



**DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN
DE SOLUCIONES INTEGRADAS LAN / WAN)**


ACTIVIDAD COLABORATIVA 4

Presentado por:

José Julián Samacá
80152935

**TUTOR
GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
NOVIEMBRE 28 DE 2017**





INTRODUCCION

En este documento encontrará laboratorios relacionados con la unidad 4 del curso diplomado de profundización Cisco 203092 de la UNAD, en el cual se estudiaron y pusieron en práctica temas como enrutamiento estático, enrutamiento dinámico, protocolos de estado de enlace como OSPF, listas de control de acceso, configuración dinámica de dirección IP o DHCP y por ultimo traducción de direcciones de red para IPv4 mediante NAT propios de dicha unidad y además se practicarán y repasarán conceptos adquiridos en las unidades anteriores.




OBJETIVOS GENERALES

OBJETIVOS

- Leer, analizar e interpretar las temáticas relacionadas con el enrutamiento estático, enrutamiento dinámico, enrutamiento mediante protocolos de estado enlace, listas de acceso, asignación dinámica de direcciones IP y traducciones de direcciones IP mediante NAT.
- Revisar el material sugerido para el abordaje de cada una de las temáticas.
- Fortalecer posteriormente el desarrollo de competencias en el área del saber específico orientadas al uso de protocolos de enrutamiento avanzado.

OBJETIVOS ESPECÍFICOS

- *CONFIGURE IP ACLS TO MITIGATE ATTACKS*
 - Verify connectivity among devices before firewall configuration.
 - Use ACLs to ensure remote access to the routers is available only from management station PC-C.
 - Configure ACLs on R1 and R3 to mitigate attacks.
 - Verify ACL functionality.
 - *CONFIGURING BASIC RIPv2 AND RIPv6*
 - Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
 - Parte 2: configurar y verificar el routing RIPv2
 - Configurar y verificar que se esté ejecutando RIPv2 en los routers.
 - Configurar una interfaz pasiva.
 - Examinar las tablas de routing.
- 

- Desactivar la sumarización automática.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.
- Parte 3: configurar IPv6 en los dispositivos
- Parte 4: configurar y verificar el routing RIPng
- Configurar y verificar que se esté ejecutando RIPng en los routers.
- Examinar las tablas de routing.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.
- **CONFIGURING BASIC DHCPV4 ON A ROUTER**
- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP
- **CONFIGURACIÓN DE OSPFv2 BÁSICO DE ÁREA ÚNICA**
- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar y verificar el routing OSPF
- Parte 3: cambiar las asignaciones de ID del router
- Parte 4: configurar interfaces OSPF pasivas
- Parte 5: cambiar las métricas de OSPF
- **CONFIGURACIÓN DE OSPFV3 BÁSICO DE ÁREA ÚNICA**
- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

- Parte 2: configurar y verificar el routing OSPFv3
- Parte 3: configurar interfaces pasivas OSPFv3

- **CONFIGURING STANDARD ACLS**

- Part 1: Plan an ACL Implementation
- Part 2: Configure, Apply, and Verify a Standard ACL

- **CONFIGURING NAMED STANDARD ACLS**

- Part 1: Configure and Apply a Named Standard ACL
- Part 2: Verify the ACL Implementation

- **CONFIGURING AN ACL ON VTY LINES**

- Part 1: Configure and Apply an ACL to VTY Lines
- Part 2: Verify the ACL Implementation

- **CONFIGURING IPV6 ACLS**

- Part 1: Configure, Apply, and Verify an IPv6 ACL
- Part 2: Configure, Apply, and Verify a Second IPv6 ACL

- **CONFIGURING BASIC DHCPV4 ON A ROUTER**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

- **CONFIGURACIÓN DE DHCPV4 BÁSICO EN UN SWITCH**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: cambiar la preferencia de SDM

- **IdT y DHCP**

- Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

- **CONFIGURACIÓN DE DHCPV6 SIN ESTADO Y CON ESTADO**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar la red para SLAAC
- Parte 3: configurar la red para DHCPv6 sin estado
- Parte 4: configurar la red para DHCPv6 con estado

