D1** o a **D2**. Registre las direcciones IP de origen y de destino. ¿A qué dispositivos pertenecen esas direcciones? 10.X.X.X y 64.100.200.1; pertenecen a la computadora y al R4.

e. Haga clic en **Capture/Forward** hasta que la PDU llegue al **R2**. Registre las direcciones IP de origen y de destino en el paquete saliente. ¿A qué dispositivos pertenecen esas direcciones? 64.100.100.X y 64.100.200.1; la primera dirección no está asignada a una interfaz. La segunda dirección corresponde al R4.

f. Inicie sesión en el R2 usando "**class**" para acceder al modo EXEC privilegiado y muestre la configuración en ejecución. La dirección provino del siguiente conjunto de direcciones:

```
ip nat pool R2Pool 64.100.100.3 64.100.100.31 netmask 255.255.255.224
```

g. Haga clic en **Capture/Forward** hasta que la PDU llegue al **R4**. Registre las direcciones IP de origen y de destino en el paquete saliente. ¿A qué dispositivos pertenecen esas direcciones? 64.100.100.X y 172.16.0.3. La primera dirección es de R2Pool en el R2. La segunda dirección corresponde a Branchserver.pka.

h. Haga clic en **Capture/Forward** hasta que la PDU llegue a **Branserver.pka**. Registre las direcciones TCP de origen y de destino en el segmento saliente.

i. En el **R2** y el **R4**, ejecute el siguiente comando y encuentre la coincidencia entre las direcciones IP y los puertos registrados anteriormente con la línea correcta del resultado:

```
R2# show ip nat translations
R4# show ip nat translations
```

j. ¿Qué tienen en común las direcciones IP locales internas? Se reservan para uso privado.

k. ¿Alguna dirección privada cruzó la intranet? N.º

l. Vuelva al modo Realtime.

Parte 2: investigar el funcionamiento de la NAT a través de Internet

Paso 1: generar una solicitud HTTP desde cualquier computadora de la oficina doméstica.

a. Abra el navegador web desde cualquier computadora en la oficina doméstica y escriba lo siguiente sin presionar la tecla Enter ni hacer clic en **Ir: http://centralserver.pka**.

b. Cambie a modo de **simulación**. Los filtros ya deben estar establecidos para mostrar solo las solicitudes HTTP.

c. Haga clic en **Ir** en el navegador; se mostrará un sobre de PDU.

d. Haga clic en **Capture/Forward** hasta que la PDU llegue a **WRS**. Registre las direcciones IP de origen y de destino de entrada y las direcciones de origen y de destino de salida. ¿A qué dispositivos pertenecen esas direcciones? 192.168.0.X y 64.100.100.2, y 64.104.223.2 y 64.100.100.2; pertenecen a la computadora y el R2, y a WRS y el R2.

e. Haga clic en **Capture/Forward** hasta que la PDU llegue al **R2**. Registre las direcciones IP de origen y de destino en el paquete saliente. ¿A qué dispositivos pertenecen esas direcciones? 64.104.223.2 y 10.10.10.2; pertenecen a WRS y centralserver.pka.

f. En el **R2**, ejecute el siguiente comando y encuentre la coincidencia entre las direcciones IP y los puertos registrados anteriormente con la línea correcta del resultado:

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

g. Vuelva al modo **Realtime.** ¿Todas las páginas web se mostraron en los navegadores? Sí.

Parte 3: profundizar la investigación

a. Experimente con más paquetes, tanto HTTP como HTTPS. Hay muchas cuestiones para considerar, por ejemplo:

- ¿Aumentan las tablas de traducción NAT?
- ¿WRS tiene un conjunto de direcciones?
- ¿Esta es la forma en que las computadoras del aula se conectan a Internet?
- ¿Por qué NAT utiliza cuatro columnas de direcciones y puertos?

