Cisco | Networking Academy®
Mind Wide Open™

Switching y routing CCNA: Conexión de redes

Manual de Packet Tracer para el instructor

Packet Tracer: Desafío de integración de habilidades sobre OSPF (versión para el instructor)

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

Nota: esta actividad y la actividad **Packet Tracer: Desafío de integración de habilidades sobre EIGRP** similar son recursos para que pueda determinar cuáles son las habilidades relacionadas con los cursos anteriores que todavía no domina. Consulte sus notas y el contenido anterior si necesita ayuda. Sin embargo, primero puede ser interesante ver cuánto recuerda.

Nota para el instructor: esta actividad se proporciona solo como método para evaluar el dominio de los estudiantes de cursos anteriores. Se puede utilizar como herramienta para orientar a los estudiantes en cuanto a estrategias de corrección.

Topología

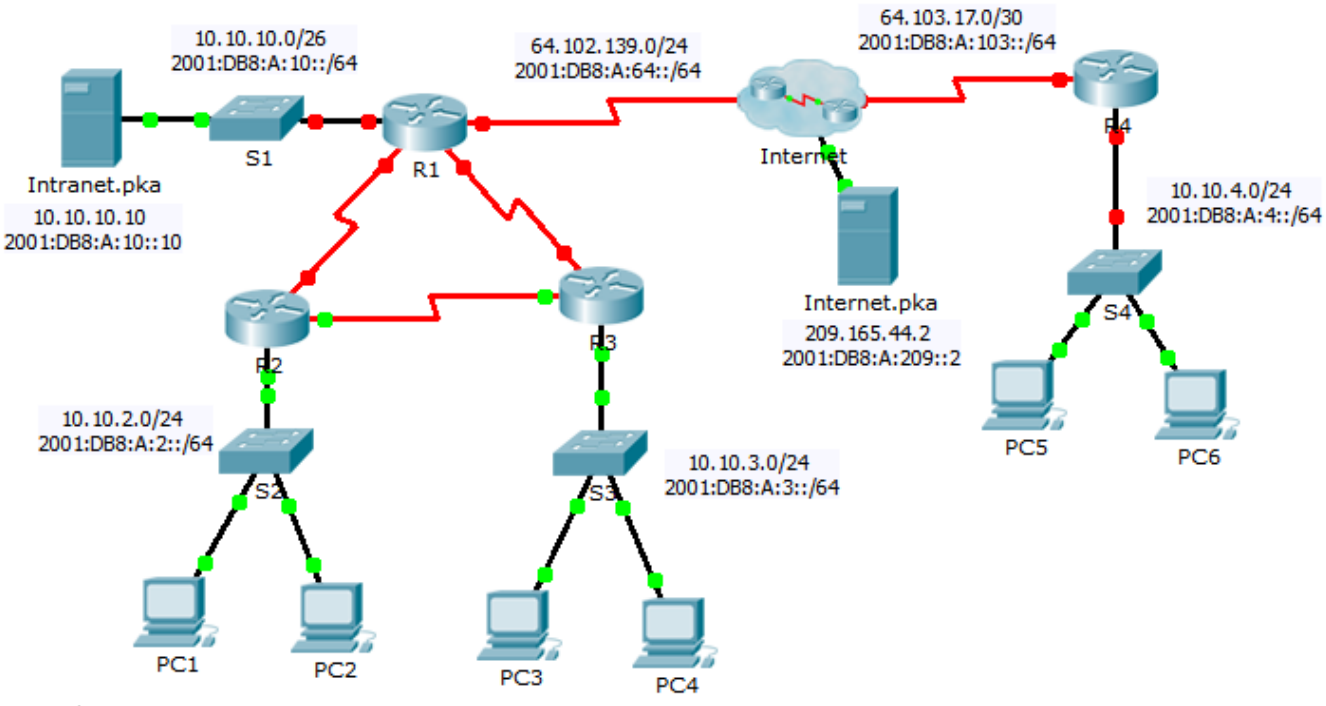


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.10.1	255.255.255.192	N/A
		2001:DB8:A:10::1/64		N/A
	S0/0/0	64.102.139.2	255.255.255.0	N/A
		2001:DB8:A:64::2/64		N/A
	S0/0/1	10.10.1.1	255.255.255.252	N/A
		2001:DB8:B:1::1/64		N/A
	S0/1/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:B:2::1/64		N/A
	Link-Local	FE80::1		N/A
R2	G0/0	10.10.2.1	255.255.255.0	N/A
		2001:DB8:A:2::1/64		N/A
	S0/0/0	10.10.1.9	255.255.255.252	N/A
		2001:DB8:B:3::1/64		N/A
	S0/0/1	10.10.1.2	255.255.255.252	N/A
		2001:DB8:B:1::2/64		N/A
	Link-Local	FE80::2		N/A
R3	G0/0	10.10.3.1	255.255.255.0	N/A
		2001:DB8:A:3::1/64		N/A
	S0/0/0	10.10.1.10	255.255.255.252	N/A
		2001:DB8:B:3::2/64		N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:B:2::2/64		N/A
	Link-Local	FE80::3		N/A
R4	G0/0	10.10.4.1	255.255.255.0	N/A
		2001:DB8:A:4::1/64		N/A
	S0/0/1	64.103.17.2	255.255.255.252	N/A
		2001:DB8:A:103::2/64		N/A
	Link-Local	FE80::4		N/A

Internet	NIC	209.165.44.2	255.255.255.252	209.165.44.1
		2001:DB8:A:209::2/64		FE80::5
Intranet	NIC	10.10.10.10	255.255.255.192	10.10.10.1
		2001:DB8:A:10::10/64		FE80::1
PC1 - PC6	NIC	DHCP assigned		DHCP assigned
		Auto Config		Auto Config

Situación

Su empresa se acaba de expandir a otra ciudad y necesita ampliar su presencia a través de Internet. Su tarea consiste en llevar a cabo las actualizaciones de la red empresarial, que incluye redes dual-stack IPv4 e IPv6 y una variedad de tecnologías de direccionamiento y routing.

Requisitos

Nota: aunque no es obligatorio, agregar etiquetas adicionales a la topología puede ayudarlo a medida que avanza. Todos los nombres y las contraseñas distinguen mayúsculas de minúsculas.

Configuración básica de dispositivos

- Configure lo siguiente en el **R1** y el **R4**.
  - Establezca los nombres de los dispositivos para que coincidan con la **tabla de direccionamiento**.
  - Establezca **cisco** como la contraseña cifrada del modo EXEC privilegiado.
  - Establezca un mensaje MOTD que incluya la palabra **warn**.
  - Establezca las direcciones IPv4 e IPv6 según la **tabla de direccionamiento**.
  - Asigne la dirección link-local a cada interfaz.

SSH

- Configure SSH en el **R4**.
  - Establezca el nombre de dominio **R4**.
  - Cree el usuario **admin** con la contraseña cifrada **cisco**.
  - Cree una clave RSA de 2048 bits.
  - Configure todas las líneas vty para que usen SSH e inicio de sesión local.

DHCPv4

- Configure el **R4** para que funcione como servidor de DHCP para su LAN.
  - Cree un pool de DHCP con el nombre **R4**.
  - Asigne la información de direccionamiento correspondiente al pool, incluida la dirección 209.165.44.2 como servidor DNS.
  - Evite que se distribuya la dirección que utiliza el router a las terminales.

NAT

- Configure NAT/PAT en el **R4** para que todos los dispositivos en la LAN utilicen la dirección IP en la interfaz Serial 0/0/1 para acceder a Internet.
  - Utilice una única instrucción en la lista de acceso **1** para definir las direcciones que participan en NAT. Admita únicamente el espacio de direcciones 10.10.4.0/24.
  - Habilite NAT/PAT con la lista de acceso.

  - Configure las interfaces apropiadas como NAT interna o externa.
- Configure PAT en el **R1**.
  - Utilice una única instrucción en la lista de acceso **1** para definir las direcciones que participan en NAT. Permita que solo se utilice el espacio de la dirección 10.10.0.0/16.
  - Defina un pool denominado **R1** para que utilice las cuatro direcciones en el espacio de direcciones 64.102.139.4/30.
  - Asigne la lista de acceso **1** al pool **R1**.
  - Configure las interfaces apropiadas como NAT interna o externa.
- Configure NAT estática en el **R1** para el acceso remoto al servidor **Intranet.pka**.
  - Utilice una instrucción de NAT estática para redirigir el tráfico del puerto TCP 80 de 64.102.139.2 a 10.10.10.10.
  - Utilice una instrucción de NAT estática para redirigir el tráfico del puerto TCP 443 de 64.102.139.2 a 10.10.10.10.

Routing predeterminado

- Configure una ruta predeterminada IPv4 en el **R1** mediante la dirección IP del siguiente salto 64.102.139.1.
- Configure una ruta predeterminada IPv6 en el **R1** mediante la interfaz de salida.
- Configure una ruta predeterminada IPv4 e IPv6 en el **R4** mediante la interfaz de salida.

Routing OSPF

- Configure el área 0 de OSPFv2 en el **R1**.
  - Utilice la ID de proceso 1
  - Anunciar las redes conectadas directamente. No incluya el enlace a Internet.
  - Evite que se envíen actualizaciones de routing a través de las interfaces LAN.
  - Propague la ruta predeterminada.
- Configure el área 0 de OSPFv3 en el **R1**.
  - Utilice la ID de proceso 1
  - Asigne 1.1.1.1 como ID del router.
  - Evite que se envíen actualizaciones de routing a través de las interfaces LAN.
  - Complete la configuración de routing OSPFv3 o IPv6 requerida.

Nota para el instructor: no se solicita al estudiante que configure **ipv6 unicast-routing** (necesario en el **R1** y el **R4**) ni que configure las interfaces para el routing OSPFv3 en el **R1**. El estudiante debería saber que se requiere está configuración antes de que el routing IPv6 y OSPFv3 esté en funcionamiento. Además, Packet Tracer 6.0.1 no califica los comandos de OSPFv3. Utilice los comandos de verificación y las pruebas de conectividad para verificar el trabajo de los estudiantes.

Verificar la conectividad

- Configure la **PC5** y la **PC6** para que se utilice DHCP para IPv4 y Autoconfig para IPv6.
- Verifique el acceso web a **Internet.pka** y a **Intranet.pka** desde cada una de las seis computadoras. Asegúrese de probar tanto IPv4 como IPv6. Los pings no se reenvían desde la PC5 y la PC6 a **Intranet.pka**.

Configuraciones de dispositivos

Router R1

```
enable
configure terminal
hostname R1
enable secret cisco
ipv6 unicast-routing
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.192
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:A:10::1/64
 ipv6 ospf 1 area 0
 no shutdown
interface Serial0/0/0
 ip address 64.102.139.2 255.255.255.0
 ip nat outside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:A:64::2/64
 ipv6 ospf 1 area 0
 no shutdown
interface Serial0/0/1
 ip address 10.10.1.1 255.255.255.252
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:B:1::1/64
 ipv6 ospf 1 area 0
 clock rate 4000000
 no shutdown
interface Serial0/1/0
 ip address 10.10.1.5 255.255.255.252
 ip nat inside
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:B:2::1/64
 ipv6 ospf 1 area 0
 clock rate 4000000
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0
 network 10.10.10.0 0.0.0.63 area 0
 network 10.10.1.0 0.0.0.3 area 0
 network 10.10.1.4 0.0.0.3 area 0
 default-information originate
ipv6 router ospf 1
 router-id 1.1.1.1
ip nat pool R1 64.102.139.4 64.102.139.7 netmask 255.255.255.252
ip nat inside source list 1 pool R1 overload
ip nat inside source static tcp 10.10.10.10 80 64.102.139.2 80
```

```
ip nat inside source static tcp 10.10.10.10 443 64.102.139.2 443
ip route 0.0.0.0 0.0.0.0 64.102.139.1
ipv6 route ::/0 Serial0/0/0
access-list 1 permit 10.10.0.0 0.0.255.255
banner motd ^CWarning^C
end
copy running-config startup-config
```

R4 del router

```
enable
configure terminal
hostname R4
enable secret cisco
ip dhcp excluded-address 10.10.4.1
ip dhcp pool R4
 network 10.10.4.0 255.255.255.0
 default-router 10.10.4.1
 dns-server 209.165.44.2
ipv6 unicast-routing
username admin secret cisco
ip domain-name R4
interface GigabitEthernet0/0
 ip address 10.10.4.1 255.255.255.0
 ip nat inside
 ipv6 address FE80::4 link-local
 ipv6 address 2001:DB8:A:4::1/64
 no shutdown
interface Serial0/0/1
 ip address 64.103.17.2 255.255.255.252
 ip nat outside
 ipv6 address FE80::4 link-local
 ipv6 address 2001:DB8:A:103::2/64
 no shutdown
ip nat inside source list 1 interface Serial0/0/1 overload
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
ipv6 route ::/0 Serial0/0/1
access-list 1 permit 10.10.4.0 0.0.0.255
banner motd ^CWarning^C
line vty 0 4
 login local
 transport input ssh
crypto key generate rsa
yes
2048

end
copy running-config startup-config
```

Packet Tracer: Desafío de integración de habilidades sobre 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.

Nota: esta actividad y la actividad **Packet Tracer: Desafío de integración de habilidades sobre OSPF** similar son recursos para que pueda determinar cuáles son las habilidades relacionadas con los cursos anteriores que todavía no domina. Consulte sus notas y el contenido anterior si necesita ayuda. Sin embargo, primero puede ser interesante ver cuánto recuerda.

Nota para el instructor: esta actividad se proporciona solo como método para evaluar el dominio de los estudiantes de cursos anteriores. Se puede utilizar como herramienta para orientar a los estudiantes en cuanto a estrategias de corrección.

Topología

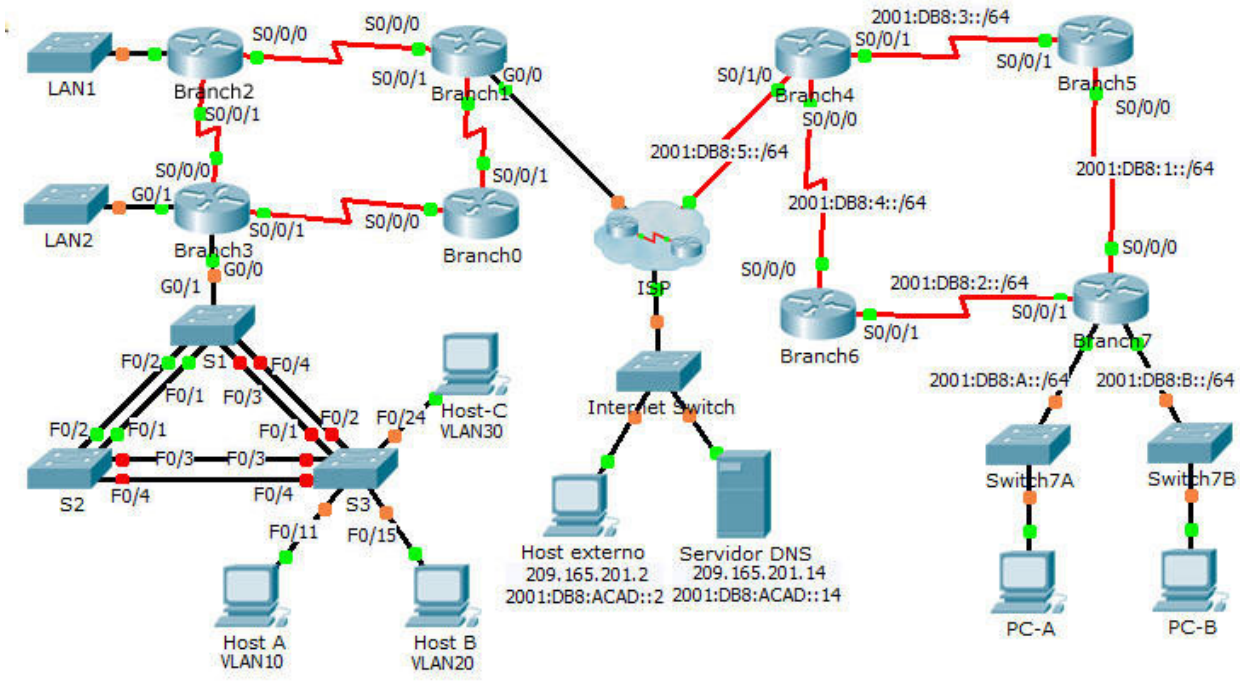


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
Branch0	S0/0/0	192.168.3.241	255.255.255.252	N/A
	S0/0/1	192.168.3.254	255.255.255.252	N/A
Branch1	G0/0	DHCP Assigned	DHCP Assigned	N/A
	S0/0/0	192.168.3.245	255.255.255.252	N/A
	S0/0/1	192.168.3.253	255.255.255.252	N/A
Branch2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.3.246	255.255.255.252	N/A
	S0/0/1	192.168.3.249	255.255.255.252	N/A
Branch3	G0/0.10	192.168.1.1	255.255.255.128	N/A
	G0/0.20	192.168.1.129	255.255.255.192	N/A
	G0/0.30	192.168.1.193	255.255.255.224	N/A
	G0/0.88	192.168.1.225	255.255.255.240	N/A
	G0/0.99	192.168.1.241	255.255.255.252	N/A
	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/0	192.168.3.250	255.255.255.252	N/A
	S0/0/1	192.168.3.242	255.255.255.252	N/A
Branch4	S0/0/0	2001:DB8:4::4/64		N/A
	S0/0/1	2001:DB8:3::4/64		N/A
	S0/1/0	2001:DB8:5::4/64		N/A
	Router ID	4.4.4.4		N/A
Branch5	S0/0/0	2001:DB8:1::5/64		N/A
	S0/0/1	2001:DB8:3::5/64		N/A
	Link-local	FE80::5		N/A
	Router ID	5.5.5.5		N/A
Branch6	S0/0/0	2001:DB8:4::6/64		N/A
	S0/0/1	2001:DB8:2::6/64		N/A
	Link-local	FE80::6		N/A

	Router ID	6.6.6.6		N/A
Branch7	G0/0	2001:DB8:7:A::1/64		N/A
	G0/1	2001:DB8:7:B::1/64		N/A
	S0/0/0	2001:DB8:1::7/64		N/A
	S0/0/1	2001:DB8:2::7/64		N/A
	Link-Local	FE80::7		N/A
	Router ID	7.7.7.7		N/A
ISP	G0/0	209.165.202.129	255.255.255.224	N/A
S1	VLAN 88	192.168.1.226	255.255.255.240	192.168.1.225
S2	VLAN 88	192.168.1.227	255.255.255.240	192.168.1.225
S3	VLAN 88	192.168.1.228	255.255.255.240	192.168.1.225
Host-A	NIC	DHCP assigned	DHCP assigned	DHCP assigned
Host-B	NIC	192.168.1.130	255.255.255.192	192.168.1.129
Host-C	NIC	192.168.1.194	255.255.255.224	192.168.1.193
PC-A	NIC	2001:DB8:7:A::A/64		FE80::7
PC-B	NIC	2001:DB8:7:B::B/64		FE80::7

Tabla de asignaciones de VLAN y de puertos

VLAN	Nombre	Interfaz
10	Students	F0/5-11
20	Faculty/Staff	F0/12-17, G0/1-2
30	Guest(Default) (Invitado(Predeterminado)	F0/18-24
88	Management	N/A
99	Nativo	F0/1-4

Situación

Usted es el nuevo técnico de red de una empresa que perdió a su técnico anterior en medio del proceso de actualización del sistema. Su tarea es completar las actualizaciones de la infraestructura de red que tiene dos ubicaciones. La mitad de la red empresarial utiliza direccionamiento IPv4 y la otra mitad utiliza direccionamiento IPv6. Además, los requisitos incluyen una variedad de tecnologías de routing y switching.

Requisitos

Tiene acceso a la consola para **Branch3**, **Branch7** y el **S3**. Puede acceder de forma remota a otros dispositivos con el nombre de usuario **admin** y la contraseña **adminpass**. La contraseña para acceder al modo EXEC privilegiado es **class**.

Asignación de direcciones IPv4

- Termine de diseñar el esquema de direccionamiento IPv4. Las subredes que ya están asignadas utilizan el espacio de direcciones 192.168.1.0/24. Utilice el espacio restante para cumplir los siguientes criterios:
  - 120 hosts para la VLAN **Student** conectada a la interfaz G0/0.10 **Branch3**.
  - 60 hosts para la VLAN **Faculty/Staff** conectada a la interfaz G0/0.20 **Branch3**.
- Configure el routing entre VLAN y asigne la primera dirección disponible de cada subred a las subinterfaces en el router **Branch3**.
- Asigne la segunda dirección disponible en la VLAN de Faculty/Staff (Cuerpo docente/Personal) al Host-B.

IPv4 Routing

- Configure EIGRP para IPv4 en **Branch3**.
  - Habilite EIGRP 22.
  - Anuncie todas las redes conectadas directamente y deshabilite la sumarización automática.
  - Evite que se envíen actualizaciones de routing por las interfaces LAN.
  - Configure una ruta resumida para las LAN de **Branch3** y anuncie la ruta a **Branch1** y **Branch2**.
- Configure una ruta predeterminada conectada directamente en **Branch1** que apunte al ISP y propáguela en las actualizaciones de EIGRP.

DHCP

- Configure **Branch3** para que funcione como servidor de DHCP para la VLAN 10 en el **S3**.
  - El nombre de conjunto, que distingue entre mayúsculas de minúsculas, es **Students**.
  - El servidor DNS es 209.165.201.14.
  - Excluya las primeras 10 direcciones del conjunto.
- Configure **Branch1** para que reciba una dirección IPv4 del **ISP**.

Routing IPv6

- Configure EIGRP para IPv6 en **Branch7**.
  - Habilite el routing IPv6 y EIGRP para IPv6 con el ASN 222.
  - Asigne la ID de router 7.7.7.7.
  - Anunciar las redes conectadas directamente.
  - Configure las rutas resumidas IPv6 para las LAN y anúncielas a los routers conectados directamente.
- Configure una ruta predeterminada completamente especificada en **Branch4** que apunte al ISP y propáguela en las actualizaciones de EIGRP.

Seguridad básica del switch

- Configure el **S3** con los siguientes parámetros de seguridad:
  - Mensaje MOTD que incluya la palabra **warning** (advertencia).
  - Usuario y contraseña de puerto de consola **cisco**.

  - Contraseña de enable cifrada **class**.
  - Cifre las contraseñas de texto no cifrado.
  - Desactive todos los puertos sin utilizar.
- Habilite la seguridad de puertos en el **S3** en las interfaces a las que están conectadas las computadoras.
  - Configúrelos como puertos de acceso.
  - Permita solo un host por puerto.
  - Habilite el aprendizaje dinámico que almacena la dirección MAC en la configuración en ejecución.
  - Asegúrese de que los puertos se deshabiliten cuando se produzcan infracciones de puertos.
  - Configure PortFast y la protección BPDU.

VLAN

- Cree y nombre las VLAN del **S3** según la **tabla de VLAN**.
- Asigne los puertos de switch en el **S3** a las VLAN según la **tabla de VLAN**.
- Configure la conexión entre **Branch3** y el **S1** como enlace troncal y asígnela a la VLAN 99.

Árbol de expansión

- Configure el **S3** para que utilice RSTP como el modo STP.
- Asigne el **S3** como puente raíz y el **S1** como puente raíz de respaldo para las VLAN 10 y 20.
- Asigne el **S1** como puente raíz y el **S3** como puente raíz de respaldo para la VLAN 30.

Enlaces troncales y EtherChannel

- Establezca las interfaces del **S3** conectadas al **S1** y al **S2** como enlaces troncales y asigne la VLAN nativa.
- Establezca EtherChannel en el **S3** como deseado.
  - Utilice el grupo de canales 2 para los enlaces troncales al **S2**.
  - Utilice el grupo de canales 3 para los enlaces troncales al **S1**.
  - Asigne la VLAN nativa.

Conectividad

- Todos los dispositivos internos deben poder hacer ping al host externo.