- **CONFIGURACIÓN DE NAT DINÁMICA Y ESTÁTICA**

- Parte 1: armar la red y verificar la conectividad
- Parte 2: configurar y verificar la NAT estática
- Parte 3: configurar y verificar la NAT dinámica

- **CONFIGURACIÓN DE UN CONJUNTO DE NAT CON SOBRECARGA Y PAT**

- Parte 1: armar la red y verificar la conectividad
- Parte 2: configurar y verificar un conjunto de NAT con sobrecarga
- Parte 3: configurar y verificar PAT

7.3.2.4 Lab - Configuring Basic RIPv2 and RIPvng

Práctica de laboratorio: configuración básica de RIPv2 y RIPvng

Topología

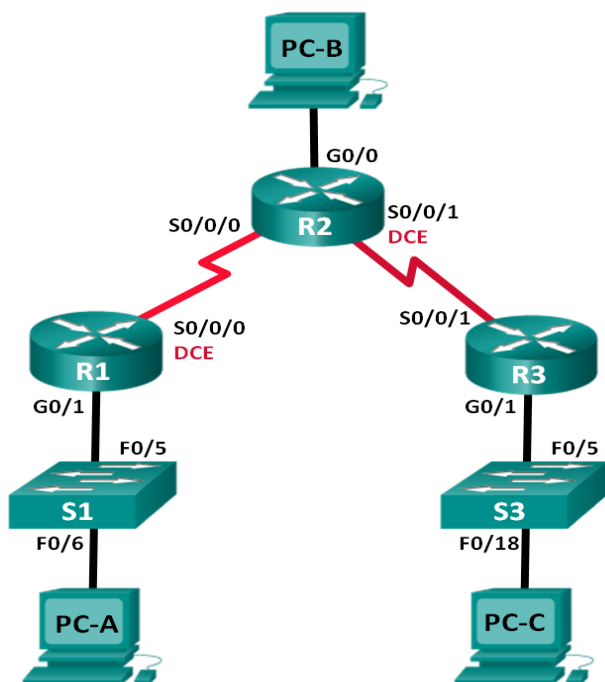


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/1/0	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Objetivos

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

Parte 2: configurar y verificar el routing RIPv2

- Configurar y verificar que se esté ejecutando RIPv2 en los routers.
- Configurar una interfaz pasiva.
- Examinar las tablas de routing.
- Desactivar la sumarización automática.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.

Parte 3: configurar IPv6 en los dispositivos

Parte 4: configurar y verificar el routing RIPv6

- Configurar y verificar que se esté ejecutando RIPng en los routers.
- Examinar las tablas de routing.
- Configurar una ruta predeterminada.
- Verificar la conectividad de extremo a extremo.

Información básica/situación

RIP versión 2 (RIPv2) se utiliza para enrutar direcciones IPv4 en redes pequeñas. RIPv2 es un protocolo de routing vector distancia sin clase, según la definición de RFC 1723. Debido a que RIPv2 es un protocolo de routing sin clase, las máscaras de subred se incluyen en las actualizaciones de routing. De manera predeterminada, RIPv2 resume automáticamente las redes en los límites de redes principales. Cuando se deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos.

RIP de última generación (RIPng) es un protocolo de routing vector distancia para enrutar direcciones IPv6, según la definición de RFC 2080. RIPng se basa en RIPv2 y tiene la misma distancia administrativa y limitación de 15 saltos.

En esta práctica de laboratorio, configurará la topología de la red con routing RIPv2, deshabilitará la sumarización automática, propagará una ruta predeterminada y usará comandos de CLI para ver y verificar la información de routing RIP. Luego, configurará la topología de la red con direcciones IPv6, configurará RIPng, propagará una ruta predeterminada y usará comandos de CLI para ver y verificar la información de routing RIPng.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