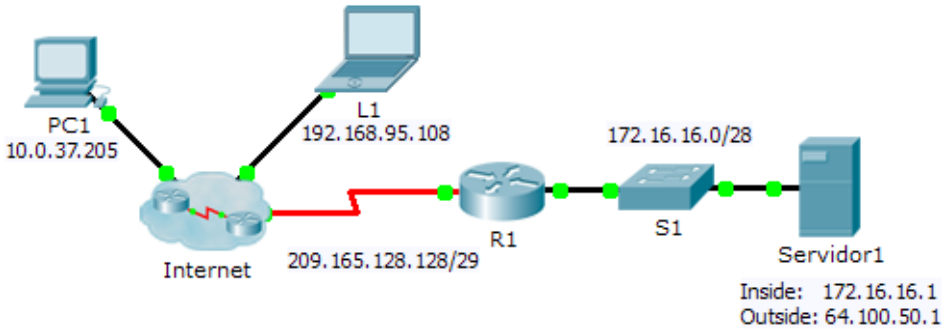
Tabla de calificación sugerida

Sección de la actividad	Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Parte 1: solicitar una página web a través de la intranet	Paso 2d	12	
	Paso 2e	12	
	Paso 2g	13	
	Paso 2j	12	
	Paso 2k	12	
	Total de la parte 1	61	
Parte 2: solicitar una página web a través de Internet	Paso 1d	13	
	Paso 1e	13	
	Paso 1g	13	
	Total de la parte 2	**39**	
	Puntuación total	**100**	

Packet Tracer: configuración de NAT estática (versión para el instructor)

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

Topología



Objetivos

Parte 1: probar el acceso sin NAT

Parte 2: configurar la NAT estática

Parte 3: probar el acceso con NAT

Situación

En las redes configuradas con IPv4, tanto los clientes como los servidores utilizan direccionamiento privado. Para que los paquetes con direccionamiento privado se puedan transmitir por Internet, se deben traducir a direccionamiento público. Los servidores a los que se accede desde afuera de la organización suelen tener asignadas una dirección IP estática pública y una privada. En esta actividad, configurará NAT estática de modo que los dispositivos externos puedan acceder al servidor interno en su dirección pública.

Parte 1: probar el acceso sin NAT

Paso 1: intentar conectarse al Servidor1 con Simulation Mode (Modo de simulación).

a. Desde la **PC1** o la **L1**, intente conectarse a la página web del **Servidor1** en 172.16.16.1. Utilice el navegador web para navegar el **Servidor1** en 172.16.16.1. Los intentos deberían fallar.

b. Desde la **PC1**, haga ping a la interfaz S0/0/0 del **R1**. El ping debe tener éxito.

Paso 2: ver la tabla de routing del R1 y la configuración en ejecución.

a. Vea la configuración en ejecución en el **R1**. Observe que no hay comandos que se refieran a NAT.

b. Verifique que la tabla de routing no tenga entradas que se refieran a las direcciones IP utilizadas por la **PC1** y la **L1**.

c. Verifique que el **R1** no utilice NAT.

```
R1# show ip nat translations
```

Parte 2: Configurar NAT estática

Paso 1: configurar instrucciones de NAT estática.

Consulte la topología. Cree una traducción de NAT estática para asignar la dirección interna del **Servidor1** a su dirección externa.

```
R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

Paso 2: configurar las interfaces.

Configure las interfaces internas y externas correctas.

```
R1(config)# interface g0/0
R1(config-if)# ip nat inside
R1(config)# interface s0/0/0
R1(config-if)# ip nat outside
```

Parte 3: probar el acceso con NAT

Paso 1: verificar la conectividad a la página web del Servidor1.

a. Abra el símbolo del sistema en la **PC1** o la **L1**, e intente hacer ping a la dirección pública del **Servidor1**. Los pings se deben realizar correctamente.

b. Verifique que tanto la **PC1** como la **L1** ahora puedan acceder a la página web del **Servidor1**.

Paso 2: ver las traducciones NAT.

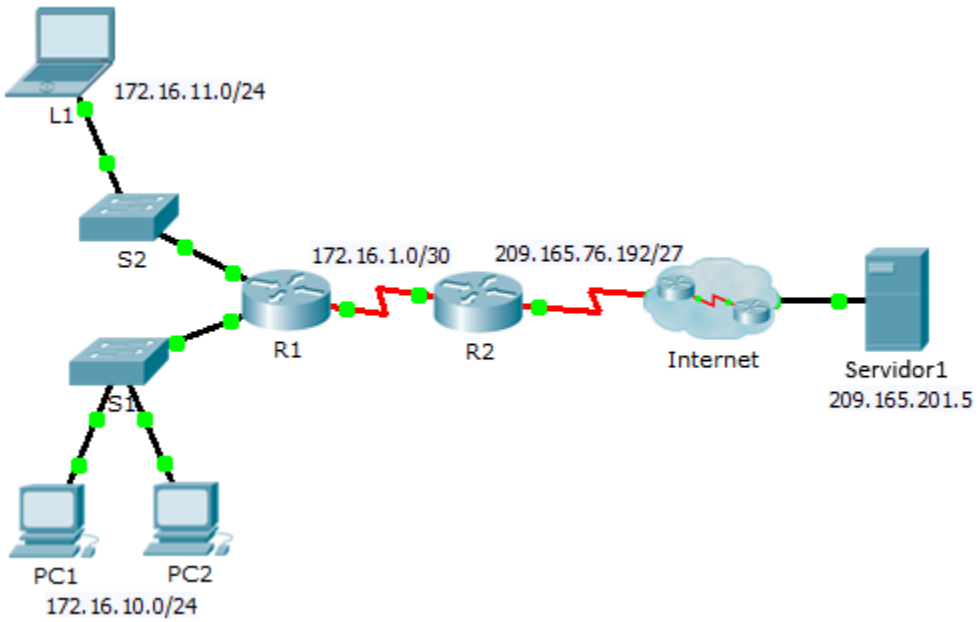
Utilice los siguientes comandos para verificar la configuración de NAT estática:

```
show running-config
show ip nat translations
show ip nat statistics
```

Packet Tracer: configuración de NAT dinámica (versión para el instructor)

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

Topología



Objetivos

Parte 1: configurar NAT dinámica

Parte 2: verificar la implementación de NAT

Parte 1: configurar la NAT dinámica

Paso 1: configurar el tráfico que se desea permitir.

En el **R2**, configure una instrucción para que la ACL 1 permita cualquier dirección que pertenezca a 172.16.0.0/16.

```
R2(config)# access-list 1 permit 172.16.0.0 0.0.255.255
```

Paso 2: configurar un conjunto de direcciones para NAT.

Configure el **R2** con un conjunto de NAT que utilice las cuatro direcciones en el espacio de direcciones 209.165.76.196/30.

```
R2(config)# ip nat pool any-name-here 209.165.76.196 209.165.76.199 netmask
255.255.255.252
```

Observe que en la topología hay tres rangos de red que se traducirán según la ACL creada. ¿Qué sucedería si más de dos dispositivos intentaran acceder a Internet? A los dispositivos adicionales se les denegaría el acceso hasta que se agote el tiempo de espera de una de las traducciones y se libere así una dirección para utilizar.

Paso 3: asociar la ACL 1 con el conjunto de NAT.

```
R2(config)# ip nat inside source list 1 pool any-name-here
```

Paso 4: configurar las interfaces NAT.

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

```
R2(config)# interface s0/0/0
R2(config-if)# ip nat outside
R2(config-if)# interface s0/0/1
R2(config-if)# ip nat inside
```

Parte 2: verificar la implementación de NAT

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

Mediante el navegador web de la **L1**, la **PC1** o la **PC2**, acceda a la página web del **Servidor1**.

Paso 2: ver las traducciones NAT.

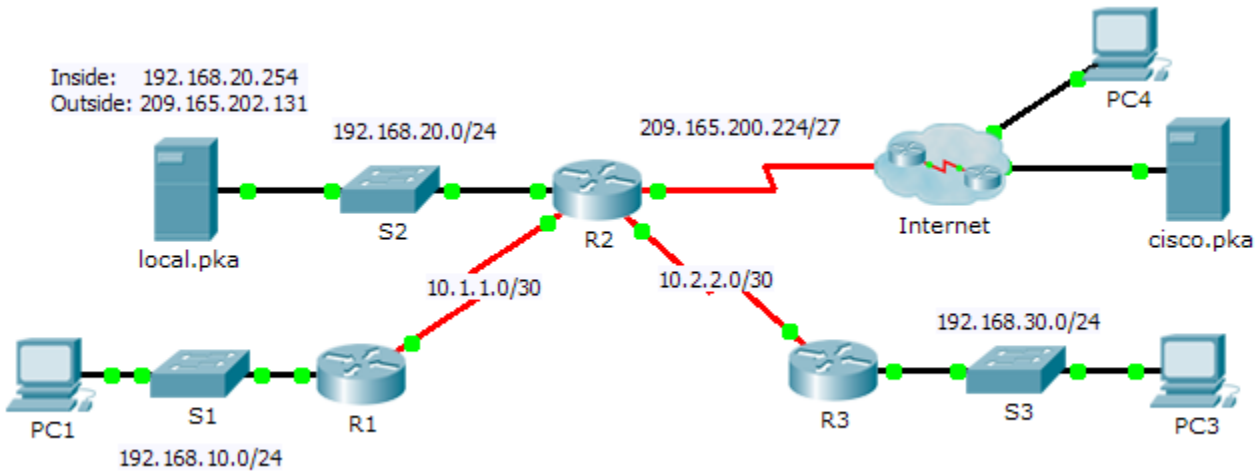
Vea las traducciones NAT en el **R2**.

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

Packet Tracer: implementación de NAT estática y dinámica (versión para el instructor)

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

Topología



Objetivos

Parte 1: configurar la NAT dinámica con PAT

Parte 2: configurar la NAT estática

Parte 3: verificar la implementación de NAT

Parte 1: configurar la NAT dinámica con PAT

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

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