Configuraciones de dispositivos

Router Branch1

```
enable
configure terminal
interface g0/0
 ip address dhcp
router eigrp 22
 redistribute static
ip route 0.0.0.0 0.0.0.0 g0/0
end
copy running-config startup-config
```


Router Branch3

```
enable
configure terminal
interface g0/0.10
 encapsulation dot1q 10
 ip address 192.168.1.1 255.255.255.128
interface g0/0.20
 encapsulation dot1q 20
 ip address 192.168.1.129 255.255.255.192
interface s0/0/0
 ip summary-address eigrp 22 192.168.0.0 255.255.254.0 5
interface s0/0/1
 ip summary-address eigrp 22 192.168.0.0 255.255.254.0 5
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.1.129 192.168.1.139
ip dhcp excluded-address 192.168.1.193 192.168.1.203
ip dhcp pool Students
 network 192.168.1.0 255.255.255.128
 default-router 192.168.1.1
 dns-server 209.165.201.14
ip dhcp pool Faculty/Staff
 network 192.168.1.128 255.255.255.192
 default-router 192.168.1.129
 dns-server 209.165.201.14
ip dhcp pool Guest(Default)
 network 192.168.1.192 255.255.255.224
 default-router 192.168.1.193
 dns-server 209.165.201.14
router eigrp 22
 network 192.168.1.0 0.0.0.127
 network 192.168.1.128 0.0.0.63
 network 192.168.1.192 0.0.0.31
 network 192.168.1.224 0.0.0.15
 network 192.168.1.240 0.0.0.3
 network 192.168.3.248 0.0.0.3
 network 192.168.3.240 0.0.0.3
 network 192.168.0.0 0.0.0.255
 passive-interface GigabitEthernet0/1
 passive-interface GigabitEthernet0/0.10
 passive-interface GigabitEthernet0/0.20
 passive-interface GigabitEthernet0/0.30
 passive-interface GigabitEthernet0/0.88
 passive-interface GigabitEthernet0/0.99
 no auto-summary
end
copy running-config startup-config
```

Router Branch4

```
enable
configure terminal
ipv6 route ::/0 Serial0/1/0 2001:DB8:5::1
ipv6 router eigrp 222
 redistribute static
end
copy running-config startup-config
```

Router Branch7

```
enable
configure terminal
ipv6 unicast-routing
interface g0/0
 ipv6 eigrp 222
interface g0/1
 ipv6 eigrp 222
interface s0/0/0
 ipv6 eigrp 222
 ipv6 summary-address eigrp 222 2001:db8:a::/47
interface s0/0/1
 ipv6 eigrp 222
 ipv6 summary-address eigrp 222 2001:db8:a::/47
ipv6 router eigrp 222
 router-id 7.7.7.7
 no shutdown
end
copy running-config startup-config
```

Switch S1

```
enable
configure terminal
spanning-tree vlan 10,20 root secondary
spanning-tree vlan 30 root primary
interface GigabitEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
end
copy running-config startup-config
```

Switch S3

```
enable
configure terminal
enable secret class
service password-encryption
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20 root primary
spanning-tree vlan 30 root secondary
```

```
vlan 10
 name Students
vlan 20
 name Faculty/Staff
vlan 30
 name Guest(Default)
vlan 88
 name Management
vlan 99
 name Native
interface range f0/5-24, g0/1-2
 shutdown
interface range f0/1-2
 channel-group 3 mode desirable
 switchport mode trunk
 switchport trunk native vlan 99
 no shutdown
interface range f0/3-4
 channel-group 2 mode desirable
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
interface range f0/5-11
 switchport access vlan 10
 switchport mode access
interface range f0/12-17, g0/1-2
 switchport access vlan 20
 switchport mode access
interface range f0/18-24
 switchport access vlan 30
 switchport mode access
interface range f0/11, f0/15, f0/24
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown
interface Port-channel 2
 switchport mode trunk
 switchport trunk native vlan 99
interface Port-channel 3
 switchport mode trunk
 switchport trunk native vlan 99
interface Vlan88
 ip address 192.168.1.228 255.255.255.240
ip default-gateway 192.168.1.225
```

```
banner motd "Warning! Unauthorized Access is Prohibited!"
line con 0
 password cisco
end
copy running-config startup-config
```


Packet Tracer: Resolución de problemas de interfaces seriales (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	Ruta predeterminada
Telco	S0/0/0 (DCE)	64.100.34.17	255.255.255.252	N/A
	S0/0/1 (DCE)	64.100.34.21	255.255.255.252	N/A
	S0/1/0 (DCE)	64.100.34.25	255.255.255.252	N/A
	S0/1/1 (DCE)	64.100.34.29	255.255.255.252	N/A
R1	S0/0/0	64.100.34.18	255.255.255.252	64.100.34.17
R2	S0/0/1	64.100.34.22	255.255.255.252	64.100.34.21
R3	S0/0/0	64.100.34.26	255.255.255.252	64.100.34.25
R4	S0/0/1	64.100.34.30	255.255.255.252	64.100.34.29

Objetivos

Parte 1: Diagnosticar y reparar la capa física

Parte 2: Diagnosticar y reparar la capa de enlace de datos

Parte 3: Diagnosticar y reparar la capa de red

Situación

Se le pidió que resuelva los problemas de las conexiones WAN de una compañía telefónica local (**Telco**). El router Telco se debe comunicar con cuatro sitios remotos, pero ninguno de estos funciona. Aplique sus conocimientos del modelo OSI y algunas reglas generales para identificar y resolver los errores en la red.

Parte 1: Diagnosticar y reparar la capa física

Paso 1: Diagnosticar y reparar el cableado.

a. Examine la tabla de direccionamiento para determinar la ubicación de las conexiones DCE.

b. Cada conexión serial tiene una conexión DCE y una DTE. Para determinar si todas las interfaces de **Telco** utilizan el extremo correcto del cable, observe la tercera línea del resultado del comando **show controllers** que se muestra a continuación.

```
Telco# show controllers [interface_type interface_num]
```

c. Revierta la conexión incorrecta de cualquier cable.

Nota: el cable entre Telco y el R4 se debe invertir, y se debe establecer la frecuencia de reloj en Telco. El cable serial en el R4 debe conectar a S0/0/1.

Nota: en configuraciones de redes reales, la conexión DCE (que establece la frecuencia de reloj) suele ser una CSU/DSU.

Paso 2: Diagnosticar y reparar las conexiones de puerto incorrectas.

a. Examine la tabla de direccionamiento para unir cada puerto de router con el puerto de **Telco** correcto.

b. Mantenga el puntero del mouse sobre cada cable para asegurarse de que los cables estén conectados según lo especificado. De lo contrario, corrija las conexiones.

Paso 3: Diagnosticar y reparar los puertos que están desactivados.

a. Muestre un breve resumen de la interfaz de cada router. Asegúrese de que todos los puertos que deban estar funcionando no estén administrativamente inactivos.

b. Habilite los puertos apropiados que estén administrativamente inactivos.

```
R3(config)# interface s0/0/0
R3(config-if)# no shutdown
```

Parte 2: Diagnosticar y reparar la capa de enlace de datos

Paso 1: Examinar y establecer las frecuencias de reloj en el equipo DCE.

a. Todos los cables DCE se deben conectar a **Telco**. Muestre la configuración en ejecución de **Telco** para verificar que se haya establecido la frecuencia de reloj en cada interfaz.

b. Establezca la frecuencia de reloj de cualquier interfaz serial que lo requiera.

```
Telco(config)# interface s0/0/0
Telco(config-if)# clock rate 4000000
Telco(config-if)# interface s0/1/1
Telco(config-if)# clock rate 4000000
```

Paso 2: Examinar la encapsulación en el equipo DCE.

a. Todas las interfaces seriales deben utilizar HDLC como tipo de encapsulación. Examine la configuración del protocolo de las interfaces seriales.

```
Telco# show interface [interface_type interface_num]
```

b. Cambie el tipo de encapsulación a HDLC en cualquier interfaz que esté configurada de otra manera.

```
R4(config)# interface s0/0/1
R4(config-if)# encapsulation hdlc
```

Parte 3: Diagnosticar y reparar la capa de red

Paso 1: Verificar el direccionamiento IP.

a. Muestre un breve resumen de la interfaz de cada router. Compare las direcciones IP con la tabla de direccionamiento y asegúrese de que estén en la subred correcta con su interfaz de conexión.

b. Corrija cualquier dirección IP que se superponga o que esté establecida para el host o la dirección de difusión.

```
R1(config)# interface s0/0/0
R1(config-if)# ip address 64.100.34.18 255.255.255.252
```

Paso 2: Verificar la conectividad entre todos los routers.

Packet Tracer: Configuración de la autenticación PAP y CHAP (versión para el instructor)

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

Topología

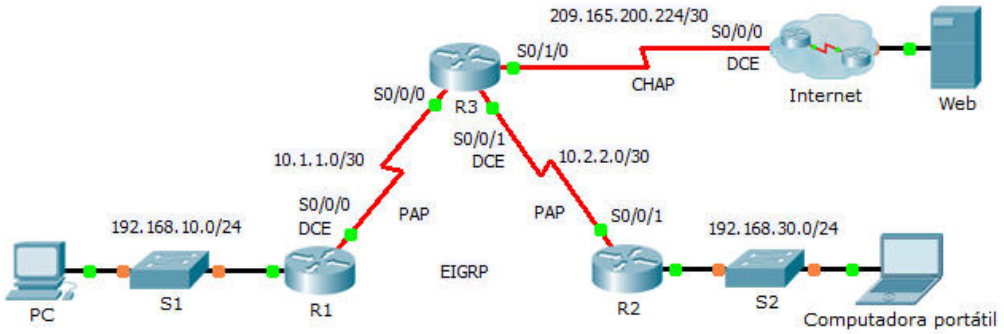


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	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
	S0/1/0	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.252	N/A
	G0/0	209.165.200.1	255.255.255.252	N/A
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Laptop	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos

Parte 1: Revisar las configuraciones del routing

Parte 2: Configurar PPP como el método de encapsulación

Parte 3: Configurar la autenticación PPP

Información básica

En esta actividad, practicará la configuración de la encapsulación PPP en los enlaces seriales. Por último, configurará la autenticación PAP de PPP y CHAP de PPP.

Parte 1: Revisar las configuraciones del routing

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

Mientras revisa la configuración del router, observe el uso de rutas tanto estáticas como dinámicas en la topología.

Paso 2: Probar la conectividad entre las computadoras y el servidor web.

Desde **PC** y **Laptop** (Computadora portátil), haga ping al servidor web en 209.165.200.2. Ambos comandos **ping** deben tener éxito. Recuerde esperar el tiempo suficiente para que el STP y el EIGRP converjan.

Parte 2: Configurar PPP como el método de encapsulación

Paso 1: Configurar el R1 para que utilice la encapsulación PPP con el R3.

Introduzca los siguientes comandos en el **R1**:

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp
```

Paso 2: Configurar el R2 para que utilice la encapsulación PPP con el R3.

Introduzca los comandos apropiados en el **R2**:

```
R2(config)# interface s0/0/1
R2(config-if)# encapsulation ppp
```

Paso 3: Configurar el R3 para que utilice la encapsulación PPP con el R1, el R2 y el ISP.

Introduzca los comandos apropiados en el **R3**:

```
R3(config)# interface s0/0/0
R3(config-if)# encapsulation ppp
R3(config)# interface s0/0/1
R3(config-if)# encapsulation ppp
R3(config)# interface s0/1/0
R3(config-if)# encapsulation ppp
```


Paso 4: Configurar el ISP para que utilice la encapsulación PPP con el R3.

a. Haga clic en la nube de **Internet** y, después, en ISP. Introduzca los siguientes comandos:

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation ppp
```

b. Salga de la nube de **Internet** haciendo clic en **Back** (Atrás) en la esquina superior izquierda de la pantalla o presionando **Alt+flecha izquierda**.

Paso 5: Probar la conectividad al servidor web.

PC y **Laptop** deben poder hacer ping al servidor web en 209.165.200.2. Esto puede llevar algo de tiempo, dado que las interfaces comienzan a funcionar nuevamente y EIGRP vuelve a convergir.

Parte 3: Configurar la autenticación PPP

Paso 1: Configurar la autenticación PAP de PPP entre el R1 y el R3.

Nota: en lugar de utilizar la palabra clave **password**, como se muestra en el currículo, utilizará la palabra clave **secret** para proporcionar un mejor cifrado de la contraseña.

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

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco
```

b. Introduzca los siguientes comandos en el **R3**:

```
R3(config)# username R1 secret cisco
R3(config)# interface s0/0/0
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

Paso 2: Configurar la autenticación PAP de PPP entre el R2 y el R3.

Repita el paso 1 para configurar la autenticación entre el **R2** y el **R3** y modifique los nombres de usuario según sea necesario. Observe que cada contraseña enviada en cada puerto serie coincide con la contraseña que espera el router opuesto.

```
R2(config-if)# username R3 secret class
R2(config)# interface s0/0/1
R2(config-if)# ppp authentication pap
R2(config-if)# ppp pap sent-username R2 password cisco

R3(config-if)# username R2 secret cisco
R3(config)# interface s0/0/1
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

Paso 3: Configurar la autenticación CHAP de PPP entre el R3 y el ISP.

a. Introduzca los siguientes comandos en el **ISP**. El nombre de host se envía como el nombre de usuario:

```
Router(config)# hostname ISP
ISP(config)# username R3 secret cisco
ISP(config)# interface s0/0/0
ISP(config-if)# ppp authentication chap
```

b. Introduzca los siguientes comandos en el **R3**. Para la autenticación CHAP, las contraseñas deben coincidir:

```
R3(config)# username ISP secret cisco
R3(config)# interface serial0/1/0
R3(config-if)# ppp authentication chap
```

Paso 4: Probar la conectividad entre las computadoras y el servidor web.

Desde **PC** y **Laptop** (Computadora portátil), haga ping al servidor web en 209.165.200.2. Ambos comandos **ping** deben tener éxito. Recuerde esperar el tiempo suficiente para que el STP y el EIGRP converjan.

Packet Tracer: Resolución de problemas de PPP con autenticación (versión para el instructor)

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

Topología

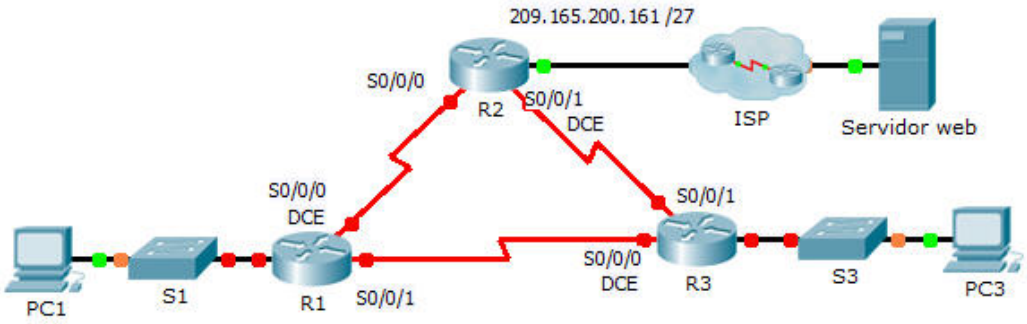


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	10.0.0.1	255.255.255.128	N/A
	S0/0/0	172.16.0.1	255.255.255.252	N/A
	S0/0/1	172.16.0.9	255.255.255.252	N/A
R2	G0/1	209.165.200.161	255.255.255.224	N/A
	S0/0/0	172.16.0.2	255.255.255.252	N/A
	S0/0/1	172.16.0.5	255.255.255.252	N/A
R3	G0/1	10.0.0.129	255.255.255.128	N/A
	S0/0/0	172.16.0.10	255.255.255.252	N/A
	S0/0/1	172.16.0.6	255.255.255.252	N/A
ISP	G0/1	209.165.200.162	255.255.255.224	N/A
PC1	NIC	10.0.0.10	255.255.255.128	10.0.0.1
PC3	NIC	10.0.0.139	255.255.255.128	10.0.0.129
Web Server	NIC	209.165.200.2	255.255.255.252	209.165.200.1

Objetivos

Parte 1: Diagnosticar y reparar la capa física

Parte 2: Diagnosticar y reparar la capa de enlace de datos

Parte 3: Diagnosticar y reparar la capa de red

Situación

Un ingeniero de redes inexperto configuró los routers de la compañía. Varios errores en la configuración han resultado en problemas de conectividad. El jefe le solicitó al usuario que resuelva y corrija los errores de configuración y que documente su trabajo. Según los conocimientos de PPP y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los enlaces seriales utilicen la autenticación PPP CHAP y de que todas las redes sean alcanzables. Las contraseñas son **cisco** y **class**.

Parte 1: Diagnosticar y reparar la capa física

Paso 1: Diagnosticar y reparar el cableado.

a. Examine la **tabla de direccionamiento** para determinar la ubicación de todas las conexiones.

b. Verifique que los cables estén conectados según lo especificado.

c. Diagnostique y repare cualquier interfaz inactiva.

```
R1(config-if)# interface g0/1
R1(config-if)# no shutdown
R1(config)# interface s0/0/0
R1(config-if)# no shutdown
R1(config-if)# interface s0/0/1
R1(config-if)# no shutdown

R2(config)# interface s0/0/0
R2(config-if)# no shutdown
R2(config-if)# interface s0/0/1
R2(config-if)# no shutdown

R3(config)# interface g0/1
R3(config-if)# no shutdown
R3(config-if)# interface s0/0/0
R3(config-if)# no shutdown
R3(config-if)# interface s0/0/1
R3(config-if)# no shutdown
```


Parte 2: Diagnosticar y reparar la capa de enlace de datos

Paso 1: Examinar y establecer las frecuencias de reloj en el equipo DCE.

Examine la configuración de cada router para verificar que se haya establecido la frecuencia de reloj en las interfaces apropiadas. Establezca la frecuencia de reloj de cualquier interfaz serial que lo requiera.

```
R2(config)# interface s0/0/1
R2(config-if)# clock rate 64000
```

Paso 2: Examinar la encapsulación en el equipo DCE.

Todas las interfaces seriales deben utilizar PPP como tipo de encapsulación. Cambie el tipo de encapsulación a PPP en cualquier interfaz que esté configurada de otra manera.

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp

R2(config)# interface s0/0/1
R2(config-if)# encapsulation ppp

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

Paso 3: Examinar y establecer los nombres de usuario y las contraseñas de CHAP.

Examine todos los enlaces para verificar que cada router inicie sesión en los demás routers de forma correcta. Todas las contraseñas de CHAP están establecidas como **cisco**. Si es necesario, utilice el comando **debug ppp authentication**. Corrija o establezca cualquier nombre de usuario y contraseña que sea necesario.

```
R1(config)# username R3 password cisco
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication chap
R1(config-if)# interface s0/0/1
R1(config-if)# ppp authentication chap

R2(config)# username R1 password cisco
R2(config)# no username R11
R2(config)# interface s0/0/1
R2(config-if)# ppp authentication chap

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

Parte 3: Diagnosticar y reparar la capa de red

Paso 1: Verificar el direccionamiento IP.

Compare las direcciones IP con la tabla de direccionamiento y asegúrese de que estén en la subred correcta con su interfaz de conexión. Corrija cualquier dirección IP que se superponga, que esté en la interfaz incorrecta, que tenga una dirección de subred incorrecta o que esté establecida para el host o la dirección de difusión.

```
R1(config)# interface g0/0
R1(config-if)# no ip address
R1(config-if)# interface g0/1
R1(config-if)# ip address 10.0.0.1 255.255.255.128
R1(config-if)# interface s0/0/0
R1(config-if)# ip address 172.16.0.1 255.255.255.252

R2(config)# interface g0/1
R2(config-if)# ip address 209.165.200.161 255.255.255.224

R3(config)# interface g0/1
R3(config-if)# ip address 10.0.0.129 255.255.255.128
R3(config-if)# interface s0/0/1
R3(config-if)# ip address 172.16.0.6 255.255.255.252
```

Paso 2: Verificar la plena conectividad mediante el rastreo de una ruta de la PC1 y la PC3 al servidor web.

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

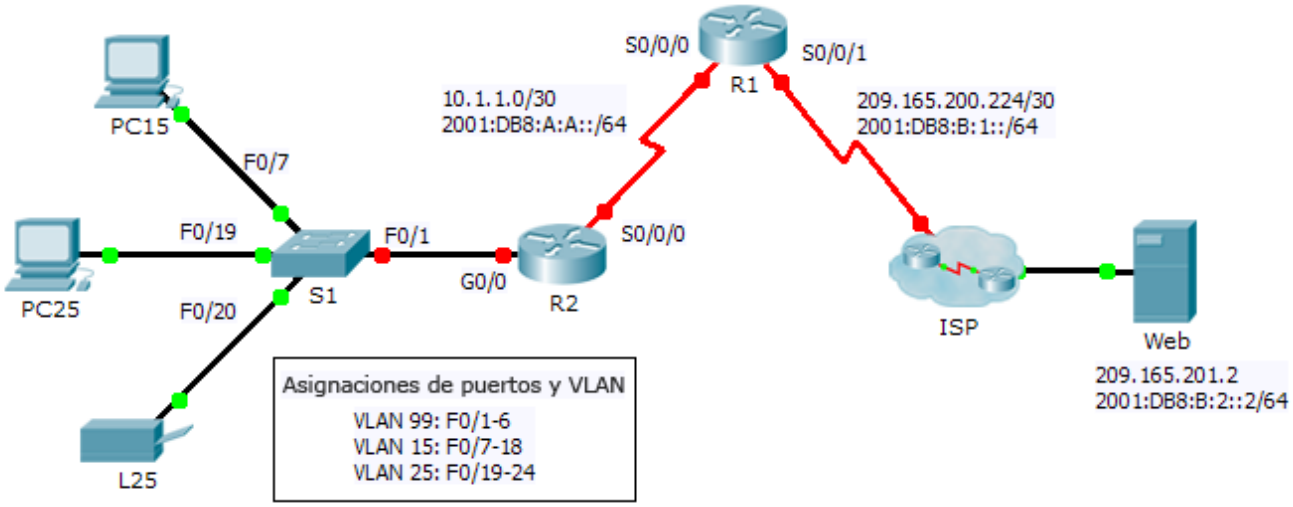


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado IPv4 e IPv6
		Dirección/Prefijo IPv6		
R1	S0/0/0	10.1.1.2	255.255.255.252	N/A
		2001:DB8:A:A::2/64		FE80::1
	S0/0/1	209.165.200.226	255.255.255.252	N/A
		2001:DB8:B:1::2/64		FE80::1
R2	G0/0.1	192.168.1.193	255.255.255.224	N/A
		2001:DB8:A:1::1/64		FE80::2
	G0/0.15	192.168.1.1	255.255.255.128	N/A
		2001:DB8:A:15::1/64		FE80::2
	G0/0.25	192.168.1.129	255.255.255.192	N/A
		2001:DB8:A:25::1/64		FE80::2
	G0/0.99	192.168.1.225	255.255.255.224	N/A
		2001:DB8:A:99::1/64		FE80::2
	S0/0/0	10.1.1.1	255.255.255.252	N/A
		2001:DB8:A:A::1/64		FE80::2
S1	VLAN 99	192.168.1.226	255.255.255.224	192.168.1.225
PC15	NIC	192.168.1.2	255.255.255.128	192.168.1.1
		2001:DB8:A:15::2/64		FE80::2
PC25	NIC	192.168.1.130	255.255.255.192	192.168.1.129
		2001:DB8:A:25::2/64		FE80::2
L25	NIC	192.168.1.190	255.255.255.192	192.168.1.129
		2001:DB8:A:25::A/64		FE80::2

Información básica

Esta actividad le permite poner en práctica diversas aptitudes, incluida la configuración de VLAN, PPP con CHAP, el routing estático y predeterminado, y el uso de IPv4 e IPv6. Debido a la gran cantidad de elementos con calificación, puede hacer clic en **Check Results** (Verificar resultados) y después, **Assessment Items** (Elementos de evaluación) para ver si introdujo correctamente un comando con calificación. Utilice las contraseñas **cisco** y **class** para acceder al modo EXEC privilegiado de la CLI para routers y switches.

Requisitos

Direccionamiento

- El esquema de direccionamiento utiliza el espacio de direcciones 192.168.1.0/24. Hay espacio de direcciones adicional entre la VLAN 15 y la VLAN 1. La VLAN 25 necesita direcciones suficientes para 50 hosts. Determine la subred y complete la tabla de subredes a continuación.

VLAN	Dirección de subred IPv4	Máscara de subred	Hosts
1	192.168.1.192	255.255.255.224	20
15	192.168.1.0	255.255.255.128	100
25	192.168.1.128	255.255.255.192	50
99	192.168.1.224	255.255.255.224	20

- Complete la **tabla de direccionamiento** asignando las siguientes direcciones a la VLAN 25:
  - **G0/0.25 del R2:** primera dirección IPv4
  - **PC25:** segunda dirección IPv4
  - **L25:** última dirección IPv4
- Configure el direccionamiento IPv4 en las terminales necesarias.
- En el **R2**, cree y aplique el direccionamiento IPv4 e IPv6 a la subinterfaz G0/0.25.