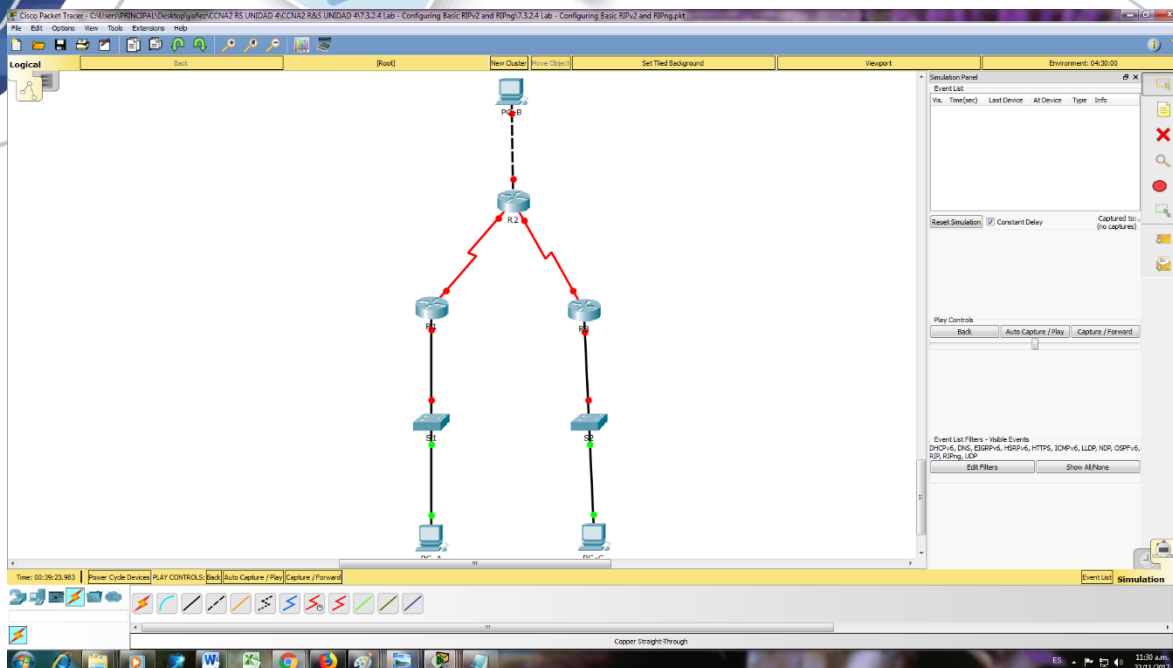
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

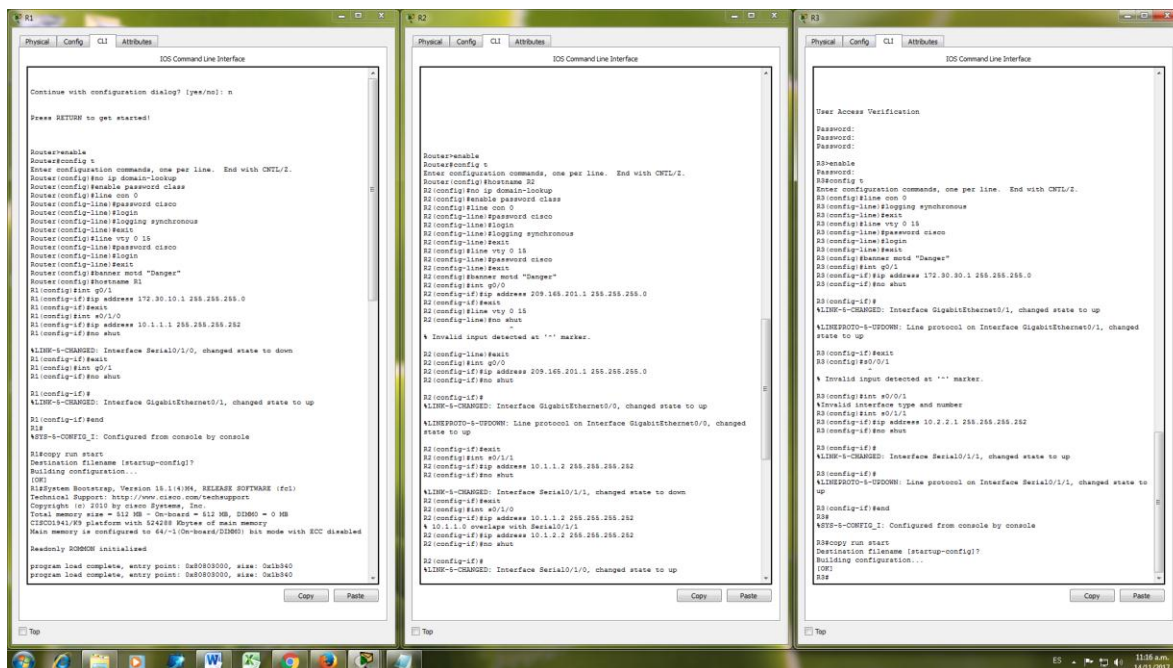
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos.