```
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: configurar un conjunto de direcciones para NAT.

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

```
R2(config)# ip nat pool any-name-here 209.165.202.128 209.165.202.130 netmask
255.255.255.252
```

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

```
R2(config)# ip nat inside source list R2NAT pool any-name-here overload
```

Paso 4: configurar las interfaces NAT.

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

```
R2(config)# inte fa0/0
R2(config-if)# ip nat inside
R2(config-if)# inte s0/0/0
R2(config-if)# ip nat inside
R2(config-if)# inte s0/0/1
R2(config-if)# ip nat inside
R2(config-if)# inte s0/1/0
R2(config-if)# ip nat outside
```

Parte 2: Configurar NAT estática

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

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

Parte 3: verificar la implementación de NAT

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

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

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

Paso 2: ver las traducciones NAT.

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

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


Packet Tracer: configuración del reenvío de puertos en un router Linksys (versión para el instructor)

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

Topología

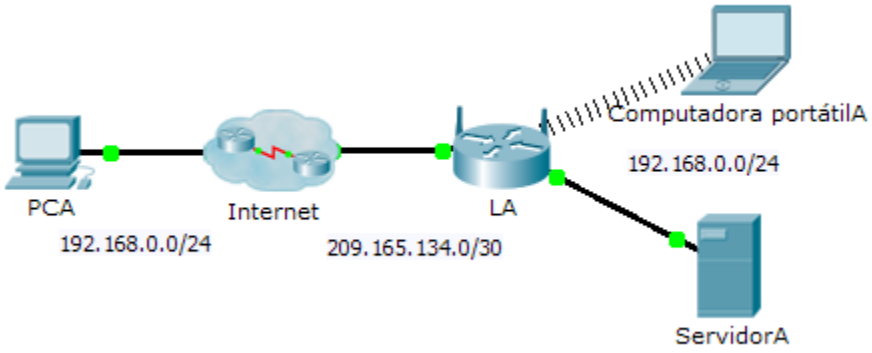


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
LA	Internet	209.165.134.1	255.255.255.252
	LAN	192.168.0.1	255.255.255.0

Objetivos

Parte 1: configurar el reenvío de puertos

Parte 2: verificar la conectividad remota al ServidorA

Situación

Un amigo desea jugar con usted en su servidor. Ambos están en sus respectivos hogares conectados a Internet. Debe configurar su router SOHO (oficina pequeña o doméstica) para reenviar las solicitudes HTTP a su servidor a través del puerto, de modo que su amigo pueda acceder a la página web del juego.

Parte 1: configurar el reenvío de puertos

a. Mediante el navegador web en la **Computadora portátilA**, acceda a **LA** con la dirección IP de la LAN: 192.168.0.1. El nombre de usuario es **admin** y la contraseña es **cisco123**.

b. Haga clic en **Applications & Gaming (Aplicaciones y juegos)**. En la primera lista desplegable a la izquierda, seleccione **HTTP** y, a continuación, introduzca 192.168.0.2 en la columna “To IP Address” (A dirección IP). Esto configura **LA** para el reenvío del puerto 80 a 192.168.0.2. Active la casilla de verificación **Enabled (Habilitada)** al lado de la columna de direcciones.

c. Desplácese hacia abajo y haga clic en **Save Settings (Guardar configuración)**.

Parte 2: verificar la conectividad remota al ServidorA

En el navegador web en la **PCA**, introduzca la dirección IP de Internet para **LA**. Debe aparecer la página web del servidor de juegos.