VLAN

- En el **S1**, cree la VLAN 86 y asígnele el nombre **BlackHole**.
- Configure los puertos del **S1** en modo estático con los siguientes requisitos:
  - **F0/1** es el enlace troncal nativo para la VLAN 99.
  - **F0/7 a F0/18** como puertos de acceso en la VLAN 15.
  - **F0/19 a F0/24** como puertos de acceso en la VLAN 25.
  - **G1/1 a 2** y **F0/2 a F0/6** no se utilizan. Deben estar correctamente asegurados y asignados a la VLAN **BlackHole**.
- En el **R2**, configure el routing entre VLAN. La VLAN 99 es la VLAN nativa.

PPP

- Configure el **R1** y el **R2** para que utilicen PPP con CHAP para el enlace compartido. La contraseña para CHAP es **cisco**.

Routing

- En el **R1**, configure las rutas predeterminadas IPv4 e IPv6 usando la interfaz de salida apropiada.
- En el **R2**, configure una ruta predeterminada IPv6 usando la interfaz de salida apropiada.
- Configure OSPF para IPv4 con los siguientes requisitos:
  - Utilice la ID de proceso 1
  - Los routers **R1** y **R2** están en el área 0.
  - El **R1** utiliza la ID de router 1.1.1.1.

- El **R2** utiliza la ID de router 2.2.2.2.
- Anuncie subredes específicas.
- En el **R1**, propague la ruta predeterminada IPv4 creada.

- Configure OSPF para IPv6 con los siguientes requisitos:
  - Utilice la ID de proceso 1
  - Los routers **R1** y **R2** están en el área 0.
  - Configure OSPF en las interfaces correspondientes en el **R1** y el **R2**.
  - El **R1** utiliza la ID de router 1.1.1.1.
  - El **R2** utiliza la ID de router 2.2.2.2.

Conectividad

- Todos los dispositivos deben poder hacer ping al servidor web.

Respuestas

```
!!!Configure PC25 and L25 with IPv4 Addressing
!!!!!!!!R1
en
config t
ipv6 unicast-routing
username R2 password 0 cisco
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
 ipv6 ospf 1 area 0
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 default-information originate
 router-id 1.1.1.1
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
ipv6 route ::/0 Serial0/0/1
end
wr

!!!!!!!!R2
ena
```



```
config t
ipv6 unicast-routing
username R1 password 0 cisco
!
int g0/0
 no shut
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1
 ip add 192.168.1.193 255.255.255.224
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip add 192.168.1.1 255.255.255.128
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.25
 encapsulation dot1Q 25
 ip address 192.168.1.129 255.255.255.192
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:A:25::1/64
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99 native
 ip add 192.168.1.225 255.255.255.224
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
 ipv6 ospf 1 area 0
!
router ospf 1
 router-id 2.2.2.2
 network 192.168.1.0 0.0.0.127 area 0
 network 192.168.1.128 0.0.0.63 area 0
 network 192.168.1.192 0.0.0.31 area 0
 network 192.168.1.224 0.0.0.31 area 0
```

```
 network 10.1.1.0 0.0.0.3 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
ipv6 route ::/0 Serial0/0/0
end
wr

!!!!!!!!!!S1
en
conf t
vlan 86
name BlackHole
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range Gig1/1 - 2 , FastEthernet0/2 - 6
 switchport access vlan 86
 switchport mode access
 shutdown
!
interface range FastEthernet0/7 - 18
 switchport access vlan 15
 switchport mode access
!
interface range FastEthernet0/19 - 24
 switchport access vlan 25
 switchport mode access
!
end
wr
```

Packet Tracer: Configuración de mapas estáticos de Frame Relay (versión para el instructor)

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

Topología

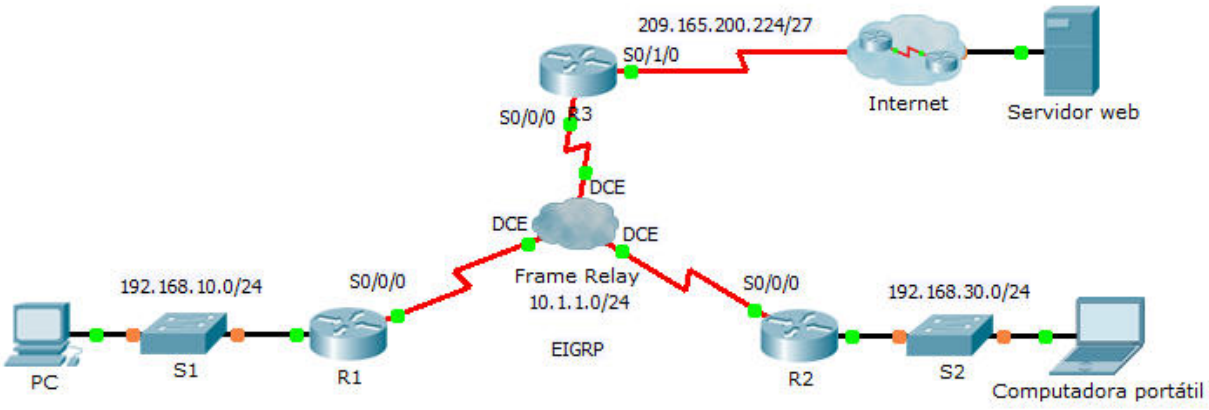


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.0	N/A
R2	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.0	N/A
R3	S0/0/0	10.1.1.3	255.255.255.0	N/A
	S0/1/0	209.165.200.225	255.255.255.224	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.224	N/A
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Laptop	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos

Parte 1: Configurar Frame Relay

Parte 2: Configurar mapas estáticos de Frame Relay y tipos de LMI

Situación

En esta actividad, configurará dos mapas estáticos de Frame Relay. Si bien el tipo LMI se detecta automáticamente en los routers, asignará el tipo de manera estática mediante la configuración manual de la LMI.

Parte 1: Configurar Frame Relay

Paso 1: Configurar la encapsulación de Frame Relay en la interfaz S0/0/0 del R1.

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation frame-relay
```

Paso 2: Configurar la encapsulación de Frame Relay en la interfaz S0/0/0 del R2 y el R3.

```
R2(config)# interface s0/0/0
R2(config-if)# encapsulation frame-relay

R3(config)# interface s0/0/0
R3(config-if)# encapsulation frame-relay
```

Paso 3: Probar la conectividad.

Desde el símbolo del sistema de **PC**, verifique la conectividad a **Laptop** (Computadora portátil), ubicada en 192.168.30.10, mediante el comando **ping**.

El ping de **PC** a **Laptop** debe fallar, dado que el **R1** no tiene una ruta para llegar a la red 192.168.30.0. El **R1** debe configurarse con un mapa de Frame Relay para que pueda encontrar el destino del siguiente salto y así alcanzar dicha red.

Parte 2: Configurar mapas estáticos de Frame Relay y tipos de LMI

Cada router necesita dos mapas estáticos para poder alcanzar a los demás routers. A continuación se indican los DLCI para llegar a estos routers.

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

a. Configure el **R1** para que utilice mapas estáticos de Frame Relay. Utilice **DLCI 102** para la comunicación del **R1** al **R2**. Utilice **DLCI 103** para la comunicación del **R1** al **R3**. Los routers también deben admitir multidifusión EIGRP en 224.0.0.10; por lo tanto, se requiere la palabra clave **broadcast**.

```
R1(config)# interface s0/0/0
R1(config-if)# frame-relay map ip 10.1.1.2 102 broadcast
R1(config-if)# frame-relay map ip 10.1.1.3 103 broadcast
```

b. Configure el **R2** para que utilice mapas estáticos de Frame Relay. Utilice **DLCI 201** para la comunicación del **R2** al **R1**. Utilice **DLCI 203** para la comunicación del **R2** al **R3**. Utilice la dirección IP correcta para cada mapa.

```
R2(config)# interface s0/0/0
R2(config-if)# frame-relay map ip 10.1.1.1 201 broadcast
R2(config-if)# frame-relay map ip 10.1.1.3 203 broadcast
```

c. Configure el **R3** para que utilice mapas estáticos de Frame Relay. Utilice **DLCI 301** para la comunicación del **R3** al **R1**. Utilice **DLCI 302** para la comunicación del **R3** al **R2**. Utilice la dirección IP correcta para cada mapa.

```
R3(config)# interface s0/0/0
R3(config-if)# frame-relay map ip 10.1.1.1 301 broadcast
R3(config-if)# frame-relay map ip 10.1.1.2 302 broadcast
```

Paso 2: Configurar ANSI como el tipo de LMI en el R1, el R2 y el R3.

Introduzca el siguiente comando en la interfaz serial de cada router:

```
R1(config-if)# frame-relay lmi-type ansi
R2(config-if)# frame-relay lmi-type ansi
R3(config-if)# frame-relay lmi-type ansi
```

Paso 3: Verificar la conectividad.

Ahora, **PC** y **Laptop** deben poder hacer ping entre sí y al **servidor web** correctamente.

Packet Tracer: Configuración de subinterfaces punto a punto de Frame Relay (versión para el instructor)

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

Topología

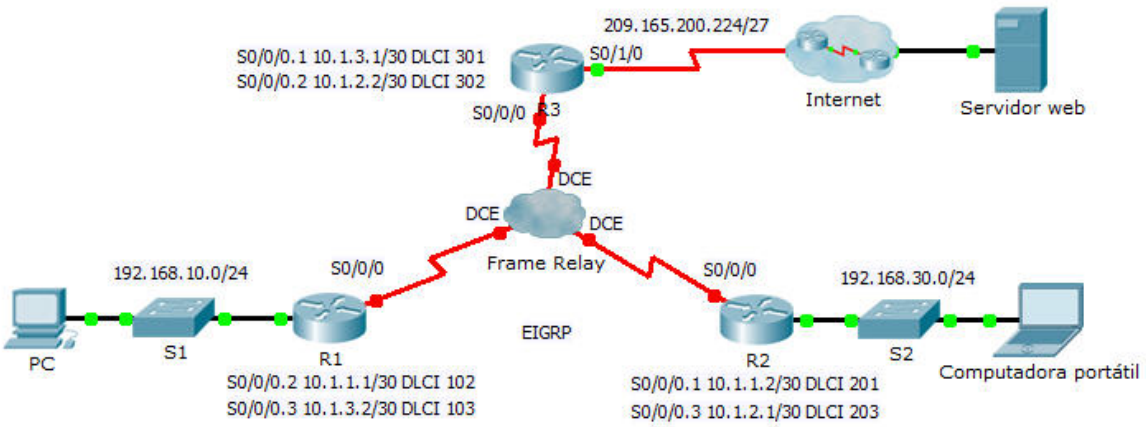


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0.2	10.1.1.1	255.255.255.252	N/A
	S0/0/0.3	10.1.3.2	255.255.255.252	N/A
R2	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0.1	10.1.1.2	255.255.255.252	N/A
	S0/0/0.3	10.1.2.1	255.255.255.252	N/A
R3	S0/0/0.1	10.1.3.1	255.255.255.252	N/A
	S0/0/0.2	10.1.2.2	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.224	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.224	N/A
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Laptop	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos

Parte 1: Configurar Frame Relay

Parte 2: Configurar las subinterfaces punto a punto de Frame Relay

Parte 3: Verificar las configuraciones y la conectividad

Situación

En esta actividad, configurará Frame Relay con dos subinterfaces en cada router para llegar a los otros dos routers. También configurará EIGRP y verificará la conectividad de extremo a extremo.

Parte 1: Configurar Frame Relay

Paso 1: Configurar la encapsulación de Frame Relay en la interfaz S0/0/0 del R1.

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation frame-relay
R1(config-if)# no shutdown
```

Paso 2: Configurar la encapsulación de Frame Relay en la interfaz S0/0/0 del R2 y el R3.

```
R2(config)# interface s0/0/0
R2(config-if)# encapsulation frame-relay
R2(config-if)# no shutdown

R3(config)# interface s0/0/0
R3(config-if)# encapsulation frame-relay
R3(config-if)# no shutdown
```

Paso 3: Probar la conectividad.

Desde el símbolo del sistema de **PC**, verifique la conectividad a **Laptop** (Computadora portátil), ubicada en 192.168.30.10, mediante el comando **ping**.

El ping de **PC** a **Laptop** debe fallar, dado que el router **R1** no tiene una ruta para llegar a la red 192.168.30.0. El **R1** se debe configurar con Frame Relay en las subinterfaces para que pueda encontrar el destino del siguiente salto para alcanzar dicha red.

Parte 2: Configurar las subinterfaces punto a punto de Frame Relay

Cada router necesita dos subinterfaces para poder llegar a los otros routers. A continuación se indican los DLCI para llegar a estos routers.

Paso 1: Configurar subinterfaces en el R1, el R2 y el R3.

a. Configure el **R1** para que utilice subinterfaces. **DLCI 102** se utiliza para la comunicación del **R1** al **R2**, mientras que **DLCI 103** se utiliza para la comunicación del **R1** al **R3**.

```
R1(config)# interface s0/0/0.2 point-to-point
R1(config-subif)# ip address 10.1.1.1 255.255.255.252
R1(config-subif)# frame-relay interface-dlci 102
R1(config-subif)# interface s0/0/0.3 point-to-point
R1(config-subif)# ip address 10.1.3.2 255.255.255.252
R1(config-subif)# frame-relay interface-dlci 103
```

b. Agregue entradas de red al sistema autónomo de EIGRP 1 para reflejar las direcciones IP que se indican arriba.

```
R1(config)# router eigrp 1
R1(config-router)# network 10.1.1.0 0.0.0.3
R1(config-router)# network 10.1.3.0 0.0.0.3
```

c. Configure el **R2** para que utilice subinterfaces. **DLCI 201** se utiliza para la comunicación del **R2** al **R1**, mientras que **DLCI 203** se utiliza para la comunicación del **R2** al **R3**. Utilice la dirección IP correcta en la **tabla de direccionamiento** para cada subinterfaz.

```
R2(config)# interface s0/0/0.1 point-to-point
R2(config-subif)# ip address 10.1.1.2 255.255.255.252
R2(config-subif)# frame-relay interface-dlci 201
R2(config-subif)# interface s0/0/0.3 point-to-point
R2(config-subif)# ip address 10.1.2.1 255.255.255.252
R2(config-subif)# frame-relay interface-dlci 203
R2(config-subif)# exit
```

d. Agregue las entradas EIGRP apropiadas al **R2** para el sistema autónomo 1.

```
R2(config)# router eigrp 1
R2(config-router)# network 10.1.1.0 0.0.0.3
R2(config-router)# network 10.1.2.0 0.0.0.3
```

e. Configure el **R3** para que utilice subinterfaces. **DLCI 301** se utiliza para la comunicación del **R3** al **R1**, mientras que **DLCI 302** se utiliza para la comunicación del **R3** al **R2**. Utilice la dirección IP correcta para cada subinterfaz.

```
R3(config)# interface s0/0/0.1 point-to-point
R3(config-subif)# ip address 10.1.3.1 255.255.255.252
R3(config-subif)# frame-relay interface-dlci 301
R3(config-subif)# interface s0/0/0.2 point-to-point
R3(config-subif)# ip address 10.1.2.2 255.255.255.252
R3(config-subif)# frame-relay interface-dlci 302
R3(config-subif)# exit
```

f. Agregue las entradas EIGRP apropiadas al **R3** para el sistema autónomo 1.

```
R3(config)# router eigrp 1
R3(config-router)# network 10.1.3.0 0.0.0.3
R3(config-router)# network 10.1.2.0 0.0.0.3
```

Parte 3: Verifique las configuraciones y la conectividad.

Paso 1: Verificar la configuración de Frame Relay.

Muestre la información acerca de Frame Relay y las conexiones que se realizaron. Observe los campos para BECN, FECN, DE, DLCI y LMI TYPE (Tipo de LMI).

```
R1# show frame-relay map
R1# show frame-relay pvc
R1# show frame-relay lmi
```

Paso 2: Verificar la conectividad de extremo a extremo.

PC y **Laptop** deben poder hacer ping entre sí y al **servidor web** correctamente.

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

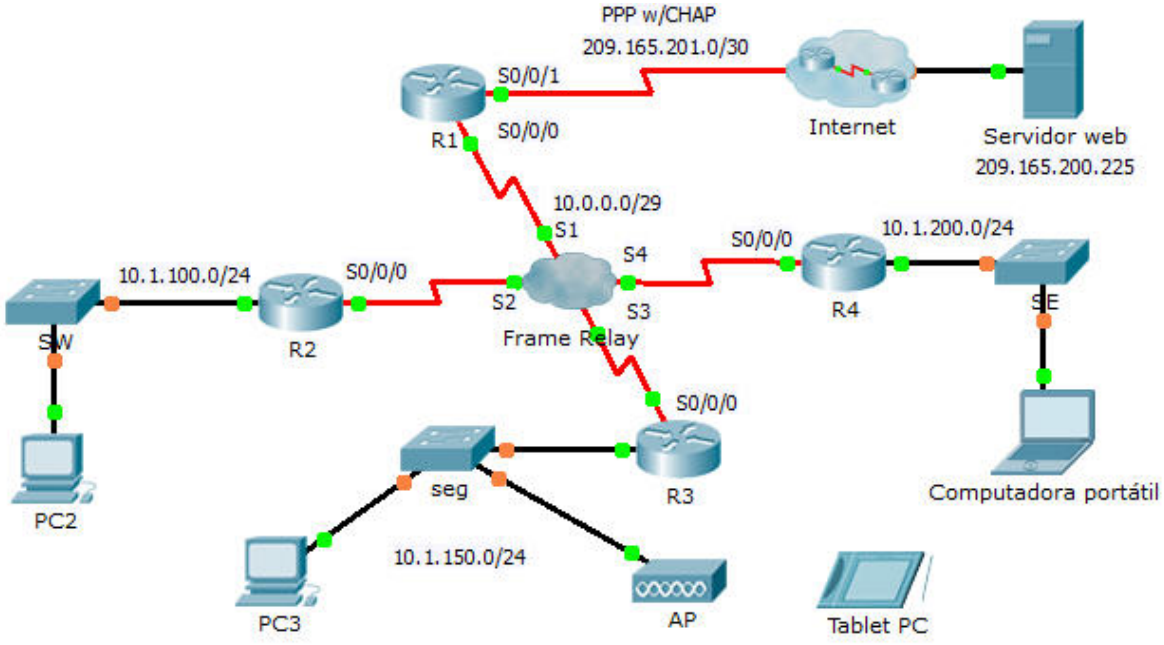


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	S0/0/0	10.0.0.1	255.255.255.248	N/A
	S0/0/1	209.165.201.2	255.255.255.252	N/A
R2	G0/0	10.1.100.1	255.255.255.0	N/A
	S0/0/0	10.0.0.2	255.255.255.248	N/A
R3	G0/0	10.1.150.1	255.255.255.0	N/A
	S0/0/0	10.0.0.3	255.255.255.248	N/A
R4	G0/0	10.1.200.1	255.255.255.0	N/A
	S0/0/0	10.0.0.4	255.255.255.248	N/A
Web	NIC	209.165.200.226	255.255.255.252	209.165.200.225
PC2	NIC	10.1.100.10	255.255.255.0	10.1.100.1
PC3	NIC	10.1.150.10	255.255.255.0	10.1.150.1
Tablet PC	NIC	10.1.150.20	255.255.255.0	10.1.150.1
Laptop	NIC	10.1.200.10	255.255.255.0	10.1.200.1

Asignaciones de DLCI

De/Para	R1	R2	R3	R4
R1	-	102	103	104
R2	201	-	203	204
R3	301	302	-	304
R4	401	402	403	-

Información básica

Esta actividad le permite poner en práctica diversas aptitudes, incluida la configuración de Frame Relay, PPP con CHAP, EIGRP, routing estático y predeterminado.

Requisitos

R1

- Configure el **R1** para que utilice PPP con CHAP en el enlace a Internet. **ISP** es el nombre de host del router. La contraseña para CHAP es **cisco**.
- Configure una ruta predeterminada a Internet. Utilice la interfaz de salida.
- Configure una ruta estática a la LAN en el **R4**. Utilice la dirección IP del siguiente salto.
- Configure EIGRP.
  - Utilice el número de AS 100.

- Anuncie la red 10.0.0.0/8 completa y deshabilite la sumarización automática.
- Propague la ruta predeterminada.

- Configure Frame Relay de malla completa.
  - Configure la encapsulación de Frame Relay.
  - Configure un mapa a cada uno de los demás routers. El PVC al **R4** utiliza encapsulación IETF.
  - El tipo de LMI es ANSI.

R2 y R3

- Configure EIGRP.
  - Utilice el número de AS 100.
  - Anuncie la red 10.0.0.0/8 completa y deshabilite la sumarización automática.
  - No envíe mensajes EIGRP por las interfaces LAN.
- Configure Frame Relay de malla completa.
  - Configure la encapsulación de Frame Relay.
  - Configure un mapa a cada uno de los demás routers. El PVC al **R4** utiliza encapsulación IETF.
  - El tipo de LMI es ANSI.

R4

- Configurar el enrutamiento estático y predeterminado
  - Configure una ruta estática para cada LAN en el **R2** y el **R3**. Utilice la dirección IP del siguiente salto.
  - Configure una ruta predeterminada al R1. Utilice la dirección IP del siguiente salto.
- Configure Frame Relay de malla completa.
  - Configure la encapsulación de Frame Relay mediante IETF.
  - Configure un mapa a cada uno de los demás routers.
  - El tipo de LMI es ANSI.

Verificar la conectividad de extremo a extremo

- Ahora, todas las terminales deben poder hacer ping entre sí y al **servidor web**.
- Si esto no ocurre, haga clic en **Check Results** (Verificar resultados) para ver qué configuración falta. Implemente las correcciones necesarias y vuelva a realizar la prueba para verificar la plena conectividad de extremo a extremo.