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



Paso 2. inicializar y volver a cargar el router y el switch.



The screenshots show the IOS Command Line Interface (CLI) for routers R1, R2, and R3. The process of initializing and reloading the devices is shown.

```

R1:
Router#enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#banner motd "Danger"
Router(config)#hostname R1
R1(config)#ip address 172.30.10.1 255.255.255.0
R1(config)#exit
R1(config)#ip address 10.1.1.1 255.255.255.252
R1(config)#exit
R1#show ip interface brief
R1#
R1#reload
R1#

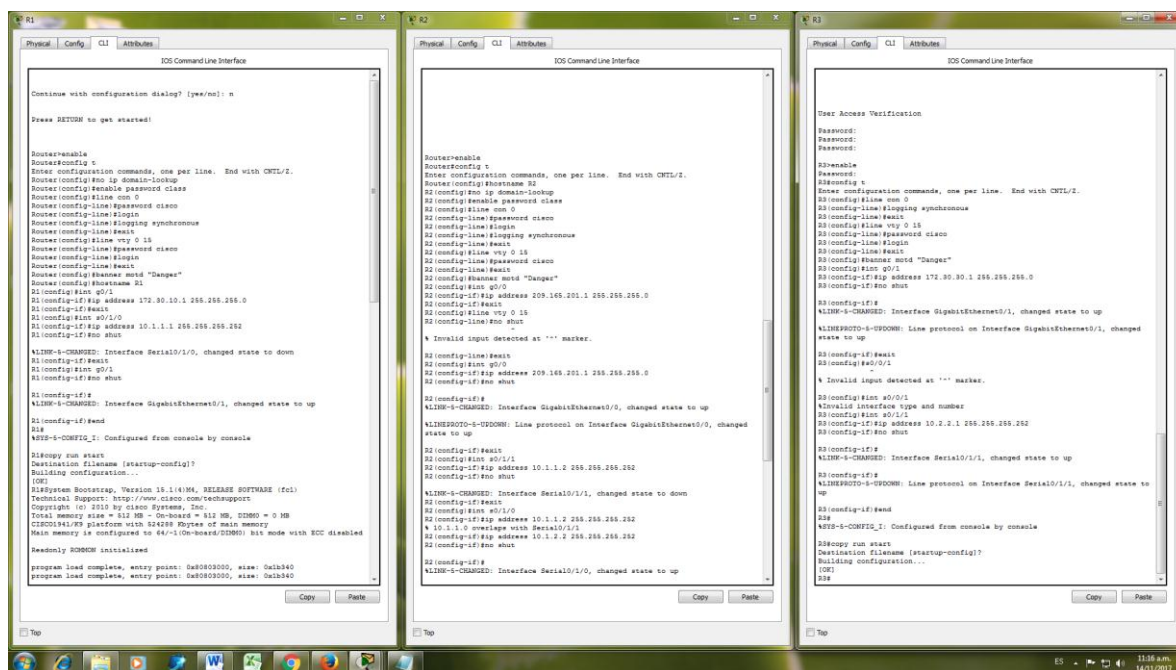
R2:
Router#enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#banner motd "Danger"
Router(config)#hostname R2
R2(config)#ip address 209.169.201.1 255.255.255.0
R2(config)#exit
R2(config)#ip address 10.1.1.2 255.255.255.252
R2(config)#exit
R2#show ip interface brief
R2#
R2#reload
R2#

R3:
User Access Verification
Password:
Password:
Router#enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
R3(config)#ip address 172.30.30.1 255.255.255.0
R3(config)#exit
R3(config)#ip address 10.2.1.1 255.255.255.252
R3(config)#exit
R3#show ip interface brief
R3#
R3#reload
R3#
  
```

Paso 3. configurar los parámetros básicos para cada router y switch.