Packet Tracer: verificación y resolución de problemas de configuración NAT (versión para el instructor)

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

Topología

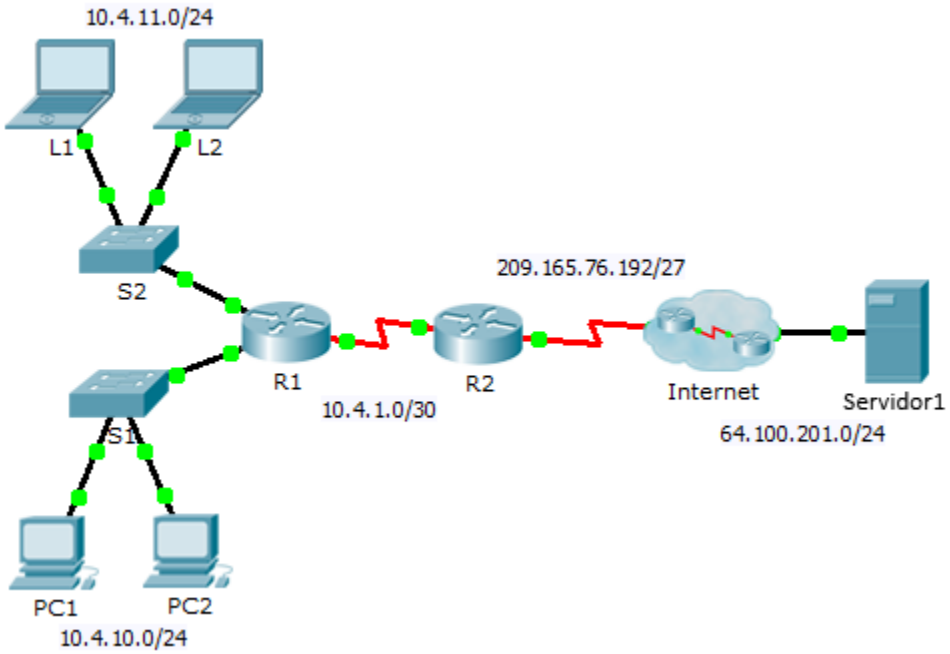


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	10.4.10.254	255.255.255.0	N/A
	G0/1	10.4.11.254	255.255.255.0	N/A
	S0/0/1	10.4.1.2	255.255.255.252	N/A
R2	S0/0/0	209.165.76.194	255.255.255.224	N/A
	S0/0/1	10.4.1.1	255.255.255.252	N/A
Server1	NIC	64.100.201.5	255.255.255.0	64.100.201.1
PC1	NIC	10.4.10.1	255.255.255.0	10.4.10.254
PC2	NIC	10.4.10.2	255.255.255.0	10.4.10.254
L1	NIC	10.4.11.1	255.255.255.0	10.4.11.254
L2	NIC	10.4.11.2	255.255.255.0	10.4.11.254

Objetivos

Parte 1: aislar los problemas

Parte 2: resolver los problemas de configuración NAT

Parte 3: verificar la conectividad

Situación

Un contratista restauró una antigua configuración en un router nuevo que ejecuta NAT. No obstante, la red se modificó y se agregó una nueva subred luego de hacer una copia de seguridad de la antigua configuración. Su trabajo es hacer que la red vuelva a funcionar.

Parte 1: aislar los problemas

Haga ping al **Servidor1** desde **PC1**, **PC2**, **L1**, **L2** y el **R2**. Registre cada ping correcto. Haga ping a cualquier otra máquina, según sea necesario.

Parte 2: resolver los problemas de configuración NAT

Paso 1: ver las traducciones NAT en el R2.

Si la NAT funciona, debería haber entradas de tabla.

Paso 2: mostrar la configuración en ejecución en el R2.

El puerto NAT interno debe alinearse con la dirección privada, mientras que el puerto NAT externo debe alinearse con la dirección pública.

Paso 3: corregir las interfaces.

Asigne los comandos **ip nat inside** e **ip nat outside** a los puertos correctos.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat outside
R2(config-if)# interface Serial0/0/1
R2(config-if)# ip nat inside
```

Paso 4: Haga ping al Servidor1 desde PC1, PC2, L1, L2 y el R2.

Registre cada ping correcto. Haga ping a cualquier otra máquina, según sea necesario.

Paso 5: ver las traducciones NAT en el R2.

Si la NAT funciona, debería haber entradas de tabla.

Paso 6: mostrar la lista de acceso 101 en el R2.

La máscara wildcard debe abarcar las redes 10.4.10.0 y 10.4.11.0.

Paso 7: corregir la lista de acceso.

Elimine la lista de acceso 101 y reemplácela por una lista similar que también tenga una sola instrucción. La única diferencia debería ser la wildcard.