Secuencias de comandos de configuración

Router R1

```
en
conf t
username ISP password 0 cisco
interface Serial0/0/0
encapsulation frame-relay
frame-relay map ip 10.0.0.2 102 broadcast
frame-relay map ip 10.0.0.3 103 broadcast
frame-relay map ip 10.0.0.4 104 broadcast ietf
frame-relay lmi-type ansi
interface Serial0/0/1
```



```
encapsulation ppp
ppp authentication chap
router eigrp 100
network 10.0.0.0
no auto-summary
redistribute static
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
ip route 10.1.200.0 255.255.255.0 10.0.0.4
end
copy run start
```

R2 del router

```
en
conf t
interface Serial0/0/0
encapsulation frame-relay
frame-relay map ip 10.0.0.1 201 broadcast
frame-relay map ip 10.0.0.3 203 broadcast
frame-relay map ip 10.0.0.4 204 broadcast ietf
frame-relay lmi-type ansi
router eigrp 100
network 10.0.0.0
no auto-summary
passive-interface g0/0
end
copy run start
```

R3 del router

```
en
conf t
interface Serial0/0/0
encapsulation frame-relay
frame-relay map ip 10.0.0.1 301 broadcast
frame-relay map ip 10.0.0.2 302 broadcast
frame-relay map ip 10.0.0.4 304 broadcast ietf
frame-relay lmi-type ansi
router eigrp 100
network 10.0.0.0
no auto-summary
passive-interface g0/0
end
copy run start
```

R4 del router

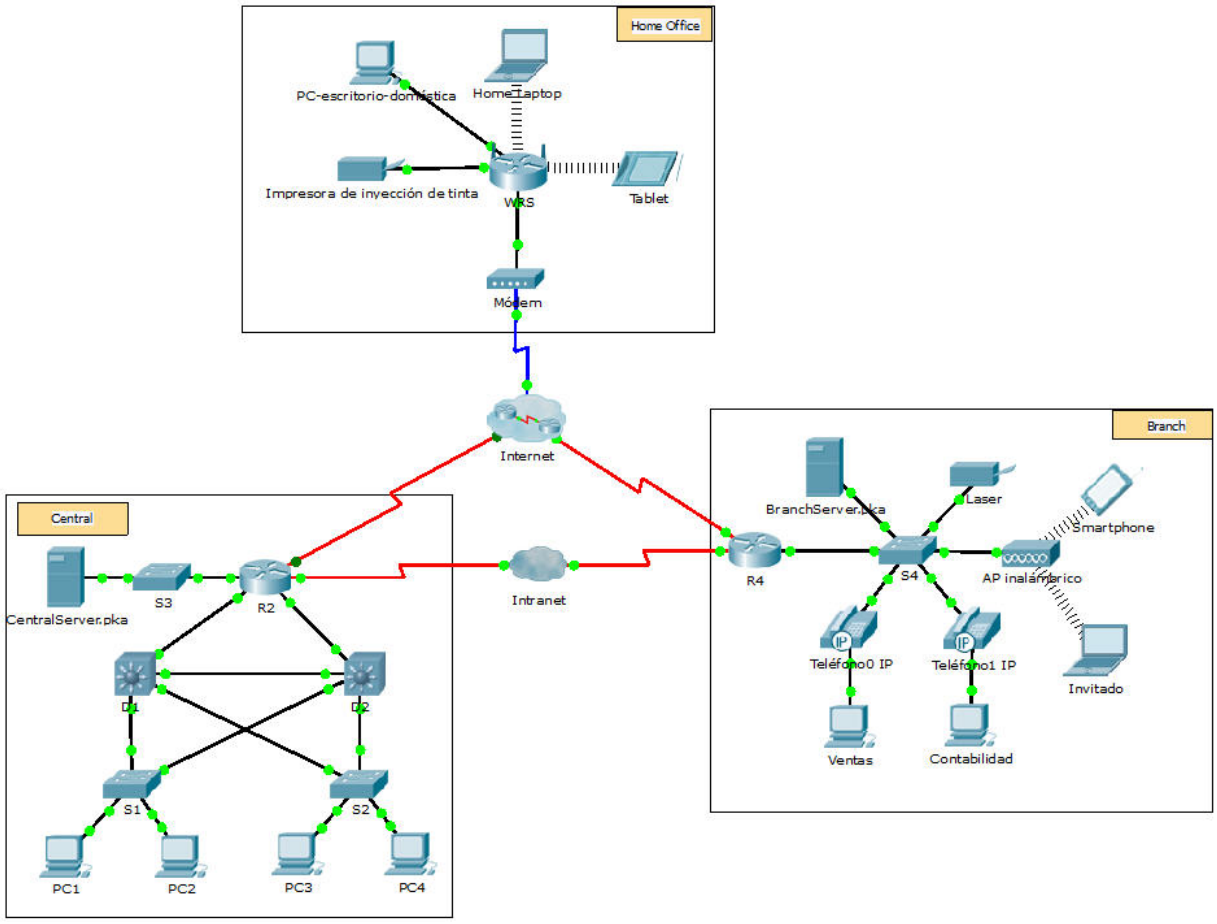
```
en
conf t
interface Serial0/0/0
encapsulation frame-relay ietf
```

```
frame-relay map ip 10.0.0.1 401 broadcast
frame-relay map ip 10.0.0.2 402 broadcast
frame-relay map ip 10.0.0.3 403 broadcast
frame-relay lmi-type ansi
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 10.1.100.0 255.255.255.0 10.0.0.2
ip route 10.1.150.0 255.255.255.0 10.0.0.3
end
copy run start
```

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: analizar el funcionamiento de NAT a través de la intranet

Parte 2: analizar el funcionamiento de NAT a través de Internet

Parte 3: investigación detallada

Situación

A medida que la trama se transmite a través de una red, las direcciones MAC pueden cambiar. Las direcciones IP también pueden cambiar cuando un paquete es reenviado por un dispositivo configurado con NAT. En esta actividad, investigaremos qué sucede a 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 tardar unos minutos. Puede acelerar el proceso si hace clic en Fast Forward Time (Tiempo de avance rápido).

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. Cambie 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** (Capturar/avanzar) hasta que la unidad de datos del protocolo (pdu) llegue a **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 de puerto TCP de origen y de destino en el paquete 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? No.

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 solamente las solicitudes de HTTP.

c. Haga clic en **Ir** en el navegador; se mostrará un sobre de PDU.

d. Haga clic en **Capture/Forward** (Capturar/avanzar) hasta que la unidad de datos del protocolo (pdu) llegue a **WRS**. Registre las direcciones IP de origen y de destino entrantes y las direcciones de origen y de destino salientes. ¿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 aparecieron en los navegadores? Sí.

Parte 3: profundizar la investigación

a. Experimente con más paquetes, tanto HTTP como HTTPS. Hay muchas preguntas que deben considerarse, por ejemplo:

- ¿Aumentan las tablas de traducción NAT?
- ¿La WRS tiene un conjunto de direcciones?
- ¿Es esta la forma en que los equipos del aula se conectan a Internet?
- ¿Por qué NAT utiliza cuatro columnas de direcciones y puertos?

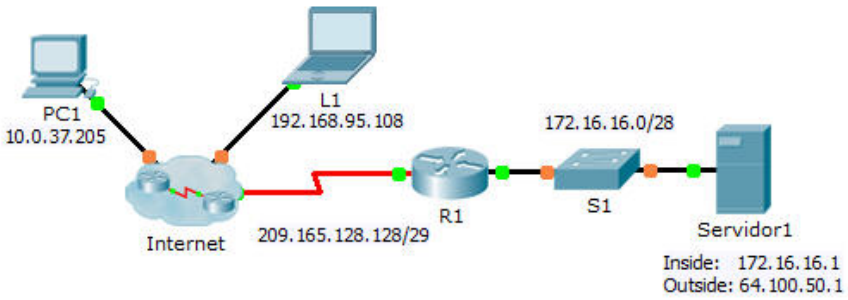
Rúbrica de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	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 NAT estática

Parte 3: probar el acceso con NAT

Situación

En las redes IPv4 configuradas, los clientes y los servidores utilizan direcciones privadas. Para que los paquetes con direcciones privadas puedan transmitirse por Internet, deben traducirse en direcciones públicas. Los servidores a los que se puede acceder desde fuera de la organización generalmente tienen asignadas una dirección IP estática pública y una privada. En esta actividad, deberá configurar 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 **Server1** (Servidor) en 172.16.16.1. Utilice el navegador web para navegar el **Server1** en 172.16.16.1. Los intentos deben 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 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 **Server1** 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 adecuadas.

```
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 **Server1**. Los pings deben tener éxito.

b. Verifique que tanto la **PC1** como la **L1** ahora puedan acceder a la página web del **Server1**.

Paso 2: ver las traducciones NAT.

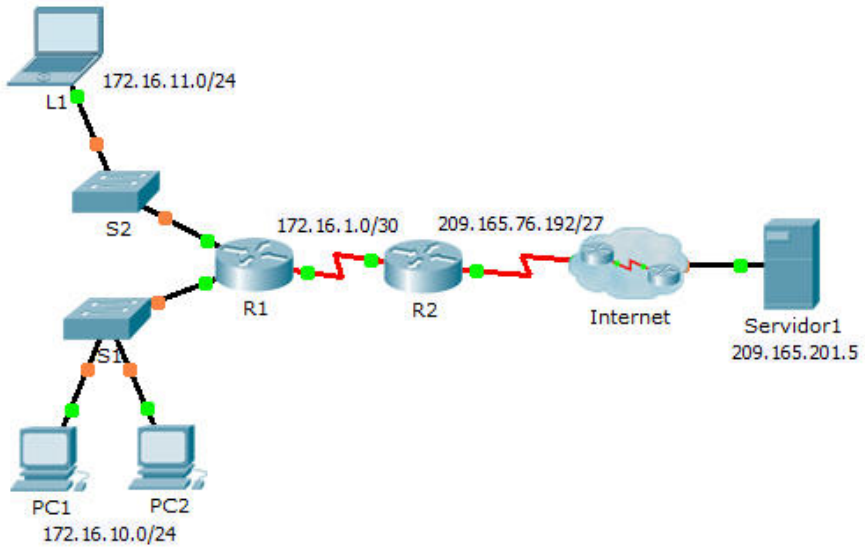
Utilice los siguientes comandos para verificar la configuración de NAT estática:

```
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

Paso 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 sucede si más de dos dispositivos intentan 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 **Server1**.

Paso 2: ver las traducciones NAT.

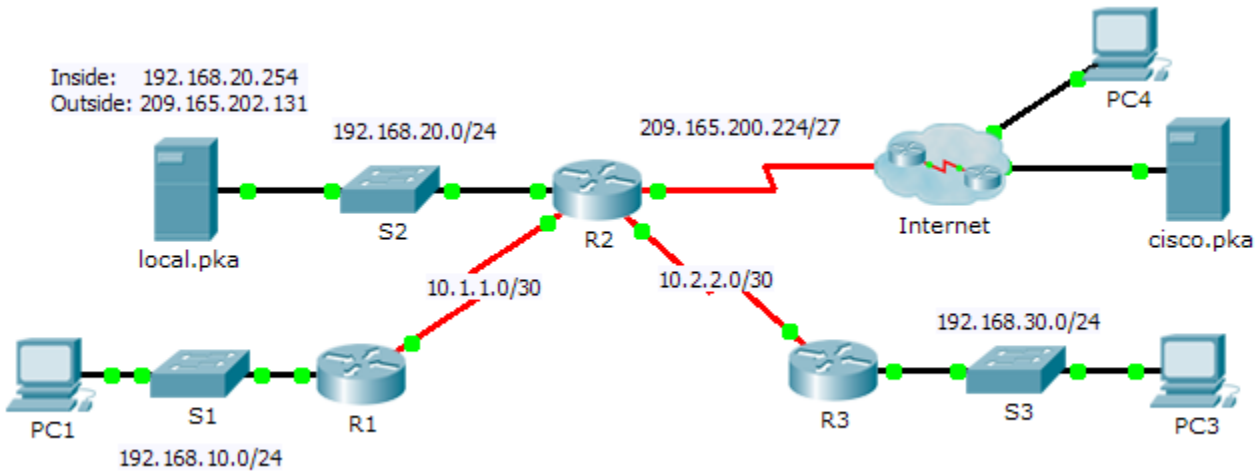
Vea las traducciones NAT en el **R2**.

```
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 NAT dinámica con PAT

Parte 2: configurar NAT estática

Paso 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

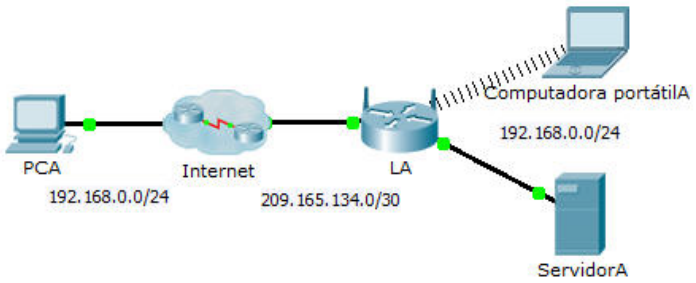


Tabla de direccionamiento

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 puerto

Parte 2: verificar la conectividad remota a ServerA

Situación

Su amigo desea jugar un juego con usted en su servidor. Ambos están en sus respectivos hogares conectados a Internet. Debe configurar su router SOHO (oficinas pequeñas/domésticas) para reenviar solicitudes de HTTP a través del puerto a su servidor 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 **LaptopA** (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 luego introduzca 192.168.0.2 en la columna “To IP Address” (Dirección de origen). Esto configura **LA** para reenviar el 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

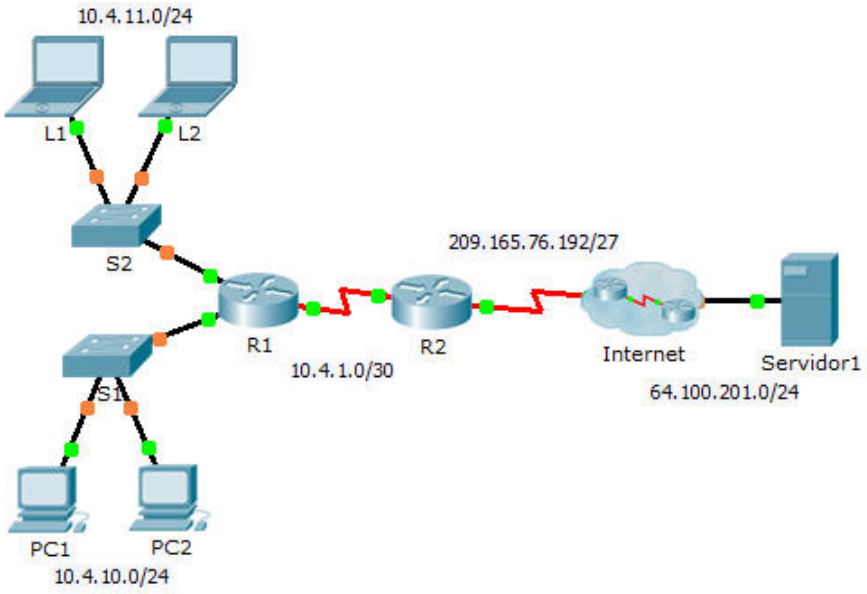


Tabla de direccionamiento

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 problemas

Parte 2: Resolver problemas de configuración de NAT

Parte 3: Verificar conectividad

Situación

Un contratista restauró una antigua configuración en un nuevo router que ejecuta NAT. Pero la red se ha cambiado y se agregó una nueva subred después de hacer una copia de seguridad de la antigua configuración. Su trabajo es hacer que la red funcione nuevamente.

Parte 1: Aislar los problemas

Hacer 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 está funcionando, debería haber entradas de tabla.

Paso 2: Mostrar la configuración en ejecución en el R2.

El puerto interno de NAT debe alinearse con la dirección privada, mientras que el puerto externo de NAT 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: Hacer 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 está funcionando, 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 access-list 101 y reemplácela por una lista similar que también tenga la longitud de 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 **Server1**, al **R1** y al **R2**. Resuelva los problemas si los mensajes ping no son correctos.

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

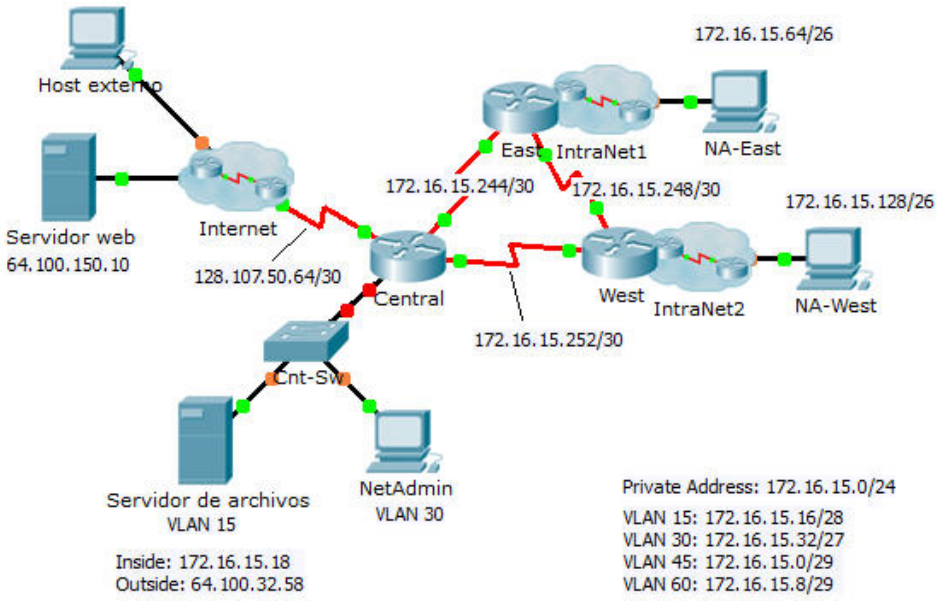


Tabla de direccionamiento

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]]	N/A
	G0/0.30	[[R1G0sub30Add]]	[[R1G0sub30SM]]	N/A
	G0/0.45	[[R1G0sub45Add]]	[[R1G0sub45SM]]	N/A
	G0/0.60	[[R1G0sub60Add]]	[[R1G0sub60SM]]	N/A
	S0/0/0	[[R1S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R1S001Add]]	255.255.255.252	N/A
	S0/1/0	[[R1S010Add]]	255.255.255.252	N/A
[[R2Name]]	G0/0	[[R2G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R2S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R2S001Add]]	255.255.255.252	N/A
[[R3Name]]	G0/0	[[R3G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R3S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R3S001Add]]	255.255.255.252	N/A
[[S1Name]]	VLAN 60	[[S1VLAN60Add]]	[[R1G0sub60SM]]	[[R1G0sub60Add]]
[[PC1Name]]	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

Tabla de asignaciones de VLAN y de puertos

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

Situación

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

Documentación

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

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

Implementación

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

Implemente los siguientes requisitos mediante su documentación:

[[S1Name]]

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

[[R1Name]]

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

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

  [[NATPoolText]]

[[PC1Name]]

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

Verificación

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

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

Documentación de resolución de problemas

Problema	Solución

Rúbrica de calificación sugerida

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

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

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



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



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

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

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



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



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

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

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



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



```
1024

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


Packet Tracer: Configuración de VPN (optativo) (versión para el instructor)

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

Topología

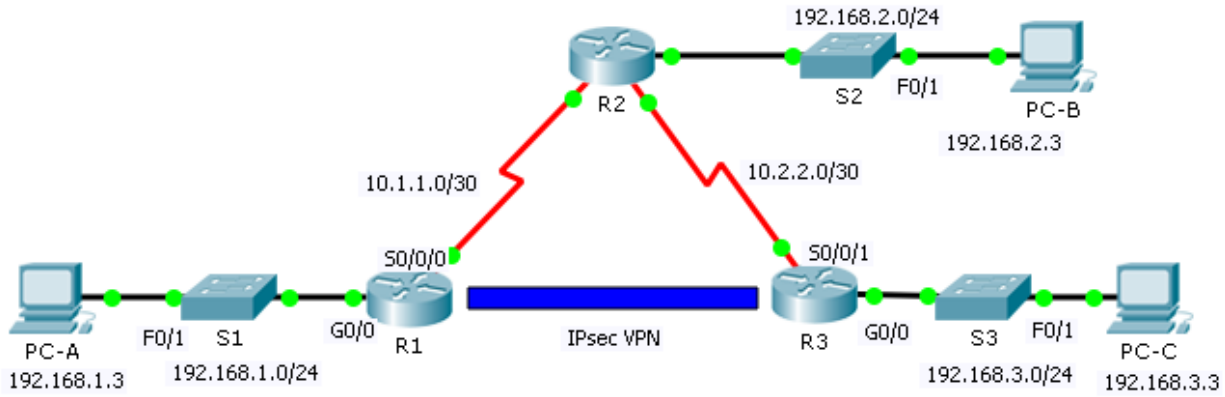


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Parámetros de política de fase 1 de ISAKMP

Parámetros		R1	R3
Método de distribución de claves	Manual o **ISAKMP**	ISAKMP	ISAKMP
Algoritmo de cifrado	**DES**, 3DES o AES	AES	AES
Algoritmo hash	MD5 o **SHA-1**	SHA-1	SHA-1
Método de autenticación	Claves previamente compartidas o **RSA**	Previamente compartidas	Previamente compartidas
Intercambio de claves	Grupo DH **1**, 2 o 5	DH 2	DH 2
Vida útil de SA IKE	86 400 segundos o menos	86400	86400
ISAKMP Key (Llave USB)		cisco	cisco

Los parámetros **en negrita** son valores predeterminados. Los demás parámetros se deben configurar explícitamente.

Parámetros de política de fase 2 de IPsec

Parámetros	R1	R3
Conjunto de transformaciones	VPN-SET	VPN-SET
Nombre de host del peer	R3	R1
Dirección IP del peer	10.2.2.2	10.1.1.2
Red para cifrar	192.168.1.0/24	192.168.3.0/24
Nombre de la asignación criptográfica	VPN-MAP	VPN-MAP
Establecimiento de SA	ipsec-isakmp	ipsec-isakmp

Objetivos

Parte 1: Habilitar las características de seguridad

Parte 2: Configurar los parámetros de IPsec en el R1

Parte 3: Configurar los parámetros de IPsec en el R3

Parte 4: Verificar la VPN con IPsec

Situación

En esta actividad, configurará dos routers para admitir una VPN con IPsec de sitio a sitio para el tráfico que fluye de sus respectivas LAN. El tráfico de la VPN con IPsec pasa a través de otro router que no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de la información confidencial a través de redes sin protección, como Internet. IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes (peers), como los routers Cisco.

Parte 1: Habilitar las características de seguridad

Paso 1: Activar el módulo securityk9.

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad.

Nota: la contraseña de los modos EXEC del usuario y EXEC privilegiado es **cisco**.

a. Emita el comando **show version** en el modo EXEC del usuario o EXEC privilegiado para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. De lo contrario, active el módulo **securityk9** para el siguiente arranque del router, acepte la licencia, guarde la configuración y reinicie.

```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. Una vez finalizada la recarga, vuelva a emitir el comando **show version** para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Repita los pasos 1a a 1c con el **R3**.

Parte 2: Configurar los parámetros de IPsec en el R1

Paso 1: Probar la conectividad.

Haga ping de la **PC-A** a la **PC-C**.

Paso 2: Identificar el tráfico interesante en el R1.

Configure la ACL 110 para identificar como interesante el tráfico proveniente de la LAN en el **R1** a la LAN en el **R3**. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN de los routers **R1** y **R3**. El resto del tráfico que se origina en las LAN no se cifra. Recuerde que debido a la instrucción implícita deny any, no hay necesidad de agregar dicha instrucción a la lista.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Paso 3: Configurar las propiedades de la fase 1 de ISAKMP en el R1.

Configure las propiedades de la política criptográfica ISAKMP **10** en el **R1** junto con la clave criptográfica compartida **cisco**. Consulte la tabla de la fase 1 de ISAKMP para ver los parámetros específicos que se deben configurar. No es necesario que se configuren los valores predeterminados, por lo que solo se deben configurar el cifrado, el método de intercambio de claves y el método DH.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Paso 4: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

Cree el conjunto de transformaciones **VPN-SET** para usar **esp-3des** y **esp-sha-hmac**. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Paso 5: Configurar la asignación criptográfica en la interfaz de salida.

Por último, vincule la asignación criptográfica **VPN-MAP** a la interfaz de salida Serial 0/0/0. **Nota:** esta actividad no se califica.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Parte 3: Configurar los parámetros de IPsec en el R3

Paso 1: Configurar el router R3 para admitir una VPN de sitio a sitio con el R1.

Ahora configure los parámetros recíprocos en el **R3**. Configure la ACL **110** para identificar como interesante el tráfico proveniente de la LAN en el **R3** a la LAN en el **R1**.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```


Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R3.

Configure las propiedades de la política criptográfica ISAKMP **10** en el **R3** junto con la clave criptográfica compartida **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

Como hizo en el **R1**, cree el conjunto de transformaciones **VPN-SET** para usar **esp-3des** y **esp-sha-hmac**. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Paso 4: Configurar la asignación criptográfica en la interfaz de salida.

Por último, vincule la asignación criptográfica **VPN-MAP** a la interfaz de salida Serial 0/0/1. **Nota:** esta actividad no se califica.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Parte 4: Verificar la VPN con IPsec

Paso 1: Verificar el túnel antes del tráfico interesante.

Emita el comando **show crypto ipsec sa** en el **R1**. Observe que la cantidad de paquetes encapsulados, cifrados, desencapsulados y descifrados se establece en 0.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```



```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
      path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
      current outbound spi: 0x0(0)
<resultado omitido>
```

Paso 2: Crear el tráfico interesante.

Haga ping de la **PC-A** a la **PC-C**.

Paso 3: Verificar el túnel después del tráfico interesante.

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Ahora observe que la cantidad de paquetes es superior a 0, lo que indica que el túnel VPN con IPsec funciona.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<resultado omitido>
```

Paso 4: Crear el tráfico no interesante.

Haga ping de la **PC-A** a la **PC-B**.

Paso 5: Verificar el túnel.

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Por último, observe que la cantidad de paquetes no cambió, lo que verifica que el tráfico no interesante no está cifrado.

Secuencias de comandos de configuración

Router R1

```
en
conf t
license boot module c2900 technology-package securityk9
yes
end
copy ru st


reload

en
conf t
service password-encryption
hostname R1
enable secret cisco
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.2.2.2
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN conection to R3
 set peer 10.2.2.2
 set transform-set VPN-SET
 match address 110
ip name-server 0.0.0.0
spanning-tree mode pvst
interface gig0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 no shut
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 clock rate 128000
 crypto map VPN-MAP
 no shut
router eigrp 100
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 no auto-summary
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
banner motd ~
************ AUTHORIZED ACCESS ONLY *************
```



```
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.~
logging trap debugging
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
copy ru st
```

R2 del router

```
en
conf t
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname R2
enable secret cisco
ip name-server 0.0.0.0
spanning-tree mode pvst
interface gig0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 no shut
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shut
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clock rate 128000
 no shut
router eigrp 100
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.2.0
 no auto-summary
banner motd ^C
************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.^C
line con 0
 password 7 cisco
 login
line vty 0 4
 password cisco
 login
```



```
end
copy ru st
end
```

R3 del router

```
en
conf t
license boot module c2900 technology-package securityk9
yes
end
copy ru st


reload

en
conf t
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname R3
enable secret cisco
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.1.1.2
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to R1
 set peer 10.1.1.2
 set transform-set VPN-SET
 match address 110
ip name-server 0.0.0.0
spanning-tree mode pvst
interface gig0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 no shut
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 crypto map VPN-MAP
 no shut
router eigrp 100
 passive-interface FastEthernet0/1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
```



```
ip classless
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
banner motd ~
************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.~
line con 0
 password 7 cisco
 login
line vty 0 4
 password 7 cisco
 login
end
copy ru st
```


Packet Tracer: Configuración de GRE (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

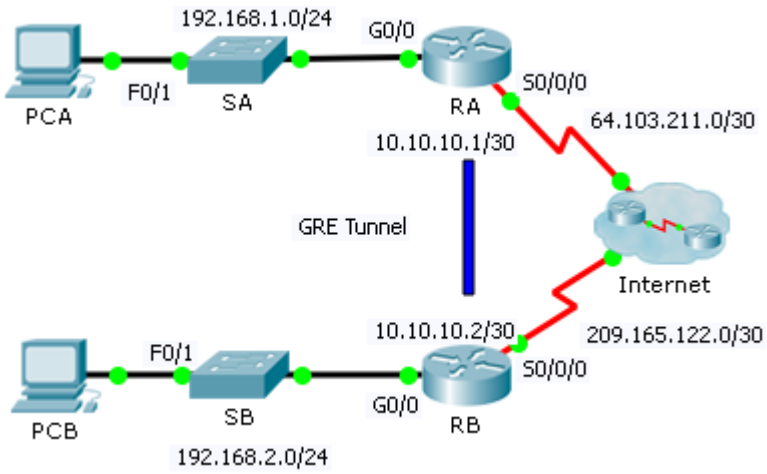


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RA	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.1	255.255.255.252	N/A
RB	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Objetivos

Parte 1: Verificar la conectividad de los routers

Parte 2: Configurar los túneles GRE

Parte 3: Verificar la conectividad de las computadoras

Situación

Usted es el administrador de red de una empresa que desea configurar un túnel GRE a una oficina remota. Ambas redes están configuradas localmente y solo necesitan que se configure el túnel.

Paso 1: Verificar la conectividad de los routers

Paso 1: Hacer ping del RB al RA.

a. Use el comando **show ip interface brief** en el **RA** para determinar la dirección IP del puerto S0/0/0.

b. Desde el **RB**, haga ping a la dirección IP S0/0/0 del **RA**.

Paso 2: Haga ping a PCA desde PCB.

Intente hacer ping de la **PCB** a la dirección IP de la **PCA**. Se debe repetir esta prueba después de configurar el túnel GRE. ¿Cuáles fueron los resultados de los pings? ¿Por qué? Los pings fallaron porque no hay ninguna ruta hacia el destino.

Paso 2: Configurar los túneles GRE

Paso 1: Configurar la interfaz Tunnel 0 del RA.

a. Ingrese al modo de configuración del túnel 0 del **RA**.

```
RA(config)# interface tunnel 0
```

b. Establezca la dirección IP como se indica en la tabla de direccionamiento.

```
RA(config-if)# ip address 10.10.10.1 255.255.255.252
```

c. Establezca el origen y el destino para las terminales del túnel 0.

```
RA(config-if)# tunnel source s0/0/0
RA(config-if)# tunnel destination 209.165.122.2
```

d. Configure el túnel 0 para trasmitir el tráfico IP por GRE.

```
RA(config-if)# tunnel mode gre ip
```

e. La interfaz de túnel 0 ya debe estar activa. En caso de que no sea así, trátela como a cualquier otra interfaz.

```
RA(config-if)# no shutdown
```

Paso 2: Configurar la interfaz Tunnel 0 del RB.

Repita los pasos 1a a 1e con el **RB**. Asegúrese de cambiar el direccionamiento IP según corresponda.

```
RB(config)# interface tunnel 0
RB(config-if)# ip address 10.10.10.2 255.255.255.252
RB(config-if)# tunnel source s0/0/0
RB(config-if)# tunnel destination 64.103.211.2
RB(config-if)# tunnel mode gre ip
RB(config-if)# no shutdown
```

Paso 3: Configurar una ruta para el tráfico IP privado.

Establezca una ruta entre las redes 192.168.X.X con la red 10.10.10.0/30 como destino.

```
RA(config)# ip route 192.168.2.0 255.255.255.0 10.10.10.2
RB(config)# ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

Paso 3: Verificar la conectividad de los routers

Paso 1: Haga ping a PCA desde PCB.

Intente hacer ping de la **PCB** a la dirección IP de la **PCA**. El ping debería realizarse correctamente.

Paso 2: Rastrear la ruta de la PCA a la PCB.

Intente rastrear la ruta de la **PCA** a la **PCB**. Observe la falta de direcciones IP públicas en el resultado.

Configuraciones de dispositivos

RA del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname RA
license udi pid CISCO2911/K9 sn FTX15242579
spanning-tree mode pvst
interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 209.165.122.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 64.103.211.2 255.255.255.252
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 192.168.2.0 255.255.255.0 10.10.10.2
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
line con 0
```

```
line aux 0
line vty 0 4
 login
end
```

RB del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
license udi pid CISCO2911/K9 sn FTX152497Z4
spanning-tree mode pvst
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 64.103.211.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 209.165.122.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
line con 0
line aux 0
line vty 0 4
 login
end
```

Packet Tracer: Resolución de problemas de GRE (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

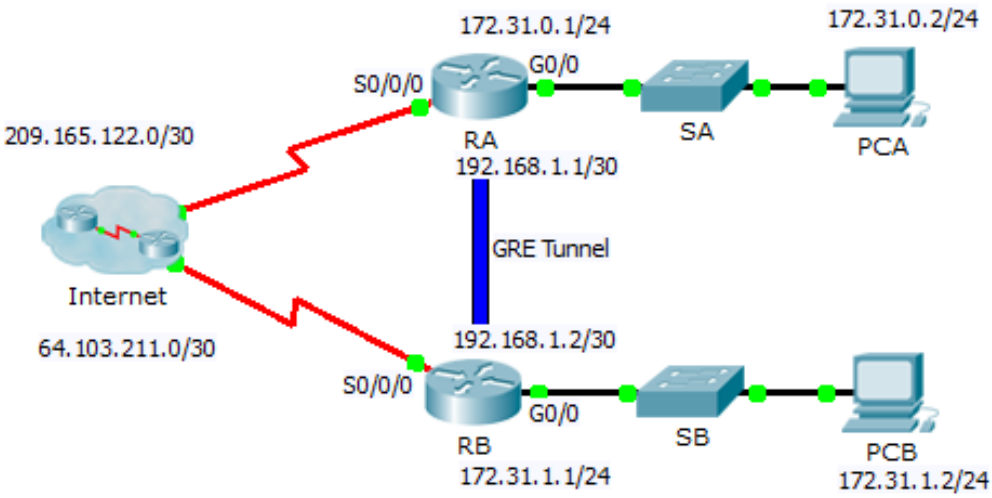


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RA	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.1	255.255.255.252	N/A
RB	G0/0	172.31.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.2	255.255.255.252	N/A
PC-A	NIC	172.31.0.2	255.255.255.0	172.31.0.1
PC-C	NIC	172.31.1.2	255.255.255.0	172.31.1.1

Objetivos

- Identificar y corregir todos los errores de red.
- Verificar la conectividad

Situación

Se contrató a un administrador de red principiante para configurar un túnel GRE entre dos sitios, pero no pudo completar la tarea. Se le solicita a usted corregir los errores de configuración en la red de la empresa.

Parte 1: Identificar y corregir todos los errores de red

Dispositivo	Error	Corrección
RA	La interfaz IP G0/0 y la máscara de subred no son correctas. Se debe eliminar la dirección de túnel para prevenir errores de superposición.	interface Tunnel 0 no ip address interface g0/0 ip address 172.31.0.1 255.255.255.0
RA	La dirección IP de T0 no es correcta.	interface Tunnel 0 ip address 192.168.1.1 255.255.255.252
RA	La ruta estática no es correcta.	no ip route 172.31.1.0 255.255.255.0 64.103.211.2 ip route 172.31.1.0 255.255.255.0 192.168.1.2
RB	La dirección de destino del túnel no es correcta.	tunnel destination 209.165.122.2
RB	El puerto de origen del túnel no es correcto.	tunnel source Serial0/0/0

Parte 2: Verificar la conectividad

Paso 1: Haga ping a PCA desde PCB.

Intente hacer ping de la **PCB** a la dirección IP de la **PCA**. El ping debería realizarse correctamente.

Paso 2: Rastrear la ruta de la PCA a la PCB.

Intente rastrear la ruta de la **PCA** a la **PCB**. Observe la falta de direcciones IP públicas en el resultado.

Configuraciones de dispositivos

RA del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname RA
interface Tunnel0
 ip address 192.168.1.1 255.255.255.252
```



```
 tunnel source Serial0/0/0
 tunnel destination 64.103.211.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 172.31.0.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 209.165.122.2 255.255.255.252
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 172.31.1.0 255.255.255.0 192.168.1.2
line con 0
line aux 0
line vty 0 4
 login
end
```

RB del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname RB
interface Tunnel0
 ip address 192.168.1.2 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 209.165.122.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 172.31.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
```

```
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 64.103.211.2 255.255.255.252
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 172.31.0.0 255.255.255.0 192.168.1.1
line con 0
line aux 0
line vty 0 4
 login
end
```

Packet Tracer: Configuración de GRE por IPsec (optativo) (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

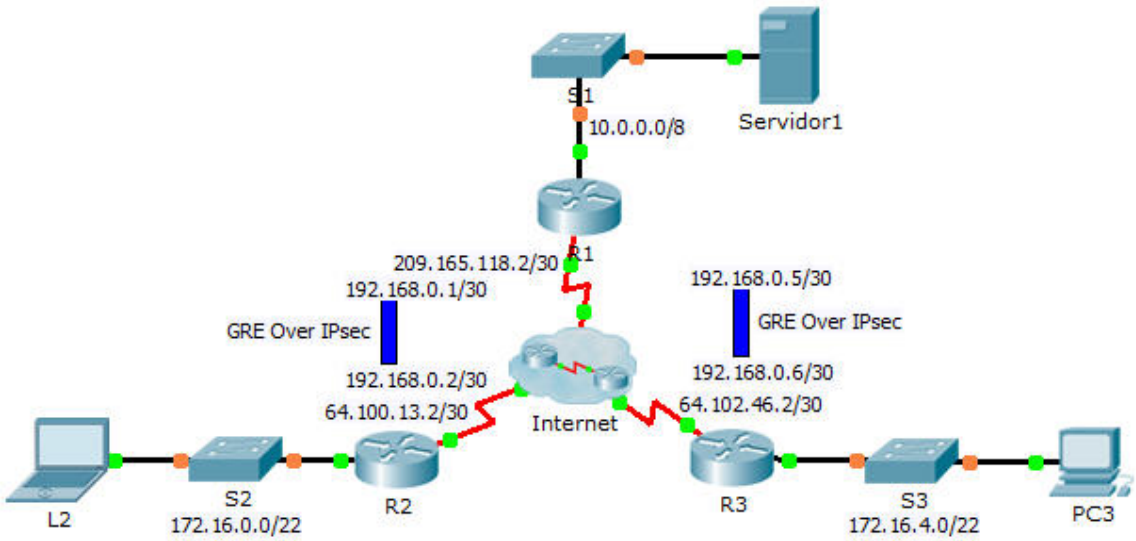


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	S0/0/0	209.165.118.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.1	255.255.255.252	N/A
	Tunnel 1	192.168.0.5	255.255.255.252	N/A
R2	G0/0	172.16.0.1	255.255.252.0	N/A
	S0/0/0	64.100.13.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.2	255.255.255.252	N/A
R3	G0/0	172.16.4.1	255.255.252.0	N/A
	S0/0/0	64.102.46.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.6	255.255.255.252	N/A
Server1	NIC	10.0.0.2	255.0.0.0	10.0.0.1
L2	NIC	172.16.0.2	255.255.252.0	172.16.0.1
PC3	NIC	172.16.4.2	255.255.252.0	172.16.4.1

Objetivos

Parte 1: Verificar la conectividad de los routers

Parte 2: Habilitar las características de seguridad

Parte 3: Configurar los parámetros de IPsec

Parte 4: Configurar los túneles GRE por IPsec

Parte 5: verificar conectividad

Situación

Usted es el administrador de red de una empresa que desea configurar un túnel GRE por IPsec a una oficina remota. Todas las redes están configuradas localmente y solo necesitan que se configure el túnel y el cifrado.

Parte 1: Verificar la conectividad de los routers

Paso 1: Hacer ping del R1 al R2 y el R3.

a. Desde el **R1**, haga ping a la dirección IP de S0/0/0 en el **R2**.

b. Desde el **R1**, haga ping a la dirección IP de S0/0/0 en el **R3**.

Paso 2: Hacer ping de la L2 y la PC3 al Server1.

Intente hacer ping de la **L2** a la dirección IP del **Server1**. Se debe repetir esta prueba después de configurar el túnel GRE por IPsec. ¿Cuáles fueron los resultados de los pings? ¿Por qué? Los pings fallaron porque no hay ninguna ruta hacia el destino.

Paso 3: Hacer ping de la L2 a la PC3.

Intente hacer ping de la **L2** a la dirección IP de la **PC3**. Se debe repetir esta prueba después de configurar el túnel GRE por IPsec. ¿Cuáles fueron los resultados de los pings? ¿Por qué? Los pings fallaron porque no hay ninguna ruta hacia el destino.

Parte 2: Habilitar las características de seguridad

Paso 1: Activar el módulo securityk9.

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad.

a. Emita el comando **show version** en el modo EXEC del usuario o EXEC privilegiado para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. De lo contrario, active el módulo **securityk9** para el siguiente arranque del router, acepte la licencia, guarde la configuración y reinicie.

```
R1(config)# license boot module c2900 technology-package securityk9
<Accept the License>
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. Una vez finalizada la recarga, vuelva a emitir el comando **show version** para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Repita los pasos 1a a 1c con el **R2** y el **R3**.

Parte 3: Configurar los parámetros de IPsec

Paso 1: Identificar el tráfico interesante en el R1.

a. Configure la ACL 102 para identificar como interesante el tráfico proveniente de la LAN en el **R1** a la LAN en el **R2**. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN del **R1** y el **R2**. El resto del tráfico que se origina en las LAN no se cifra. Recuerde que debido a la instrucción implícita deny any, no hay necesidad de agregar dicha instrucción a la lista.

```
R1(config)# access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0
0.0.3.255
```

b. Repita el paso 1a para configurar la ACL 103 a fin de identificar como interesante el tráfico en la LAN del R3.

```
R1(config)# access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0
0.0.3.255
```

Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R1.

a. Configure las propiedades de la política criptográfica ISAKMP **102** en el **R1** junto con la clave criptográfica compartida **cisco**. No es necesario que se configuren los valores predeterminados, por lo que solo se deben configurar el cifrado, el método de intercambio de claves y el método DH.

```
R1(config)# crypto isakmp policy 102
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 64.100.13.2
```

b. Repita el paso 2a para configurar la política 103. Cambie el direccionamiento IP según corresponda.

```
R1(config)# crypto isakmp policy 103
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 64.102.46.2
```

Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

a. Cree el conjunto de transformaciones **VPN-SET** para usar **esp-aes** y **esp-sha-hmac**. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

```
R1(config)# crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R1(config-crypto-map)# set peer 64.100.13.2
R1(config-crypto-map)# set transform-set R1_R2_Set
R1(config-crypto-map)# match address 102
R1(config-crypto-map)# exit
```

b. Repita el paso 3a para configurar R1_R3_Set y R1_R3_Map. Cambie el direccionamiento según corresponda.


```
R1(config)# crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R3_Map 103 ipsec-isakmp
R1(config-crypto-map)# set peer 64.102.46.2
R1(config-crypto-map)# set transform-set R1_R3_Set
R1(config-crypto-map)# match address 103
R1(config-crypto-map)# exit
```

Paso 4: Configurar la asignación criptográfica en la interfaz de salida.

Por último, vincule las asignaciones criptográficas **R1_R2_Map** y **R1_R3_Map** a la interfaz de salida Serial 0/0/0. **Nota:** esta actividad no se califica.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map R1_R2_Map
R1(config-if)# crypto map R1_R3_Map
```

Paso 5: Configurar los parámetros de IPsec en el R2 y el R3.

Repita los pasos 1 a 5 en el **R2** y el **R3**. Use los mismos nombres de ACL, conjunto y asignación que en el **R1**. Tenga en cuenta que cada router solo necesita una conexión cifrada al **R1**. No hay ninguna conexión cifrada entre el **R2** y el **R3**.

```
R2(config)# access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0
0.255.255.255
R2(config)# crypto isakmp policy 102
R2(config-isakmp)# encryption aes
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 5
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco address 209.165.118.2
R2(config)# crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
R2(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R2(config-crypto-map)# set peer 209.165.118.2
R2(config-crypto-map)# set transform-set R1_R2_Set
R2(config-crypto-map)# match address 102
R2(config-crypto-map)# exit
R2(config-if)# interface s0/0/0
R2(config-if)# crypto map R1_R2_Map
```

```
R3(config)# access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0
0.255.255.255
R3(config)# crypto isakmp policy 103
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 209.165.118.2
R3(config)# crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
R3(config)# crypto  map R1_R3_Map 103 ipsec-isakmp
```



```
R3(config-crypto-map)# set peer 209.165.118.2
R3(config-crypto-map)# set transform-set R1_R3_Set
R3(config-crypto-map)# match address 103
R3(config-crypto-map)# exit
R3(config)# interface s0/0/0
R3(config-if)# crypto map R1_R3_Map
```

Parte 4: Configurar los túneles GRE por IPsec

Paso 1: Configurar las interfaces de túnel del R1.

a. Ingrese al modo de configuración del túnel 0 del **R1**.

```
R1(config)# interface tunnel 0
```

b. Establezca la dirección IP como se indica en la tabla de direccionamiento.

```
R1(config-if)# ip address 192.168.0.1 255.255.255.252
```

c. Establezca el origen y el destino para las terminales del túnel 0.

```
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 64.100.13.2
```

d. Configure el túnel 0 para trasmitir el tráfico IP por GRE.

```
R1(config-if)# tunnel mode gre ip
```

e. La interfaz de túnel 0 ya debe estar activa. En caso de que no sea así, trátela como a cualquier otra interfaz.

f. Repita los pasos 1a a 1f para crear la interfaz de túnel 1 al R3. Cambie el direccionamiento según corresponda.

```
R1(config)# interface tunnel 1
R1(config-if)# ip address 192.168.0.5 255.255.255.252
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 64.102.46.2
R1(config-if)# tunnel mode gre ip
```

Paso 2: Configurar la interfaz Tunnel 0 del R2 y el R3.

a. Repita los pasos 1a a 1e con el **R2**. Asegúrese de cambiar el direccionamiento IP según corresponda.

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 192.168.0.2 255.255.255.252
R2(config-if)# tunnel source s0/0/0
R2(config-if)# tunnel destination 209.165.118.2
R2(config-if)# tunnel mode gre ip
```

b. Repita los pasos 1a a 1e con el **R3**. Asegúrese de cambiar el direccionamiento IP según corresponda.

```
R3(config)# interface tunnel 0
R3(config-if)# ip address 192.168.0.6 255.255.255.252
R3(config-if)# tunnel source s0/0/0
R3(config-if)# tunnel destination 209.165.118.2
R3(config-if)# tunnel mode gre ip
```


Paso 3: Configurar una ruta para el tráfico IP privado.

a. Defina una ruta del **R1** a las redes 172.16.0.0 y 172.16.4.0 con la dirección de siguiente salto de la interfaz de túnel.

```
R1(config)# ip route 172.16.0.0 255.255.252.0 192.168.0.2
R1(config)# ip route 172.16.4.0 255.255.252.0 192.168.0.6
```

b. Defina una ruta del **R2** y el **R3** a la red 10.0.0.0 con la dirección de siguiente salto de la interfaz de túnel.

```
R2(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.1
R3(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.5
```

Parte 5: Verificar la conectividad

Paso 1: Hacer ping de la L2 y la PC3 al Server1.

a. Intente hacer ping de la **L2** y la **PC3** a la dirección IP del **Server1**. El ping debería realizarse correctamente.

b. Intente hacer ping de la **PC3** a la dirección IP de la **L2**. El ping debe fallar, porque no hay ningún túnel entre las dos redes.