```
R2(config)# no access-list 101
```

```
R2(config)# access-list 101 permit ip 10.4.10.0 0.0.1.255 any
```

Parte 3: Verificar la conectividad

Paso 1: verificar la conectividad al Servidor1.

Registre cada ping correcto. Todos los hosts deben poder hacer ping al **Servidor1**, al **R1** y al **R2**. Resuelva los problemas si los ping no se realizan correctamente.

Paso 2: ver las traducciones NAT en el R2.

La NAT debe mostrar varias entradas de tabla.

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

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

Topología

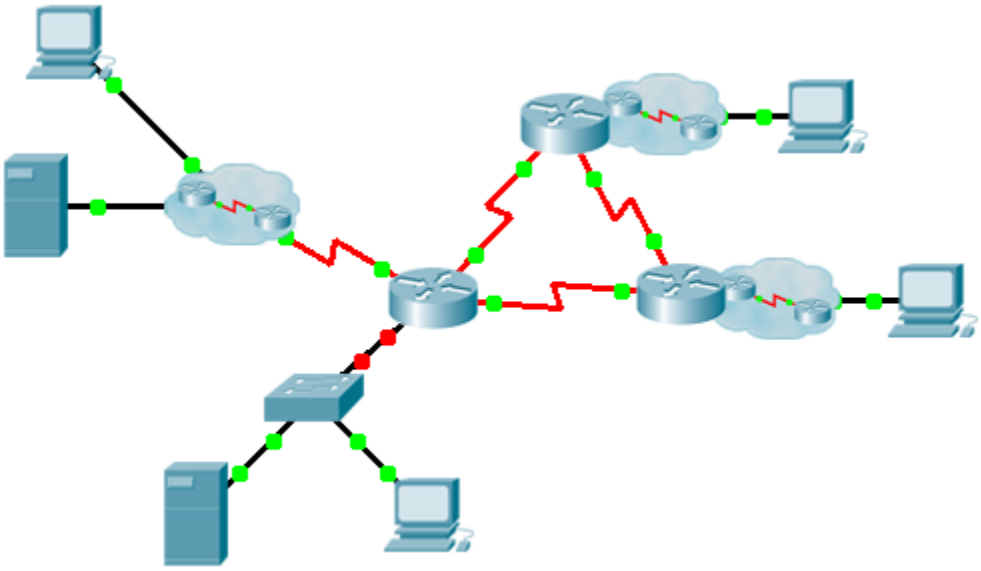


Tabla de direccionamiento

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

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0.15	[[R1G0sub15Add]]	[[R1G0sub15SM]]	No aplicable
	G0/0.30	[[R1G0sub30Add]]	[[R1G0sub30SM]]	No aplicable
	G0/0.45	[[R1G0sub45Add]]	[[R1G0sub45SM]]	No aplicable
	G0/0.60	[[R1G0sub60Add]]	[[R1G0sub60SM]]	No aplicable
	S0/0/0	[[R1S000Add]]	255.255.255.252	No aplicable
	S0/0/1	[[R1S001Add]]	255.255.255.252	No aplicable
	S0/1/0	[[R1S010Add]]	255.255.255.252	No aplicable
[[R2Name]]	G0/0	[[R2G00Add]]	[[R2R3LanSM]]	No aplicable
	S0/0/0	[[R2S000Add]]	255.255.255.252	No aplicable
	S0/0/1	[[R2S001Add]]	255.255.255.252	No aplicable
[[R3Name]]	G0/0	[[R3G00Add]]	[[R2R3LanSM]]	No aplicable
	S0/0/0	[[R3S000Add]]	255.255.255.252	No aplicable
	S0/0/1	[[R3S001Add]]	255.255.255.252	No aplicable
[[S1Name]]	VLAN 60	[[S1VLAN60Add]]	[[R1G0sub60SM]]	[[R1G0sub60Add]]
[[PC1Name]]	NIC	DHCP asignado	DHCP asignado	DHCP asignado

Tabla de asignación de VLAN y de puertos

Número y nombre de VLAN	Asignación de puertos	Red
15: Servidores	F0/11-F0/20	[[R1-VLANsrvNet]]
30: PC	F0/1-F0/10	[[R1-VLANpcNet]]
45: Nativa	G1/1	[[R1-VLANntvNet]]
60: Administración	VLAN 60	[[R1-VLANmanNet]]

Situación

Esta actividad de culminación incluye muchas de las habilidades que adquirió durante este curso. En primer lugar, deberá completar el registro de la red. Por lo tanto, conserve una versión impresa de las instrucciones. Durante la implementación, configurará las VLAN, los enlaces troncales, la seguridad de puertos y el acceso remoto mediante SSH en un switch. A continuación, implementará el routing entre VLAN y NAT en un router. Por último, utilizará su registro para verificar la implementación mediante la prueba de la conectividad de extremo a extremo.

Documentación

Debe registrar la red por completo. Necesitará una copia impresa de este conjunto de instrucciones, que incluye un diagrama de topología sin etiquetas.

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

Implementación

Nota: Todos los dispositivos en la topología, excepto **[[R1Name]]**, **[[S1Name]]**, y **[[PC1Name]]**, están totalmente configurados. No tiene acceso a los otros routers. Puede acceder a todos los servidores y computadoras con el fin de probarlos.

Utilice su registro para implementar los siguientes requisitos:

[[S1Name]]

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

[[R1Name]]

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

- Consulte su registro y configure NAT estática para el Servidor de archivos.
- Configure la NAT dinámica con PAT con un nombre de conjunto de su elección y estas dos direcciones públicas:

  [[NATPoolText]]

[[PC1Name]]

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

Verificación

Ahora, todos los dispositivos deberían poder hacer ping a todos los demás dispositivos. Si no es así, revise las configuraciones para aislar y resolver problemas. Entre las pruebas se incluyen las siguientes:

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

Registro de resolución de problemas

Problema	Solución

Tabla de calificación sugerida

Packet Tracer tiene una puntuación de 70 puntos. El registro vale 30 puntos.

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