Secuencias de comandos de configuración

Router R1

```
license boot module c2900 technology-package securityk9
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255
crypto isakmp policy 102
 encryption aes
 authentication pre-share
 group 5
 exit
crypto isakmp key cisco address 64.100.13.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set R1_R2_Set
 match address 102
interface S0/0/0
 crypto map  R1_R2_Map
access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255
crypto isakmp policy 103
 encryption aes
 authentication pre-share
 group 5
 exit
crypto isakmp key cisco address 64.102.46.2
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R3_Map 103 ipsec-isakmp
 set peer 64.102.46.2
 set transform-set R1_R3_Set
 match address 103
```



```
interface S0/0/0
 crypto map R1_R3_Map
interface Tunnel 0
 ip address 192.168.0.1 255.255.255.252
 tunnel source serial 0/0/0
 tunnel destination 64.100.13.2
 tunnel mode gre ip
ip route 172.16.0.0 255.255.252.0 192.168.0.2
interface Tunnel 1
 ip address 192.168.0.5 255.255.255.252
 tunnel source serial 0/0/0
 tunnel destination 64.102.46.2
 tunnel mode gre ip
ip route 172.16.4.0 255.255.252.0 192.168.0.6
```

R2 del router

```
license boot module c2900 technology-package securityk9
access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255
crypto isakmp policy 102
 encryption aes
 authentication pre-share
 group 5
 exit
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
 set peer 209.165.118.2
 set transform-set R1_R2_Set
 match address 102
interface Serial0/0/0
 crypto map R1_R2_Map
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 209.165.118.2
 tunnel mode gre ip
ip route 10.0.0.0 255.0.0.0 192.168.0.1
```

R3 del router

```
license boot module c2900 technology-package securityk9
access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255
crypto isakmp policy 103
 encryption aes
 authentication pre-share
 group 5
 exit
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
```

```
crypto map R1_R3_Map 103 ipsec-isakmp
 set peer 209.165.118.2
 set transform-set R1_R3_Set
 match address 103
interface S0/0/0
 crypto map  R1_R3_Map
interface Tunnel 0
 ip address 192.168.0.6 255.255.255.252
 tunnel source serial 0/0/0
 tunnel destination 209.165.118.2
 tunnel mode gre ip
ip route 10.0.0.0 255.0.0.0 192.168.0.5
```

Configuraciones de dispositivos

Router R1

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
crypto isakmp policy 102
 encr aes
 authentication pre-share
 group 5
crypto isakmp policy 103
 encr aes
 authentication pre-share
 group 5
crypto isakmp key cisco address 64.100.13.2
crypto isakmp key cisco address 64.102.46.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set R1_R2_Set
 match address 102
crypto map R1_R3_Map 103 ipsec-isakmp
 set peer 64.102.46.2
 set transform-set R1_R3_Set
 match address 103
license udi pid CISCO2911/K9 sn FTX15241LLM
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 64.100.13.2
 tunnel mode gre ip
interface Tunnel1
```



```
 ip address 192.168.0.5 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 64.102.46.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 209.165.118.2 255.255.255.252
 crypto map R1_R3_Map
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 172.16.0.0 255.255.252.0 192.168.0.2
ip route 172.16.4.0 255.255.252.0 192.168.0.6
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255
access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255
line con 0
line aux 0
line vty 0 4
 login
end
```

R2 del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
crypto isakmp policy 102
 encr aes
 authentication pre-share
 group 5
crypto isakmp key cisco address 209.165.118.2
```



```
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
 set peer 209.165.118.2
 set transform-set R1_R2_Set
 match address 102
license udi pid CISCO2911/K9 sn FTX15249J0B
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 209.165.118.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 172.16.0.1 255.255.252.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 64.100.13.2 255.255.255.252
 crypto map R1_R2_Map
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 10.0.0.0 255.0.0.0 192.168.0.1
access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255
line con 0
line aux 0
line vty 0 4
 login
end
```

R3 del router

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
```



```
no service password-encryption
hostname R3
crypto isakmp policy 103
 encr aes
 authentication pre-share
 group 5
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R3_Map 103 ipsec-isakmp
 set peer 209.165.118.2
 set transform-set R1_R3_Set
 match address 103
license udi pid CISCO2911/K9 sn FTX1524446J
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
 ip address 192.168.0.6 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 209.165.118.2
 tunnel mode gre ip
interface GigabitEthernet0/0
 ip address 172.16.4.1 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 64.102.46.2 255.255.255.252
 crypto map R1_R3_Map
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 10.0.0.0 255.0.0.0 192.168.0.5
access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255
line con 0
line aux 0
```



```
line vty 0 4
 login
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

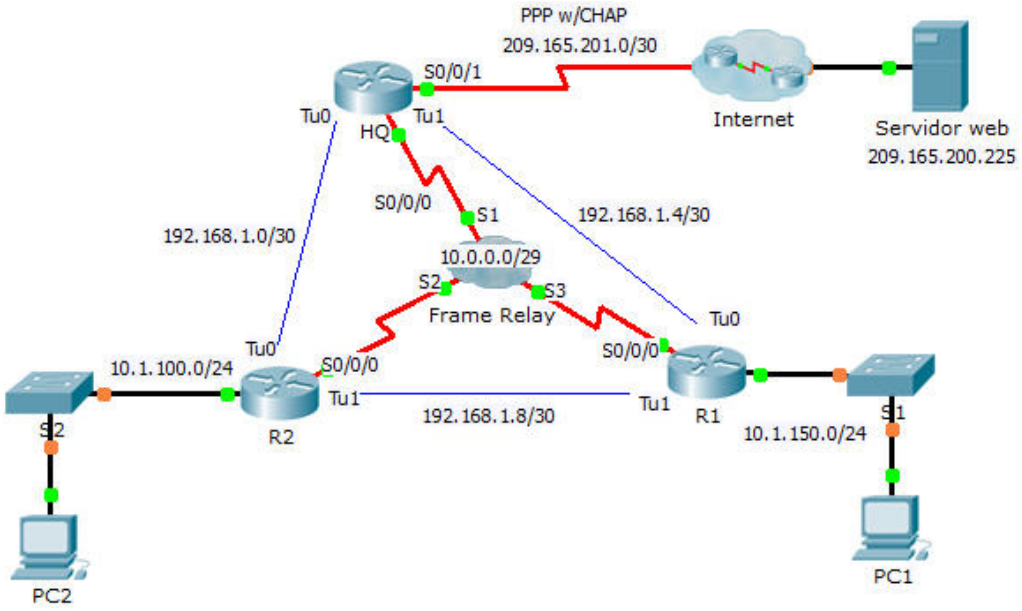


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
HQ	S0/0/0	10.0.0.1	255.255.255.248	N/A
	S0/0/1	209.165.201.2	255.255.255.252	N/A
	Tu0	192.168.1.1	255.255.255.252	N/A
	Tu1	192.168.1.5	255.255.255.252	N/A
R1	G0/0	10.1.150.1	255.255.255.0	N/A
	S0/0/0	10.0.0.3	255.255.255.248	N/A
	Tu0	192.168.1.6	255.255.255.252	N/A
	Tu1	192.168.1.9	255.255.255.252	N/A
R2	G0/0	10.1.100.1	255.255.255.0	N/A
	S0/0/0	10.0.0.2	255.255.255.248	N/A
	Tu0	192.168.1.2	255.255.255.252	N/A
	Tu1	162.168.1.10	255.255.255.252	N/A
Web	NIC	209.165.200.226	255.255.255.252	209.165.200.225
PC1	NIC	10.1.150.10	255.255.255.0	10.1.150.1
PC2	NIC	10.1.100.10	255.255.255.0	10.1.100.1

Asignaciones de DLCI

De/Para	HQ	R1	R2
HQ	-	103	102
R1	301	-	302
R2	201	203	-

Información básica

Esta actividad le permite poner en práctica una variedad de habilidades, incluida la configuración de Frame Relay, PPP con CHAP, NAT con sobrecarga (PAT) y túneles GRE. Los routers están parcialmente configurados.

Requisitos

Nota: usted solo tiene acceso a la consola del router R1 y acceso por Telnet al router HQ. El nombre de usuario es **admin** y la contraseña es **adminpass** para el acceso mediante Telnet.

R1

- Configure Frame Relay de malla completa.
  - Configure la encapsulación de Frame Relay.
  - Configure un mapa a cada uno de los demás routers.

  - El tipo de LMI es ANSI.
- Configurar túneles GRE a los otros routers.
  - Configurar el puerto de origen y la dirección de destino.
  - Configurar la dirección IP de la interfaz de túnel según la **tabla de direccionamiento**.

HQ

- Configurar **HQ** para usar PPP con CHAP en el enlace a Internet. **ISP** es el nombre de host del router. La contraseña para CHAP es **cisco**.
- Configurar túneles GRE a los otros routers.
  - Configurar el puerto de origen y la dirección de destino.
  - Configurar la dirección IP de la interfaz de túnel según la **tabla de direccionamiento**.
- Configurar NAT para compartir la dirección IP pública con todo el rango privado de clase A.
  - Configure la lista de acceso 1 para utilizarla con NAT.
  - Identifique las interfaces internas y externas.

Verificar la conectividad de extremo a extremo

- Ahora, todas las terminales deben poder hacer ping entre sí y al **servidor web**.
- Si esto no ocurre, haga clic en **Check Results** (Verificar resultados) para ver qué configuración falta. Implemente las correcciones necesarias y vuelva a realizar la prueba para verificar la plena conectividad de extremo a extremo.

Configuraciones de dispositivos

Router R1

```
enable
configure terminal
interface s0/0/0
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 301 broadcast
 frame-relay map ip 10.0.0.2 302 broadcast
 frame-relay lmi-type ansi
interface tunnel 0
 ip address 192.168.1.6 255.255.255.252
 tunnel source s0/0/0
 tunnel destination 10.0.0.1
interface tunnel 1
 ip address 192.168.1.9 255.255.255.252
 tunnel source s0/0/0
 tunnel destination 10.0.0.2
end
copy running-config startup-config
```

HQ del router

```
enable
configure terminal
username ISP password cisco
```

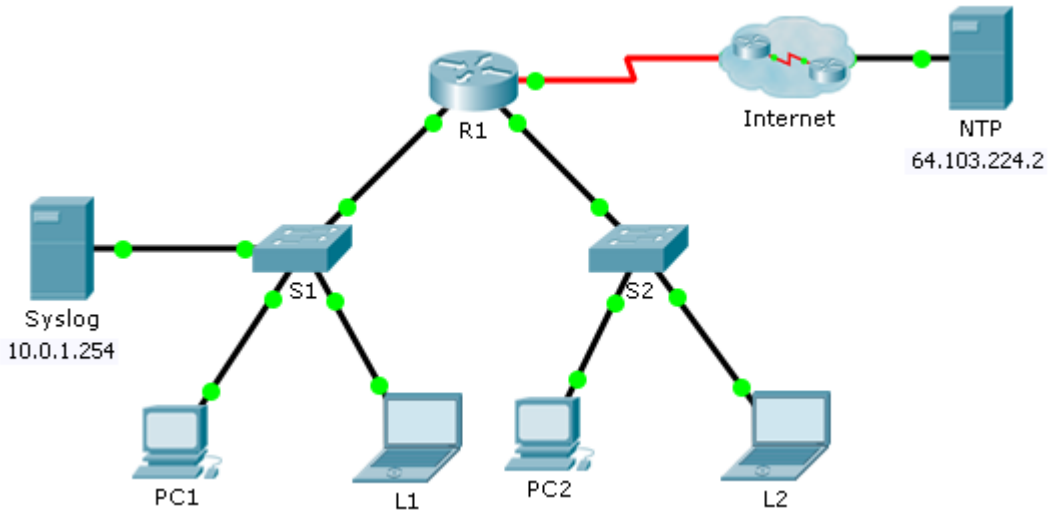


```
interface s0/0/0
 ip nat inside
interface s0/0/1
 encapsulation ppp
 ppp authentication chap
 ip nat outside
interface tunnel 0
 ip address 192.168.1.1 255.255.255.252
 tunnel source s0/0/0
 tunnel destination 10.0.0.2
interface tunnel 1
 ip address 192.168.1.5 255.255.255.252
 tunnel source s0/0/0
 tunnel destination 10.0.0.3
ip nat inside source list 1 interface s0/0/1 overload
access-list 1 permit 10.0.0.0 0.255.255.255
end
copy running-config startup-config
```

Packet Tracer: Configuración de syslog y NTP (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 el servicio de syslog

Parte 2: Generar eventos registrados

Parte 3: Establecer manualmente los relojes de los switches

Parte 4: Configurar el servicio NTP

Parte 5: Verificar los registros con marca de hora

Situación

En esta actividad, habilitará y usará los servicios de syslog y NTP para que el administrador de red pueda monitorear la red de forma más eficaz.

Parte 1: Configurar el servicio de syslog

Paso 1: Habilitar el servicio de syslog.

a. Haga clic en **Syslog** y, a continuación, en la ficha **Config**.

b. Active el servicio de **syslog** y mueva la ventana para poder monitorear la actividad.

Paso 2: Configurar los dispositivos intermediarios para que utilicen el servicio de syslog.

a. Configure el **R1** para enviar eventos de registro al servidor de **Syslog**.

```
R1(config)# logging 10.0.1.254
```

b. Configure el **S1**y el **S2** para enviar eventos de registro al servidor de **Syslog**.

```
S1(config)# logging 10.0.1.254
```

c. Configure el **S2** para enviar eventos de registro a la dirección IP del servidor de **Syslog**.

```
S2(config)# logging 10.0.1.254
```

Parte 2: Generar eventos registrados

Paso 1: Cambiar el estado de las interfaces para crear registros de eventos.

a. Configure una interfaz Loopback 0 en **R1** y, a continuación, deshabilítela.

```
R1(config)# interface loopback 0
R1(config-if)# shutdown
```

b. Apague la **PC1** y la **PC2**. Vuelva a prenderlas.

Paso 2: Analizar los eventos de syslog.

a. Observe los eventos de syslog. **Nota:** se registraron todos los eventos; sin embargo, las marcas de hora son incorrectas.

b. Borre el registro antes de continuar con la parte siguiente.

Parte 3: Establecer manualmente los relojes de los switches

Paso 1: Establecer manualmente los relojes de los switches.

Configure manualmente el reloj en el **S1** y el **S2** con la fecha actual y la hora aproximada. Se proporciona un ejemplo.

```
S1# clock set 11:47:00 July 10 2013
```

Paso 2: Habilitar el servicio de marca de hora de registro en los switches.

Configure el **S1** y el **S2** para enviar la marca de hora con los registros que envían al servidor de **Syslog**.

```
S1(config)# service timestamps log datetime msec
S2(config)# service timestamps log datetime msec
```

Parte 4: Configurar el servicio NTP

Paso 1: Habilitar el servicio NTP.

En esta actividad, se supone que el servicio NTP se aloja en un servidor de Internet pública. Si el servidor NTP fuera privado, también se podría usar la autenticación.

a. Abra la ficha **Config** del servidor **NTP**.

b. Active el servicio NTP y observe la fecha y la hora que se muestran.

Paso 2: Establecer automáticamente el reloj del router.

Configure el reloj en el **R1** según la fecha y la hora del servidor NTP.

```
R1(config)# ntp server 64.103.224.2
```


Paso 3: Habilitar el servicio de marca de hora de registro en el router.

Configure el **R1** para enviar la marca de hora con los registros que envía al servidor de **Syslog**.

```
R1(config)# service timestamps log datetime msec
```

Parte 5: Verificar los registros con marca de hora

Paso 1: Cambiar el estado de las interfaces para crear registros de eventos.

a. Vuelva a habilitar y después deshabilite la interfaz Loopback 0 en R1.

```
R1(config)# interface loopback 0
R1(config-if)# no shutdown
R1(config-if)# shutdown
```

b. Apague las computadoras portátiles **L1** y **L2**. Vuelva a prenderlas.

Paso 2: Analizar los eventos de syslog.

Observe los eventos de syslog. **Nota:** se registraron todos los eventos, y las marcas de hora son correctas como se configuraron. **Nota:** el **R1** usa la configuración de reloj del servidor NTP, y el **S1** y el **S2** usan la configuración de reloj que usted configuró en la parte 3.

Packet Tracer: Desafío de resolución de problemas sobre la documentación 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

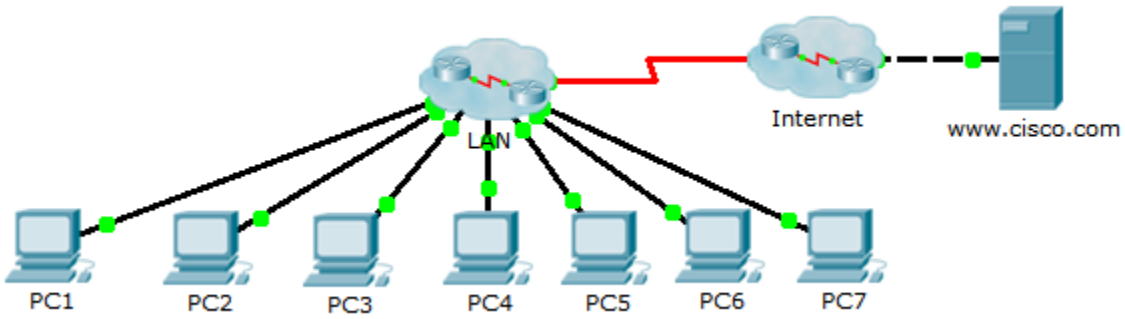


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC1	NIC	10.2.15.10	255.255.255.0	10.2.15.1
PC2	NIC	10.2.25.10	255.255.255.0	10.2.25.1
PC3	NIC	10.2.35.10	255.255.255.0	10.2.35.1
PC4	NIC	10.3.100.4	255.255.255.0	10.3.100.1
PC5	NIC	10.3.100.5	255.255.255.0	10.3.100.1
PC6	NIC	10.4.1.10	255.255.255.0	10.4.1.1
PC7	NIC	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	NIC	10.1.100.2	255.255.255.0	10.1.100.1
R1	S0/0/0	10.1.0.4	255.255.255.248	N/A
R1	G0/0	10.4.1.1	255.255.255.0	N/A
R2	S0/0/0	10.1.0.3	255.255.255.248	N/A
R2	G0/0.100	10.3.100.1	255.255.255.0	N/A
R2	G0/0.105	10.3.105.1	255.255.255.0	N/A
R3	S0/0/0	10.1.0.2	255.255.255.248	N/A
R3	G0/0.5	10.2.5.1	255.255.255.0	N/A
R3	G0/0.15	10.2.15.1	255.255.255.0	N/A
R3	G0/0.25	10.2.25.1	255.255.255.0	N/A
R3	G0/0.35	10.2.35.1	255.255.255.0	N/A
R4	S0/0/0	10.1.0.5	255.255.255.248	N/A
R4	G0/0	10.5.1.1	255.255.255.0	N/A
R5	S0/0/0	10.1.0.1	255.255.255.248	N/A
R5	S0/0/1	209.165.201.2	255.255.255.252	N/A
R5	G0/0	10.1.100.1	255.255.255.0	N/A
S1	None	None	None	None
S2	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
S3	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
S4	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
S5	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
S6	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
S7	None	None	None	None

Objetivos

Parte 1: Probar la conectividad

Parte 2: Detectar la información de configuración de las computadoras

Parte 3: Detectar la información de configuración del gateway predeterminado

Parte 4: Detectar las rutas y los vecinos en la red

Parte 5: Dibujar la topología de la red

Información básica/situación

En esta actividad, se abarcan los pasos que se deben seguir para detectar una red principalmente mediante el uso de los comandos telnet, **show cdp neighbors detail** y **show ip route**. Esta es la parte 1 de una actividad que consta de dos partes. La parte 2 es **Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas**.

La topología que ve cuando abre la actividad de Packet Tracer no muestra todos los detalles de la red. Los detalles se ocultaron mediante la función de clúster de Packet Tracer. La infraestructura de la red se contrajo, y la topología en el archivo muestra solo las terminales. Su tarea consiste en usar sus conocimientos sobre comandos de detección y redes para obtener información acerca de la topología de la red completa y registrarla.

Parte 1: Probar la conectividad

Packet Tracer necesita cierto tiempo para converger la red. Haga ping entre las computadoras y el servidor www.cisco.com para verificar la convergencia y probar la red. Todas las computadoras deben poder hacer ping entre sí y al servidor. Recuerde que es posible que deba realizar varios pings antes de que se realicen correctamente.

Parte 2: Detectar la información de configuración de la computadora

Paso 1: Acceder al símbolo del sistema de la PC1.

Haga clic en **PC1**, ficha **Desktop** (Escritorio) y, a continuación, **Command Prompt** (Símbolo del sistema).

Paso 2: Determinar la información de direccionamiento de la PC1.

Para determinar la configuración de direccionamiento IP actual, introduzca el comando **ipconfig /all**.

Nota: en Packet Tracer, debe introducir un espacio entre **ipconfig** y **/all**.

Paso 3: Registrar la información de la PC1 en la tabla de direccionamiento.

```
PC> ipconfig /all

FastEthernet0 Connection:(default port)
Physical Address.................: 0001.97DA.E057
Link-local IPv6 Address.........: FE80::201:97FF:FEDA:E057
IP Address......................: 10.2.15.10
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 10.2.15.1
DNS Servers.....................: 10.1.100.2
DHCP Servers....................: 0.0.0.0
```


Paso 4: Repetir los pasos 1 a 3 en las PC 2 a 7.

Parte 3: Detectar la información de configuración del gateway predeterminado

Paso 1: Probar la conectividad entre la PC1 y su gateway predeterminado.

Desde la PC1, haga ping al gateway predeterminado para asegurarse de que tiene conectividad.

Paso 2: Acceder al gateway predeterminado mediante telnet.

Use el comando **telnet** *dirección-ip*. La dirección IP es la del gateway predeterminado. Cuando se le solicite la contraseña, escriba **cisco**.

Paso 3: Ver las configuraciones de interfaz actuales.

a. Use los comandos **show ip interface brief** y **show protocols** para determinar la configuración actual de interfaces.

b. Registre la información de máscara de subred a partir del comando **show protocols**.

Paso 4: Registrar el nombre de host y la configuración de la interfaz del router de gateway de la PC1 en la tabla de direccionamiento.

Parte 4: Detectar las rutas y los vecinos en la red

Paso 1: En el router de gateway de la PC1, mostrar la tabla de routing.

a. Muestre la tabla de routing con el comando **show ip route**. Debe ver cinco rutas conectadas y seis rutas descubiertas mediante EIGRP, una de las cuales es una ruta predeterminada.

b. Además de las rutas, registre cualquier otra información útil que proporcione la tabla de routing para ayudarle a continuar con la detección y el registro de la red.

c. Determine si hay más direcciones IP a las que puede acceder mediante Telnet para continuar con la detección de la red.

Paso 2: Detectar los dispositivos Cisco conectados directamente.

En el router de gateway de la PC1, use el comando **show cdp neighbors detail** para detectar otros dispositivos Cisco conectados directamente.

Paso 3: Registrar la información de vecinos y probar la conectividad.

El comando **show cdp neighbors detail** indica la información de un vecino, incluida la dirección IP. Registre el nombre de host y la dirección IP del vecino, y luego haga ping a la dirección IP para probar la conectividad. Los primeros dos o tres pings fallan mientras ARP resuelve la dirección MAC.

Paso 4: Acceder al vecino mediante telnet y detectar los dispositivos Cisco conectados directamente.

a. Acceda al vecino mediante Telnet y use el comando **show cdp neighbors detail** para detectar otros dispositivos Cisco conectados directamente.

b. Esta vez debe ver que se indican tres dispositivos. Es posible que se indique el router de gateway de la PC1 para cada subinterfaz.

Nota: use el comando **show interfaces** en los switches para determinar la información de máscara de subred.

Paso 5: Registrar los nombres de host y las direcciones IP de los vecinos y probar la conectividad.

Registre los nuevos vecinos que detecte y haga ping a estos. Recuerde que los primeros dos o tres pings fallan mientras ARP resuelve las direcciones MAC.

Paso 6: Acceder a cada vecino mediante telnet y revisar si hay dispositivos de Cisco adicionales.

Acceda mediante Telnet a cada uno de los nuevos vecinos que detectó y use el comando **show cdp neighbors detail** para revisar si hay dispositivos de Cisco adicionales. La contraseña de acceso es **cisco**.

Paso 7: Continuar con la detección y la documentación de la red.

Salga de las sesiones de Telnet para volver al router de gateway predeterminado de la PC1. Desde este router, acceda mediante Telnet a otros dispositivos en la red para continuar con la detección y la documentación de la red. Recuerde usar los comandos **show ip route** y **show cdp neighbors** para detectar las direcciones IP que puede usar para Telnet.

Nota: use el comando **show interfaces** en los switches para determinar la información de máscara de subred.

Paso 8: Para descubrir la topología completa de la red, repetir los pasos 1 a 7 según sea necesario.

Parte 5: Dibujar la topología de la red

Paso 1: Dibujar una topología.

Una vez que detectó todos los dispositivos de red y registró sus direcciones, use la información de la tabla de direccionamiento para dibujar una topología.

Sugerencia: hay una nube de Frame Relay en medio de la red.

Paso 2: Conservar este registro.

a. Muestre su diagrama de topología y su tabla de direccionamiento al instructor para que los verifique.

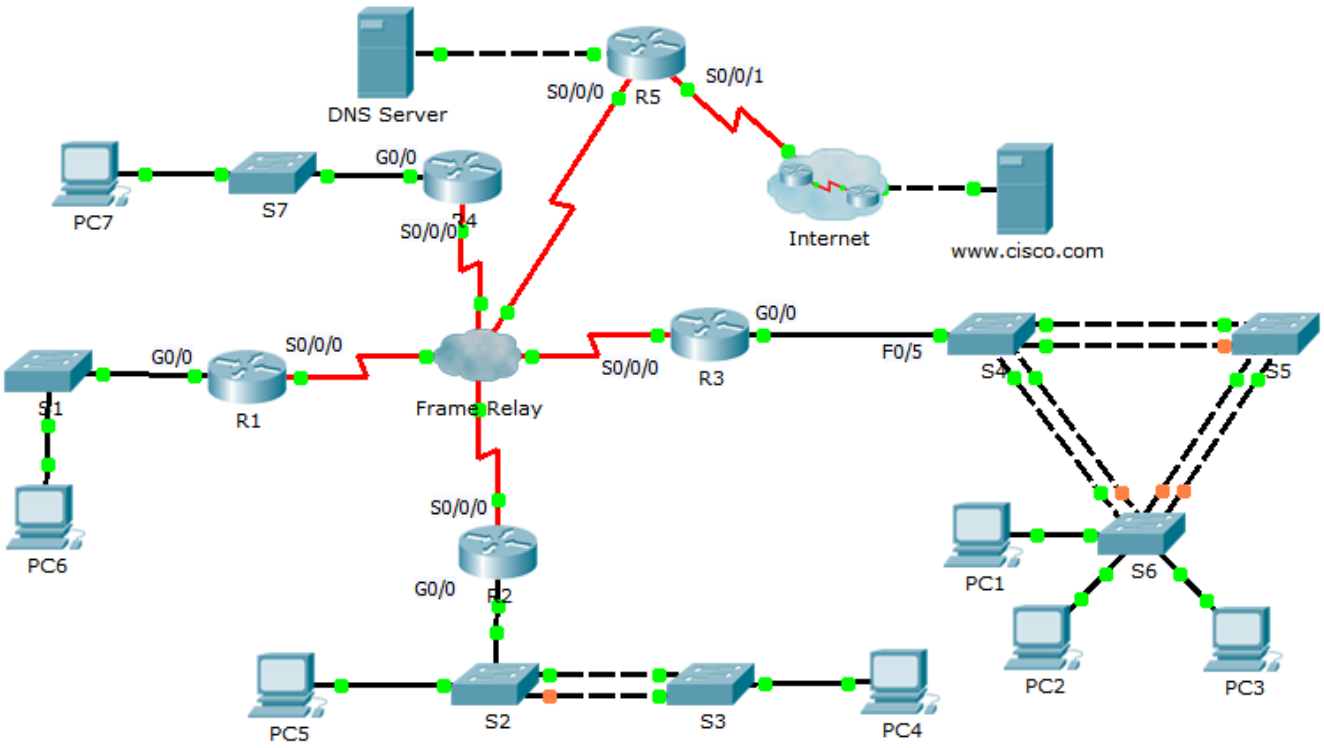
b. Necesitará el diagrama de topología y la tabla de direccionamiento para la parte 2 de esta actividad.

Rúbrica de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 5: Dibujar la topología de la red	Paso 2-a	100	
	Total de la parte 5	100	
	Puntuación de Packet Tracer	**0**	
	Puntuación total	**100**	

Respuesta de topología

Esta topología es una captura de pantalla de la red de respuesta en el archivo PKA. La topología del estudiante puede verse bastante diferente, pero las conexiones deben ser las mismas. Un buen ejercicio para la clase es hacer que los estudiantes comparen los diagramas de topología correctos para considerar los beneficios y las limitaciones de las diferentes disposiciones. Esto también les ayudará a entender que pueden existir numerosas formas excelentes de representar la misma red.



Configuraciones de dispositivos

Router R1

```
R1#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable secret class
```



```
spanning-tree mode pvst
interface Gig0/0
 ip address 10.4.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.4 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
passive-interface Gig0/0
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R2 del router

```
R2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
enable secret class
spanning-tree mode pvst
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.3.100.1 255.255.255.0
interface GigabitEthernet0/0.105
```



```
 encapsulation dot1Q 105 native
 ip address 10.3.105.1 255.255.255.0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.3 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R3 del router

```
R3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R3
enable secret class
spanning-tree mode pvst
interface Gig0/0
 no ip address
 duplex auto
 speed auto
interface Gig0/0.5
 encapsulation dot1Q 5 native
 ip address 10.2.5.1 255.255.255.0
interface Gig0/0.15
 encapsulation dot1Q 15
 ip address 10.2.15.1 255.255.255.0
interface Gig0/0.25
 encapsulation dot1Q 25
```



```
 ip address 10.2.25.1 255.255.255.0
interface Gig0/0.35
 encapsulation dot1Q 35
 ip address 10.2.35.1 255.255.255.0
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R4 del router

```
R4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R4
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.5.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
```



```
 ip address 10.1.0.5 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R5 del router

```
R5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R5
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.1.100.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.248
 encapsulation frame-relay
 ip nat inside
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 ip nat outside
 no cdp enable
interface Vlan1
 no ip address
```



```
 shutdown
router eigrp 1
 passive-interface Gig0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 default-information originate
 no auto-summary
ip nat pool LAN 209.165.202.128 209.165.202.159 netmask 255.255.255.224
ip nat inside source list 1 pool LAN overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
access-list 1 permit 10.0.0.0 0.255.255.255
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

ISP del router

```
ISP#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname ISP
spanning-tree mode pvst
interface Gig0/0
 ip address 209.165.200.225 255.255.255.252
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 209.165.201.1 255.255.255.252
 clock rate 64000
interface Serial0/0/1
 no ip address
interface Serial0/2/0
 no ip address
interface Serial0/2/1
 no ip address
interface Vlan1
 no ip address
 shutdown
```



```
ip classless
ip route 209.165.202.128 255.255.255.224 Serial0/0/0
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

Switch S1

```
S1#sh run
hostname S1
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```



```
line vty 5 15
 login
end
```

Switch S2

```
S2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S2
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
```



```
interface Vlan105
 ip address 10.3.105.21 255.255.255.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S3

```
S3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S3
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
```



```
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan105
 ip address 10.3.105.22 255.255.255.0
ip default-gateway 10.3.1.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S4

```
S4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S4
enable secret class
spanning-tree mode pvst
spanning-tree vlan 1,5,15,25,35 priority 4096
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
```



```
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.21 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S5

```
S5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S5
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
```



```
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.23 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S6

```
S6#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S6
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
```



```
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
 switchport access vlan 15
 switchport mode access
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
 switchport access vlan 25
 switchport mode access
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
 switchport access vlan 35
 switchport mode access
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.22 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
```



```
 password cisco
 login
line vty 5 15
 login
end
```

Switch S7

```
S7#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S7
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```


Packet Tracer: Resolución de problemas de redes empresariales 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

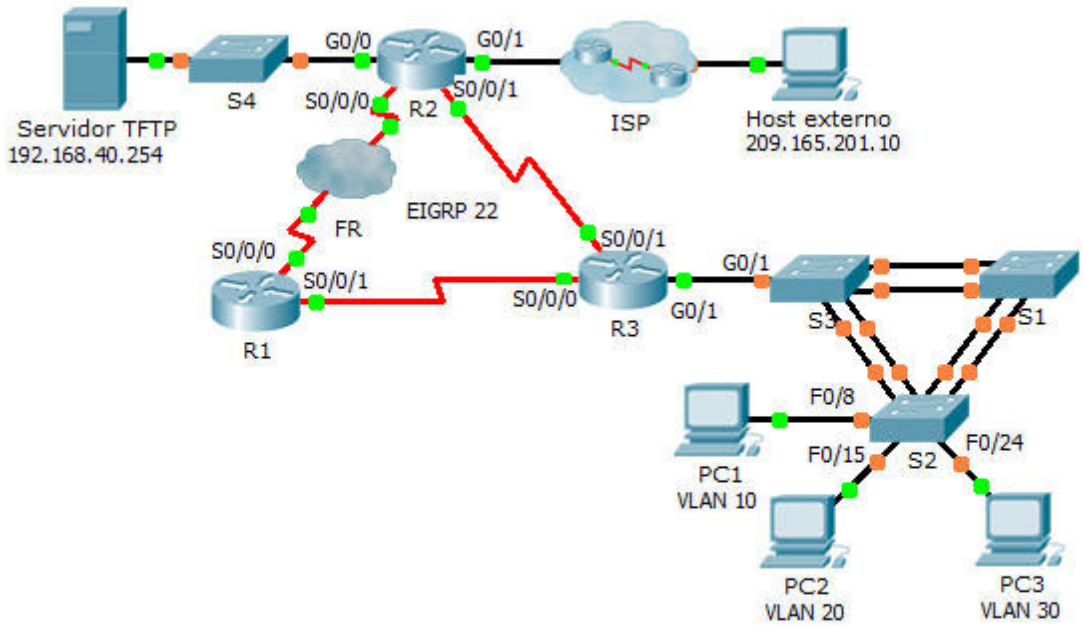


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	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	G0/0	192.168.40.1	255.255.255.0	N/A
	G0/1	DHCP assigned	DHCP assigned	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	G0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0.20	192.168.20.1	255.255.255.0	N/A
	G0/0.30	192.168.30.1	255.255.255.0	N/A
	G0/0.88	192.168.88.1	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
S1	VLAN 88	192.168.88.2	255.255.255.0	192.168.88.1
S2	VLAN 88	192.168.88.3	255.255.255.0	192.168.88.1
S3	VLAN 88	192.168.88.4	255.255.255.0	192.168.88.1
PC1	NIC	DHCP assigned	DHCP assigned	DHCP assigned
PC2	NIC	DHCP assigned	DHCP assigned	DHCP assigned
PC3	NIC	DHCP assigned	DHCP assigned	DHCP assigned
TFTP Server	NIC	192.168.40.254	255.255.255.0	192.168.40.1

Información básica

En esta actividad, se usa una variedad de tecnologías con las que se encontró durante sus estudios de CCNA, entre ellas, la tecnología VLAN, STP, el routing, el routing entre VLAN, DHCP, NAT, PPP y Frame Relay. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Requisitos

VLAN y acceso

- El S2 es la raíz del árbol de expansión para las VLAN 1, 10 y 20. El S3 es la raíz del árbol de expansión para las VLAN 30 y 88.
- Los enlaces troncales que conectan los switches están en la VLAN 99 nativa.
- El R3 es responsable del routing entre VLAN y funciona como servidor de DHCP para las VLAN 10, 20 y 30.

Routing

- Cada router se configura con EIGRP y usa el número de AS 22.
- El R2 se configura con una ruta predeterminada que apunta al ISP y redistribuye la ruta predeterminada.
- Se configura NAT en el R2, y no se permite que las direcciones sin traducir crucen Internet.

WAN Technologies

- El enlace serial entre el R1 y el R2 usa Frame Relay.
- El enlace serial entre el R2 y el R3 usa la encapsulación HDLC.
- El enlace serial entre el R1 y el R3 usa PPP con CHAP.

Conectividad

- Se deben configurar los dispositivos según la tabla de direccionamiento.
- Cada dispositivo debe poder hacer ping a todos los demás dispositivos.

Documentación de resolución de problemas

Dispositivo	Problema	Solución
R1	El R1 y el R2 no forman una adyacencia.	`interface Serial0/0/0` `encapsulation frame-relay`
R1	El nombre de usuario y las contraseñas son incorrectos.	`username R3 password 0 ciscoccna`

R2	El servidor TFTP no puede hacer ping al host externo.	`interface g0/0`
		`no ip nat outside`
		`ip nat inside`
		`interface g0/1`
		`ip nat outside`

R2	La ruta predeterminada apunta a la interfaz incorrecta.	`no ip route 0.0.0.0 0.0.0.0 g0/0` `ip route 0.0.0.0 0.0.0.0 g0/1`
S1	Falta de concordancia con la VLAN nativa	`interface range fa0/1-4` `switchport trunk native vlan 99`
S2	Este switch no es el puente raíz para las VLAN 1, 10 y 20.	`spanning-tree vlan 1,10,20 root primary`
S3	Las computadoras no extraen una dirección DHCP.	`interface g0/1` `switchport mode trunk`

Documentación de verificación

Capture el resultado de los comandos de verificación y proporcione la documentación que comprueba que se cumplió con cada uno de los requisitos.

Nota para el instructor: las respuestas para esta sección se dejan en blanco porque existen muchas formas de verificar los requisitos.

Rúbrica de calificación sugerida

Packet Tracer suma 60 puntos. El registro de resolución de problemas y la verificación del instructor valen 40 puntos.

Packet Tracer: Resolución de problemas de redes empresariales 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

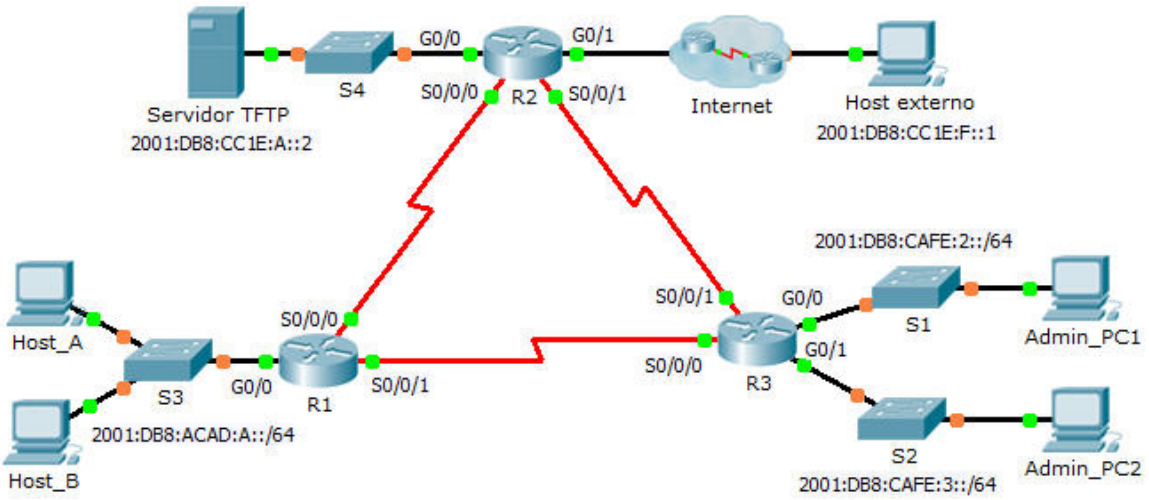


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0	2001:DB8:ACAD:12::1/64	N/A
	S0/0/1	2001:DB8:ACAD:31::1/64	N/A
R2	G0/0	2001:DB8:CC1E:A::1/64	N/A
	G0/1	2001:DB8:ACAD:F::2/64	N/A
	S0/0/0	2001:DB8:ACAD:12::2/64	N/A
	S0/0/1	2001:DB8:ACAD:23::2/64	N/A
R3	G0/0	2001:DB8:CAFE:2::1/64	N/A
	G0/1	2001:DB8:CAFE:3::1/64	N/A
	S0/0/0	2001:DB8:ACAD:31::2/64	N/A
	S0/0/1	2001:DB8:ACAD:23::1/64	N/A
Admin_PC1	NIC	2001:DB8:CAFE:2::2/64	FE80::3
Admin_PC2	NIC	2001:DB8:CAFE:3::2/64	FE80::3
Host_A	NIC	DHCP Assigned	DHCP Assigned
Host_B	NIC	DHCP Assigned	DHCP Assigned
TFTP Server	NIC	2001:DB8:CC1E:A::2/64	FE80::2
Outside Host	NIC	2001:DB8:CC1E:F::1/64	FE80::4

Información básica

En esta actividad, se usan configuraciones de IPv6, incluidas DHCPv6, EIGRPv6 y el routing IPv6 predeterminado. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Requisitos

DHCPv6

- El **Host_A** y el **Host_B** se asignan mediante DHCP IPv6 configurado en el R1.

Routing IPv6

- Cada router se configura con EIGRP IPv6 y usa el número de AS 100.
- El **R3** anuncia una ruta resumida al **R2** y el **R1** para las dos LAN del **R3**.
- El **R2** se configura con una ruta predeterminada completamente especificada que apunta al **ISP**.

Conectividad

- Se deben configurar los dispositivos según la tabla de direccionamiento.
- Cada dispositivo debe poder hacer ping a todos los demás dispositivos.

Documentación de resolución de problemas

Dispositivo	Error	Corrección
R1	El host_A y el host_B no obtienen direccionamiento del R1 porque el pool de DHCPv6 IPv6 no está asignado en la interfaz G0/0.	`interface g0/0` `ipv6 dhcp server R1_LAN`

R1	La interfaz S0/0/1 está configurada con una dirección IPv6 incorrecta.	`int s0/0/1`
		`no ipv6 address 2001:DB8:ACAD:32::1/64`
		`ipv6 address 2001:DB8:ACAD:31::1/64`

R1	El S3 está conectado a una interfaz incorrecta del R1.	`Switch the cable in the topology from G0/1 to G0/0`
R2	La ruta predeterminada tiene configurada una dirección de siguiente salto incorrecta.	`no ipv6 route ::/0 GigabitEthernet0/0 2001:DB8:ACAD:F::` `ipv6 route ::/0 GigabitEthernet0/1 2001:DB8:ACAD:F::1`

R2	EIGRP para IPv6 está configurado con un sistema autónomo incorrecto.	`int g0/0`
		`no ipv6 eigrp 1000`
		`ipv6 eigrp 100`

R3	EIGRP para IPv6 100 está desactivado.	`ipv6 router eigrp 100` `no shutdown`

R3	La dirección de resumen EIGRP se anuncia incorrectamente en S0/0/1.	`int s0/0/0`
		`no ipv6 summary-address eigrp 100 2001:DB8:CAFE::/65 5`
		`ipv6 summary-address eigrp 100 2001:DB8:CAFÉ:2::/63 5`
		`int s0/0/1`
		`no ipv6 summary-address eigrp 100 2001:DB8:CAFE::/65 5`
		`ipv6 summary-address eigrp 100 2001:DB8:CAFE:2::/63 5`

Documentación de verificación

Capture el resultado de los comandos de verificación y proporcione la documentación que comprueba que se cumplió con cada uno de los requisitos.

Nota: algunos comandos EIGRPv6 no tienen puntuación en Packet Tracer v6.0.1. El instructor verifica que se cumpla con todos los requisitos.

Nota para el instructor: las respuestas para esta sección se dejan en blanco porque existen muchas formas de verificar los requisitos. Para fines de calificación, observe que las rutas resumidas EIGRPv6 no se califican en Packet Tracer. Además, Packet Tracer no califica la dirección del siguiente salto en la ruta predeterminada IPv6 completamente especificada. Revise el archivo del estudiante para verificar las configuraciones.

Rúbrica de calificación sugerida

Packet Tracer suma 50 puntos. El registro de resolución de problemas y la verificación del instructor valen 50 puntos.

Packet Tracer: Resolución de problemas de redes empresariales 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

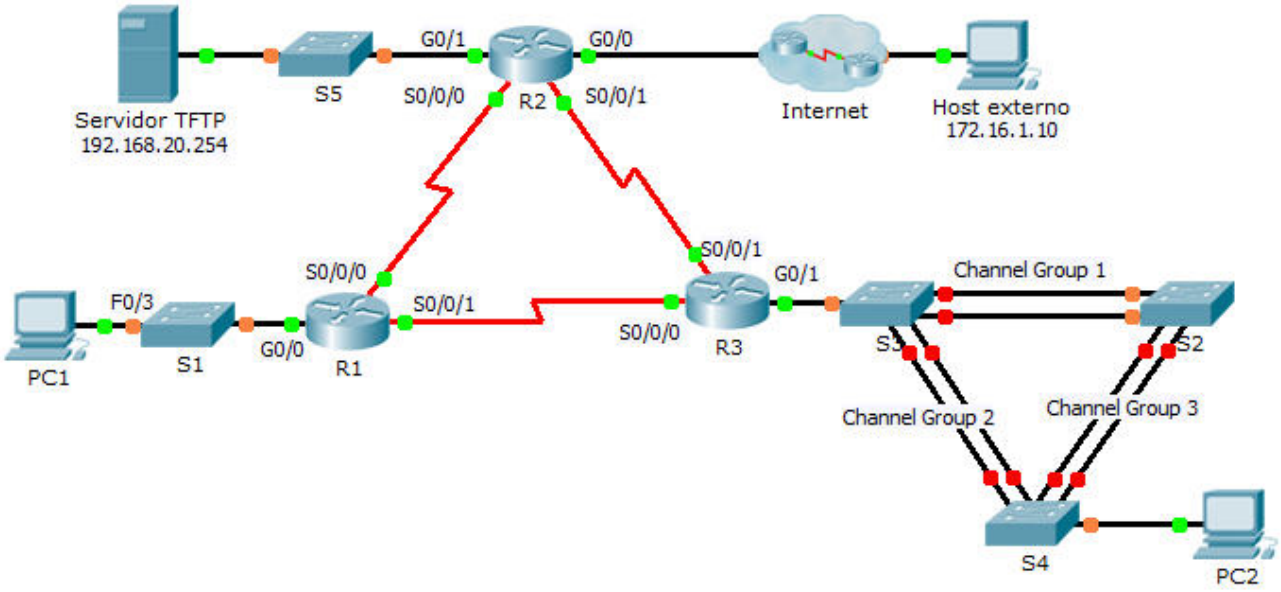


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	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	G0/0	209.165.200.225	255.255.255.224	N/A
	G0/1	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	G0/1	192.168.30.1	255.255.255.0	NN/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
S1	VLAN10	DHCP assigned	DHCP assigned	DHCP assigned
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	DHCP assigned	DHCP assigned	DHCP assigned
PC2	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Información básica

En esta actividad, se usa una variedad de tecnologías con las que se encontró durante sus estudios de CCNA, entre ellas, el routing, la seguridad de puertos, EtherChannel, DHCP, NAT, PPP y Frame Relay. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Nota: esta actividad comienza con una puntuación parcial.

Requisitos

DHCP

- El R1 es el servidor de DHCP para la LAN del R1.

Tecnologías de switching

- La seguridad de puertos se configura para permitir que solo la **PC1** acceda a la interfaz F0/3 del **S1**. La interfaz se debe deshabilitar cuando se produzca cualquier infracción.
- Se configura la agregación de enlaces mediante EtherChannel en el **S2**, el **S3** y el **S4**.

Routing

- Todos los routers se configuran con la ID de proceso OSPF 1, y no se debe enviar ninguna actualización de routing a través de las interfaces que no tienen routers conectados.

- El R2 se configura con una ruta predeterminada que apunta al ISP y redistribuye la ruta predeterminada.
- Se configura NAT en el R2, y no se permite que las direcciones sin traducir crucen Internet.

WAN Technologies

- El enlace serial entre el R1 y el R2 usa Frame Relay.
- El enlace serial entre el R2 y el R3 usa la encapsulación HDLC.
- El enlace serial entre el R1 y el R3 usa PPP con PAP.

Conectividad

- Se deben configurar los dispositivos según la tabla de direccionamiento.
- Cada dispositivo debe poder hacer ping a todos los demás dispositivos.

Documentación de resolución de problemas

Dispositivo	Error	Corrección
R1	Hay un gateway predeterminado incorrecto en el pool de DHCP.	`ip dhcp pool Access` `default-router 192.168.10.1`
R1	La propagación de la ruta predeterminada no se debe configurar en este router.	`router ospf 1` `no default-information originate`
R2	La propagación de la ruta predeterminada se debe configurar en este router.	`router ospf 1` `default-information originate`
R2	Encapsulación incorrecta en S0/0/1.	`interface s0/0/1` `encapsulation hdlc`

R3	El R3 no forma una adyacencia con el R1 y el R2.	`router ospf 1`
		`no passive-interface default`
		`passive-interface g0/1`

S1	La seguridad del puerto se configuró en la interfaz incorrecta.	`interface FastEthernet0/3`
		` switchport access vlan 10`
		` switchport mode access`
		` switchport port-security`
		` switchport port-security mac-address sticky`

S3	El puerto de switch de la interfaz G1/1 no está configurado como puerto de enlace troncal.	`interface g1/1` `switchport mode trunk`

S4	Los canales de puertos están configurados incorrectamente.	`interface range f0/1-2`
		` no channel-group 3 mode auto`
		` channel-group 2 mode auto`
		
		`interface range f0/3-4`
		` no channel-group 2 mode auto`
		` channel-group 3 mode auto`

Documentación de verificación

Capture el resultado de los comandos de verificación y proporcione la documentación que comprueba que se cumplió con cada uno de los requisitos.

Nota para el instructor: las respuestas para esta sección se dejan en blanco porque existen muchas formas de verificar los requisitos.

Rúbrica de calificación sugerida

Packet Tracer suma 60 puntos. El registro de resolución de problemas y la verificación del instructor valen 40 puntos.

Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas (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

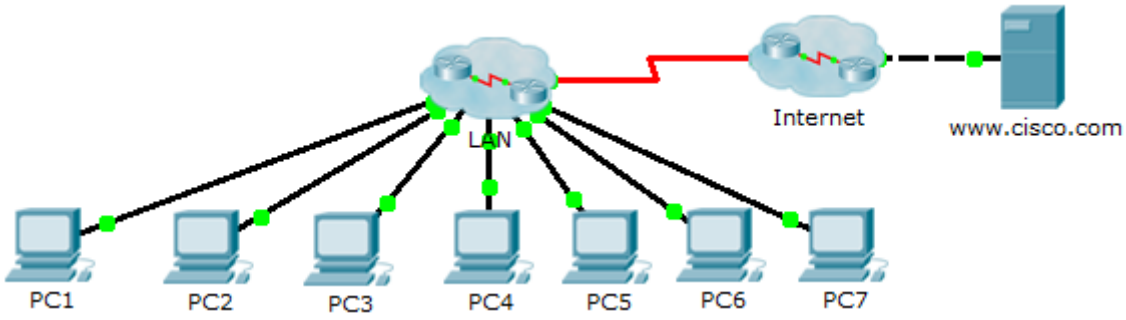


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC1	NIC	10.2.15.10	255.255.255.0	10.2.15.1
PC2	NIC	10.2.25.10	255.255.255.0	10.2.25.1
PC3	NIC	10.2.35.10	255.255.255.0	10.2.35.1
PC4	NIC	10.3.100.4	255.255.255.0	10.3.100.1
PC5	NIC	10.3.100.5	255.255.255.0	10.3.100.1
PC6	NIC	10.4.1.10	255.255.255.0	10.4.1.1
PC7	NIC	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	NIC	10.1.100.2	255.255.255.0	10.1.100.1
R1	S0/0/0	10.1.0.4	255.255.255.248	N/A
	G0/0	10.4.1.1	255.255.255.0	N/A
R2	S0/0/0	10.1.0.3	255.255.255.248	N/A
	G0/0.100	10.3.100.1	255.255.255.0	N/A
	G0/0.105	10.3.105.1	255.255.255.0	N/A
R3	S0/0/0	10.1.0.2	255.255.255.248	N/A
	G0/0.5	10.2.5.1	255.255.255.0	N/A
	G0/0.15	10.2.15.1	255.255.255.0	N/A
	G0/0.25	10.2.25.1	255.255.255.0	N/A
	G0/0.35	10.2.35.1	255.255.255.0	N/A
R4	S0/0/0	10.1.0.5	255.255.255.248	N/A
	G0/0	10.5.1.1	255.255.255.0	N/A
R5	S0/0/0	10.1.0.1	255.255.255.248	N/A
	S0/0/1	209.165.201.2	255.255.255.252	N/A
	G0/0	10.1.100.1	255.255.255.0	N/A
S1	None	None	None	None
S2	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
S3	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
S4	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
S5	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
S6	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
S7	None	None	None	None

Objetivos

Parte 1: Reunir información para el registro

Parte 2: Probar la conectividad

Parte 3: Reunir datos e implementar soluciones

Parte 4: Probar la conectividad

Situación

Esta es la parte 2 de una actividad que consta de dos partes. La parte 1 es **Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red**, que debe haber completado anteriormente en el capítulo. En la parte 2, usará sus habilidades de resolución de problemas y el registro de la parte 1 para resolver los problemas de conectividad entre las computadoras.