```
**************************************************
ISOMORPH ID KEY:
ID = XYZ where;
 X = indexAdds for /24 private address space
 Y = indexNATs for NAT and SSH specific configs
 Z = indexNAMES for device names
Note: Each seed contains variables that are independent
of the other seeds. You do not need to test all the
various combinations.
==========================================================
ISOMORPH ID = 000
==========================================================
!HQ!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 172.16.15.32 255.255.255.224
 default-router 172.16.15.33
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 172.16.15.17 255.255.255.240
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.15.33 255.255.255.224
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 172.16.15.1 255.255.255.248
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.15.9 255.255.255.248
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 172.16.15.0 0.0.0.255 area 0
!
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 172.16.15.18 209.165.200.227
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 172.16.15.0 0.0.0.255
interface s0/0/0
```



```
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!HQ-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
en
conf t
int vlan 60
ip add 172.16.15.10 255.255.255.248
no shut
ip default-gateway 172.16.15.9
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user HQadmin pass ciscoclass
```



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

=========================================================
ISOMORPH ID = 111
=========================================================
!Admin!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 10.10.10.192 255.255.255.192
 default-router 10.10.10.193
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 10.10.10.161 255.255.255.224
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.10.10.193 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 10.10.10.129 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.10.10.145 255.255.255.240
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 10.10.10.0 0.0.0.255 area 0
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
!
ip nat pool TEST 198.133.219.128 198.133.219.129 netmask 255.255.255.252
```



```
ip nat inside source list 1 pool TEST overload
ip nat inside source static 10.10.10.162 198.133.219.130
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 10.10.10.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!!
!Admin-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 10.10.10.146 255.255.255.240
no shut
ip default-gateway 10.10.10.145
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user Admin pass letmein
service password-encryption
ip ssh version 2
```



```
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh

================================================================
ISOMORPH ID: 222
================================================================
!Central!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 192.168.45.128 255.255.255.192
 default-router 192.168.45.129
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 192.168.45.65 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.45.129 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 192.168.45.17 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.45.33 255.255.255.240
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
network 192.168.45.0 0.0.0.255 area 0
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
!
ip nat pool TEST 64.100.32.56 64.100.32.57 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 192.168.45.66 64.100.32.58
```

```
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 192.168.45.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!
!Cnt-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 192.168.45.34 255.255.255.240
no shut
ip default-gateway 192.168.45.33
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g1/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g1/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user CAdmin pass itsasecret
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
```



```
line vty 0 15
login local
transport input ssh
```