Parte 1: Reunir información para el registro

Paso 1: Recuperar la documentación de red.

Para completar esta actividad correctamente, necesitará la documentación de la actividad **Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red**, que completó anteriormente en este capítulo. Ahora busque dicha documentación.

Paso 2: Requisitos del registro.

La documentación que completó en la actividad anterior debe contar con una topología y una tabla de direccionamiento precisas. De ser necesario, actualice la documentación para reflejar una representación precisa de una respuesta correcta de la actividad **Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red**. Es posible que deba consultar al instructor.

Nota para el instructor: el estudiante debe tener una representación completa y precisa de la red de respuesta de la actividad anterior, **Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red**. Necesitará verificar que el trabajo anterior del estudiante sea correcto o proporcionar un registro preciso.

Parte 2: Probar la conectividad

Paso 1: Determinar la ubicación de la falla de conectividad.

Al final de esta actividad, debe haber plena conectividad entre las computadoras, así como entre las computadoras y el servidor www.cisco.pka. No obstante, ahora debe determinar dónde falla la conectividad mediante los siguientes pings:

- De las computadoras al servidor **www.cisco.pka**
- PC a PC
- De las computadoras al gateway predeterminado

Paso 2: ¿Qué pings se realizaron correctamente?

Registre los pings que se realizaron correctamente y los que fallaron.

Ninguna de las computadoras puede hacer ping al servidor www.cisco.pka. La PC1, la PC2 y la PC3 pueden hacer ping entre sí. La PC4 y la PC5 pueden hacer ping entre sí. Todas las computadoras pueden hacer ping a sus respectivos gateways predeterminados.

Parte 3: Reunir datos e implementar soluciones

Paso 1: Elegir una computadora para comenzar a reunir datos.

Elija cualquier computadora y comience a recopilar datos probando la conectividad al gateway predeterminado. También puede usar **traceroute** para ver dónde falla la conectividad.

Paso 2: Acceder al gateway predeterminado mediante telnet y continuar con la recolección de datos.

a. Si la computadora que eligió no tiene conectividad a su gateway predeterminado, elija otra computadora para abordar el problema desde un sentido diferente.

b. Una vez que estableció la conectividad a través de un gateway predeterminado, la contraseña de inicio de sesión es **cisco** y la contraseña del modo EXEC privilegiado es **class**.

Paso 3: Usar las herramientas de resolución de problemas para verificar la configuración.

En el router de gateway predeterminado, use las herramientas de resolución de problemas para verificar la configuración con su propia documentación. Recuerde revisar los switches además de los routers. Asegúrese de verificar lo siguiente:

- Información de direccionamiento
- Activación de interfaces
- Encapsulación
- Routing
- configuración de la VLAN
- Incompatibilidades de dúplex o de velocidad

Paso 4: Registrar los síntomas de la red y las posibles soluciones.

A medida que detecte los síntomas del problema de conectividad de las computadoras, agréguelos a la documentación.

Nota para el instructor: la siguiente es solo una manera en la que el estudiante puede avanzar a lo largo de esta actividad. El estudiante puede comenzar por cualquier computadora, excepto **www.cisco.pka.** En esta respuesta de ejemplo, comenzamos en la **PC4**.

Problema 1: desde la **PC4**, puede acceder al gateway predeterminado, el **R2**. Accede al **R2** mediante telnet y verifica la tabla de routing. El **R2** solo tiene rutas conectadas directamente; por lo tanto, verifica la configuración de interfaz actual mediante el comando **show protocols** o **show ip interface brief**. Un análisis cuidadoso de las direcciones IP revela que la dirección de S0/0/0 es incorrecta. Debe ser 10.1.0.3 en vez de 10.1.100.3. El comando **show ip protocols** revela que no hay problemas con la configuración de EIGRP en el **R2**.

Solución 1: configura la dirección IP correcta para la interfaz S0/0/0 en el **R2**.

Problema 2: después de que EIGRP converge en el **R2**, usa el comando **show ip route** para reunir más información sobre posibles problemas. El **R2** tiene rutas conectadas correctas, pero solo tiene dos rutas EIGRP. Las rutas faltantes incluyen las cuatro VLAN para el **R3**, la LAN del **R1** y la LAN del **R4**. El ping al **R3** es correcto; por lo tanto, accede al **R3** mediante telnet. Dado que el **R2** no recibe rutas del **R3**, verifica la configuración de EIGRP en el **R3** con el comando **show ip protocols**. El **R3** envía y recibe actualizaciones de EIGRP y anuncia la red correcta. Sin embargo, la sumarización automática de redes está vigente. Por lo tanto, el **R3** solo envía la red con clase 10.0.0.0/8 en las actualizaciones periódicas de EIGRP.

Solución 2: configura el **R3** con el comando **no auto-summary**.

Problema 3: sale al **R3** y verifica la tabla de routing. Faltan las rutas para las LAN del **R1** y el **R4**. Prueba la conectividad al **R1** y al **R4** por medio de pings a las interfaces seriales de esos routers. Los pings al **R1** fallan, pero los pings al **R4** se realizan correctamente. Accede al **R4** mediante telnet. En el **R4**, muestra la tabla de routing. El **R4** no tiene rutas EIGRP; por lo tanto, usa el comando **show ip protocols** para verificar el routing EIGRP. El comando no genera ningún resultado en la sección Routing for Networks (Routing de redes), de modo que EIGRP tampoco está configurado correctamente. Usa el comando **show run** para verificar los comandos EIGRP. A EIGRP le falta el comando network.

Solución 3: configura el **R4** con el comando network 10.0.0.0 de EIGRP.

Problema 4: después de que EIGRP converge, verifica la tabla de routing del **R4**. Aún falta la LAN del **R1**. Dado que los ping al **R1** fallan, accede al **R1** desde la **PC6**. Primero, hace ping a la dirección de gateway predeterminado y, luego, accede al **R1** mediante telnet. Muestre la tabla de routing. Observa que solo la red F0/0 está en la tabla de routing. Revisa la configuración de interfaz con el comando **show ip interface brief**. La interfaz S0/0/0 está físicamente activa, pero la capa de enlace de datos está inactiva. Investiga S0/0/0 con el comando **show interface**. La encapsulación está establecida como PPP en lugar de como Frame Relay.

Solución 4: cambia la encapsulación de la interfaz S0/0/0 en el R1 de PPP a Frame Relay con el comando **encapsulation frame-relay**. Ahora, todas las computadoras deben poder hacer ping entre sí.

Problema 5: las computadoras aún no pueden hacer ping al servidor www.cisco.pka. Desde cualquier dispositivo, prueba la conectividad y después accede al **R5** mediante telnet. Investiga el estado de la interfaz con el comando **show ip interface brief**. La interfaz S0/0/1 está administrativamente inactiva.

Solución 5: activa la interfaz S0/0/1 en el **R5** con el comando **no shutdown**.

Problema 6: las computadoras aún no pueden hacer ping al servidor www.cisco.pka. Sin embargo, las computadoras pueden hacer ping al servidor DNS. El problema está en la configuración del **R5** o en la configuración del ISP. Dado que no tiene acceso al router ISP, verifica la configuración en el **R5**. El comando **show run** revela que el **R5** usa NAT. A la configuración le falta la instrucción de NAT que vincula al conjunto de NAT con la lista de acceso.

Solución 6: configura el **R5** con el comando **ip nat inside source list 1 pool LAN overload**.

Paso 5: Realizar los cambios basados en las soluciones del paso anterior.

Parte 4: Probar la conectividad

Paso 1: Probar la conectividad de la computadora.

a. Ahora, todas las computadoras deben poder hacer ping entre sí y al servidor **www.cisco.pka**. Si modificó las configuraciones IP, cree nuevos pings, dado que los pings anteriores usan la dirección IP antigua.

b. Si siguen existiendo problemas de conectividad entre las computadoras o entre estas y el servidor, vuelva a la parte 3 y continúe con la resolución de problemas.

Paso 2: Verificar los resultados.

Su puntuación de Packet Tracer debe ser de 70/70. De lo contrario, vuelva a la parte 2 y continúe con la resolución de problemas y la implementación de las soluciones sugeridas. No podrá hacer clic en **Check Results** (Verificar resultados) y ver qué componentes obligatorios aún no se completaron.

Rúbrica de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Probar la conectividad	Paso 2-a	15	
	Total de la parte 2	**15**	
Parte 3: Reunir datos e implementar soluciones	Paso 4-a	15	
	Total de la parte 3	**15**	
	Puntuación de Packet Tracer	**70**	
	Puntuación total	**100**	

Configuraciones de dispositivos

Router R1

```
R1#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.4.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.4 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 network 10.0.0.0
 no auto-summary
ip classless
```



```
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R2 del router

```
R2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
enable secret class
spanning-tree mode pvst
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.3.100.1 255.255.255.0
interface GigabitEthernet0/0.105
 encapsulation dot1Q 105 native
 ip address 10.3.105.1 255.255.255.0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.3 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
```



```
line vty 0 4
 password cisco
 login
end
```

R3 del router

```
R3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R3
enable secret class
spanning-tree mode pvst
interface Gig0/0
 no ip address
 duplex auto
 speed auto
interface Gig0/0.5
 encapsulation dot1Q 5 native
 ip address 10.2.5.1 255.255.255.0
interface Gig0/0.15
 encapsulation dot1Q 15
 ip address 10.2.15.1 255.255.255.0
interface Gig0/0.25
 encapsulation dot1Q 25
 ip address 10.2.25.1 255.255.255.0
interface Gig0/0.35
 encapsulation dot1Q 35
 ip address 10.2.35.1 255.255.255.0
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
```



```
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

R4 del router

```
R4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R4
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.5.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.5 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```


R5 del router

```
R5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R5
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.1.100.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.248
 encapsulation frame-relay
 ip nat inside
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 ip nat outside
 no cdp enable
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 default-information originate
 no auto-summary
ip nat pool LAN 209.165.202.128 209.165.202.159 netmask 255.255.255.224
ip nat inside source list 1 pool LAN overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
access-list 1 permit 10.0.0.0 0.255.255.255
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```


ISP del router

```
ISP#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname ISP
spanning-tree mode pvst
interface Gig0/0
 ip address 209.165.200.225 255.255.255.252
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 209.165.201.1 255.255.255.252
 clock rate 64000
interface Serial0/0/1
 no ip address
interface Serial0/2/0
 no ip address
interface Serial0/2/1
 no ip address
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 209.165.202.128 255.255.255.224 Serial0/0/0
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

Switch S1

```
S1#sh run
hostname S1
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
```



```
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S2

```
S2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S2
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
```



```
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan105
 ip address 10.3.105.21 255.255.255.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S3

```
S3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S3
enable secret class
spanning-tree mode pvst
```



```
interface FastEthernet0/1
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan105
 ip address 10.3.105.22 255.255.255.0
ip default-gateway 10.3.1.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```


Switch S4

```
S4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S4
enable secret class
spanning-tree mode pvst
spanning-tree vlan 1,5,15,25,35 priority 4096
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
```



```
 ip address 10.2.5.21 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S5

```
S5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S5
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
```



```
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.23 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S6

```
S6#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S6
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
 switchport access vlan 15
 switchport mode access
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
```



```
interface FastEthernet0/11
 switchport access vlan 25
 switchport mode access
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
 switchport access vlan 35
 switchport mode access
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.22 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Switch S7

```
S7#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S7
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
```



```
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```


Packet Tracer: Desafío de integración de habilidades de CCNA

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

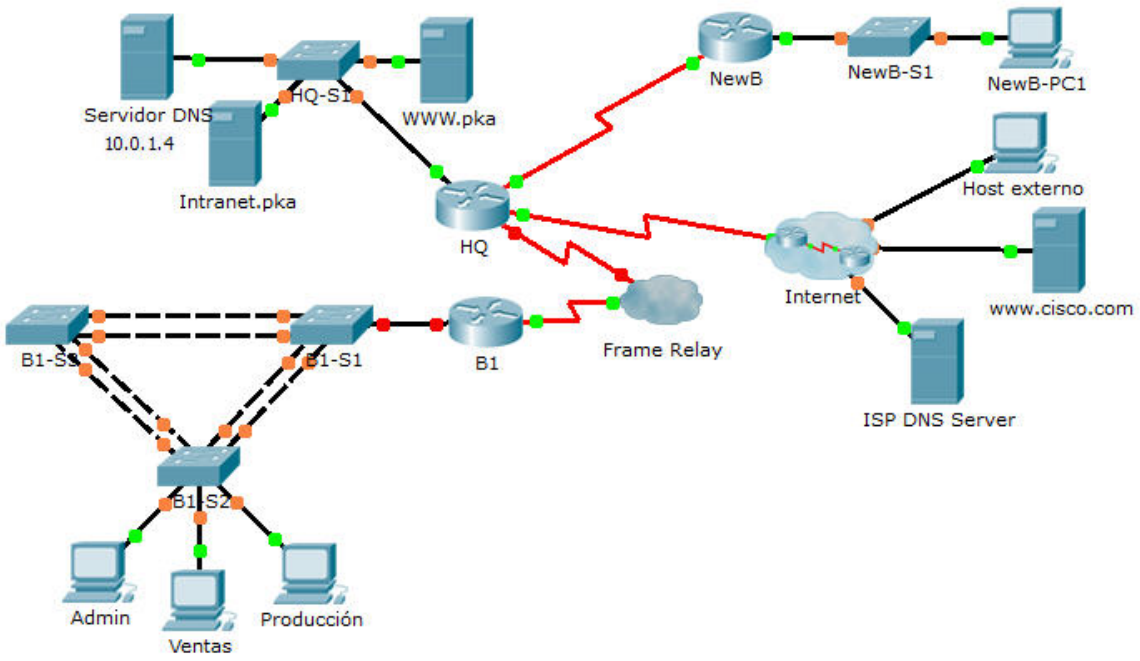


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado Asignación DLCI
HQ	G0/0	10.0.1.1	255.255.255.0	N/A
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 to B1
	S0/0/1	10.255.255.253	255.255.255.252	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A
B1	G0/0.10	10.1.10.1	255.255.255.0	N/A
	G0/0.20	10.1.20.1	255.255.255.0	N/A
	G0/0.30	10.1.30.1	255.255.255.0	N/A
	G0/0.99	10.1.99.1	255.255.255.0	N/A
	S0/0/0	10.255.255.2	255.255.255.252	N/A
B1-S2	VLAN 99	10.1.99.22	255.255.255.0	10.1.99.1

Configuración de VLAN y asignaciones de puertos

Número de VLAN	Dirección de red	Nombre de la VLAN	Asignaciones de puertos
10	10.1.10.0/24	Admin	Fa0/6
20	10.1.20.0/24	Ventas	Fa0/11
30	10.1.30.0/24	Producción	Fa0/16
99	10.1.99.0/24	Mgmt&Native	Fa0/1-4
999	No aplicable	BlackHole	Puertos no utilizados

Situación

En esta actividad integral de habilidades de CCNA, la empresa XYZ usa una combinación de Frame Relay y PPP para las conexiones WAN. Otras tecnologías incluyen NAT, DHCP, el routing estático y predeterminado, EIGRP para IPv4, el routing entre VLAN y la configuración de VLAN. Las configuraciones de seguridad incluyen SSH, seguridad de puertos, seguridad de switches y ACL.

Requisitos

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

SSH

- Configure **HQ** para usar acceso remoto mediante SSH.
  - Establezca el módulo en **2048**. El nombre de dominio es **CCNASkills.com**.
  - El nombre de usuario es **admin** y la contraseña es **adminonly**.
  - Solo se debería permitir SSH en las líneas VTY.
  - Modifique los valores predeterminados de SSH: versión 2; tiempo de espera de 60 segundos; dos reintentos.

Frame Relay

- Configure Frame Relay entre **HQ** y **B1**.
  - Consulte la tabla de direccionamiento para obtener la dirección IP, la máscara de subred y el DLCI.
  - **HQ** usa una subinterfaz punto a punto y un DLCI 41 para conectarse a **B1**.
  - El tipo de LMI se debe configurar manualmente como **q933a** para **HQ** y **B1**.

PPP

- Configure el enlace WAN de **HQ** a Internet mediante la encapsulación PPP y la autenticación CHAP.
  - Cree un usuario **ISP** con la contraseña **cisco**.
- Configure el enlace WAN de **HQ** a **NewB** (NuevoB) mediante la encapsulación PPP y la autenticación PAP.
  - **HQ** es el lado DCE del enlace. Elija la frecuencia de reloj.
  - Cree un usuario **NewB** con la contraseña **cisco**.

NAT

- Configure la NAT estática y dinámica en HQ.
  - Permita que todas las direcciones del espacio de direcciones 10.0.0.0/8 se traduzcan mediante una lista de acceso estándar con nombre **NAT**.
  - La compañía XYZ posee el espacio de direcciones 209.165.200.240/29. El conjunto, **HQ**, usa las direcciones .241 a .245 con una máscara /29.
  - El sitio web **WWW.pka** en 10.0.1.2 está registrado en el sistema DNS público en la dirección IP 209.165.200.246 y se debe poder acceder a él desde el **host externo**.

DHCP

- En **B1**, configure un pool de DHCP para la VLAN 20 de Ventas con los siguientes requisitos:
  - Excluya las primeras 10 direcciones IP en el rango.
  - El nombre del pool, que distingue mayúsculas de minúsculas, es **VLAN20**.
  - Incluya el servidor DNS conectado a la LAN de **HQ** como parte de la configuración DHCP.
- Configure la computadora **Ventas** para usar DHCP.

Enrutamiento estático y predeterminado

- Configure **HQ** con una ruta predeterminada a **Internet** y una ruta estática a la LAN de **NewB**. Use la interfaz de salida como argumento.

Routing EIGRP

- Configure y optimice **HQ** y **B1** con el routing EIGRP.
  - Use el sistema autónomo 100 y deshabilite la sumarización automática.
  - **HQ** debe anunciar el router estático y predeterminado a **B1**.
  - Deshabilite las actualizaciones de EIGRP en las interfaces adecuadas.
  - Resuma manualmente las rutas EIGRP de modo que el router **B1** solo anuncie el espacio de direcciones 10.1.0.0/16 a **HQ**.

Routing entre VLAN

- Configure **B1** para el routing entre VLAN.
  - Mediante la tabla de direccionamiento para los routers de sucursal, configure y active la interfaz LAN para el routing entre VLAN. La VLAN 99 es la VLAN nativa.

Configuraciones de VLAN y enlaces troncales

- Configure los enlaces troncales y las VLAN en **B1-S2**.
  - Cree y nombre las VLAN que se indican en la tabla de **Configuración de VLAN y asignaciones de puertos** solo en **B1-S2**.
  - Configure la interfaz y el gateway predeterminado de la VLAN 99.
  - Asigne las VLAN a los puertos de acceso adecuados.
  - Establezca el modo de enlace troncal en activado para Fa0/1 a Fa0/4.
  - Deshabilite todos los puertos sin utilizar y asigne la VLAN **BlackHole**.

Seguridad del puerto

- Use la siguiente política para establecer la seguridad de puertos en los puertos de acceso de **B1-S2**:
  - Permita que se descubra una de las direcciones MAC en el puerto.

- Configure la primera dirección MAC descubierta para que se ajuste a la configuración.
- Configure el puerto para que se desconecte si se produce una violación de seguridad.

Política de lista de acceso

- Debido a que HQ se conecta a Internet, configure una ACL con nombre denominada **HQINBOUND,** en el siguiente orden:
  - Permita las solicitudes HTTP entrantes en el servidor de **WWW.pka**.
  - Permita solo las sesiones TCP establecidas desde Internet.
  - Permita solo las respuestas de ping entrantes desde Internet.
  - Bloquee explícitamente todos los demás accesos entrantes desde Internet.

Conectividad

- Verifique la plena conectividad de cada computadora a **WWW.pka** y a **www.cisco.pka**.

Configuraciones de dispositivos

HQ del router

```
enable
conf t
username ISP password cisco
username NewB password cisco
username admin password adminonly
ip domain-name CCNASkills.com
crypto key generate rsa
1024
line vty 0 16
 transport input ssh
 login local
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 60
interface Gig0/0
 ip nat inside
interface Serial0/0/0
 encapsulation frame-relay
 frame-relay lmi-type q933a
 no shut
interface Serial0/0/0.41 point-to-point
 ip address 10.255.255.1 255.255.255.252
 frame-relay interface-dlci 41
 ip nat inside
interface Serial0/0/1
 description Link to NewB
 ip address 10.255.255.253 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username HQ password cisco
 ip nat inside
```



```
 no shut
interface Serial0/1/0
 description Link to ISP
 encapsulation ppp
 ppp authentication chap
 ip access-group HQINBOUND in
 ip nat outside
router eigrp 100
 passive-interface Gig0/0
 passive-interface Serial0/0/1
 passive-interface Serial0/1/0
 network 10.0.0.0
 redistribute static
 no auto-summary
ip nat pool HQ 209.165.200.241 209.165.200.245 netmask 255.255.255.248
ip nat inside source list NAT pool HQ overload
ip nat inside source static 10.0.1.2 209.165.200.246
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
ip route 10.4.5.0 255.255.255.0 Serial0/0/1
ip access-list standard NAT
 permit 10.0.0.0 0.255.255.255
ip access-list extended HQINBOUND
 permit tcp any host 209.165.200.246 eq www
 permit tcp any any established
 permit icmp any any echo-reply
 deny ip any any
line vty 0 15
 login local
 transport input ssh
end
```

Router B1

```
enable
conf t
ip dhcp excluded-address 10.1.20.1 10.1.20.10
ip dhcp pool VLAN20
 network 10.1.20.0 255.255.255.0
 default-router 10.1.20.1
 dns-server 10.0.1.4
interface Gig0/0
 no shut
interface Gig0/0.10
 description Admin VLAN 10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
interface Gig0/0.20
 description Sales VLAN 20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
```

```
interface Gig0/0.30
 description Production VLAN 30
 encapsulation dot1Q 30
 ip address 10.1.30.1 255.255.255.0
interface Gig0/0.99
 description Mgmt&Native VLAN 99
 encapsulation dot1Q 99 native
 ip address 10.1.99.1 255.255.255.0
interface Serial0/0/0
 ip address 10.255.255.2 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 ip summary-address eigrp 100 10.1.0.0 255.255.0.0 5
 no shut
router eigrp 100
 passive-interface Gig0/0.10
 passive-interface Gig0/0.20
 passive-interface Gig0/0.30
 passive-interface Gig0/0.88
 passive-interface Gig0/0.99
 network 10.0.0.0
 no auto-summary
end
```

Switch B1-S2

```
enable
conf t
vlan 10
 name Admin
vlan 20
 name Sales
vlan 30
 name Production
vlan 99
 name Mgmt&Native
vlan 999
 name BlackHole
interface range FastEthernet0/1-0/4
 switchport trunk native vlan 99
 switchport mode trunk
interface range fa0/5,fa0/7-10,fa0/12-15,fa0/17-24,g1/1-2
 description Unused port
 switchport access vlan 999
 switchport mode access
 shutdown
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 switchport port-security
```

```
 switchport port-security mac-address sticky
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
interface Vlan99
 ip address 10.1.99.22 255.255.255.0
ip default-gateway 10.1.99.1
end
```