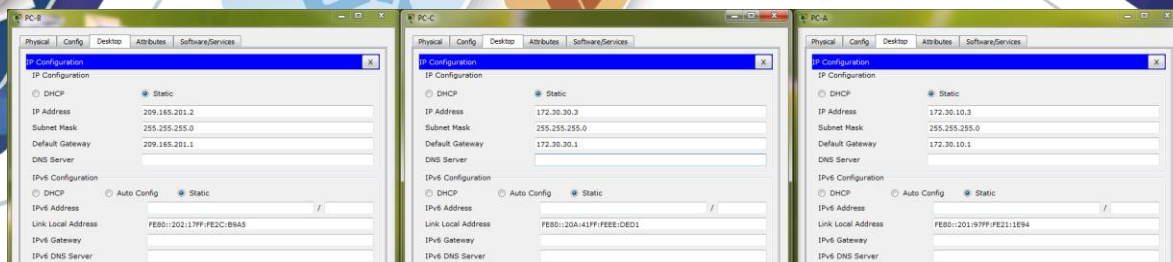
- Desactive la búsqueda del DNS.
- Configure los nombres de los dispositivos como se muestra en la topología.

- c. Configurar la encriptación de contraseñas.
- d. Asigne **class** como la contraseña del modo EXEC privilegiado.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- g. Configure **logging synchronous** para la línea de consola.
- h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- i. Configure una descripción para cada interfaz con una dirección IP.
- j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.
- k. Copie la configuración en ejecución en la configuración de inicio.



Paso 4. configurar los equipos host.

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



Paso 5. Probar la conectividad.

En este momento, las computadoras no pueden hacerse ping entre sí.

- Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

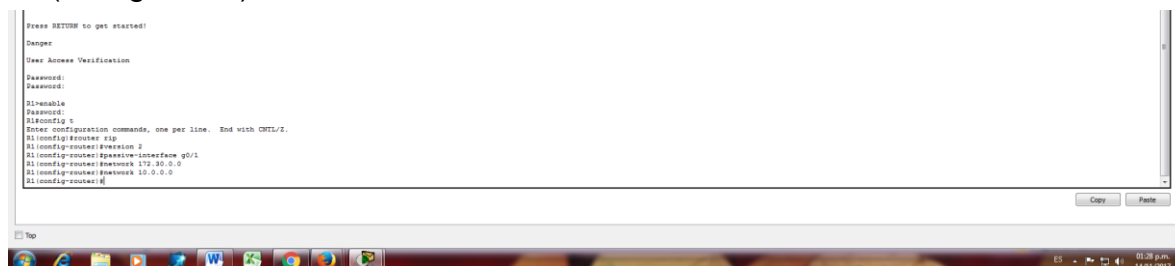
Parte 2: configurar y verificar el routing RIPv2

En la parte 2, configurará el routing RIPv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Una vez que haya verificado RIPv2, deshabilitará el sumarización automática, configurará una ruta predeterminada y verificará la conectividad de extremo a extremo.

Paso 1. Configurar el enrutamiento RIPv2.

- En el R1, configure RIPv2 como el protocolo de routing y anuncie las redes correspondientes.

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```



El comando **passive-interface** evita que las actualizaciones de routing se envíen a través de la interfaz especificada. Este proceso evita tráfico de routing innecesario en la LAN. Sin embargo, la red a la que pertenece la

interfaz especificada aún se anuncia en las actualizaciones de routing enviadas por otras interfaces.

- d. Configure RIPv2 en el R3 y utilice la instrucción **network** para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.
- e. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

Nota: no es necesario establecer la interfaz G0/0 como pasiva en el R2, porque la red asociada a esta interfaz no se está anunciando.

Paso 2. examinar el estado actual de la red.

- a. Se pueden verificar los dos enlaces seriales rápidamente mediante el comando **show ip interface brief** en R2.

R2# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	209.165.201.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.1.1.2	YES	manual	up	up
Serial0/0/1	10.2.2.2	YES	manual	up	up

```

R2>enable
R2>configure terminal
R2>router rip
R2>network 10.0.0.0
R2>network 224.0.0.9
R2>network 10.1.1.2
R2>network 10.2.2.2
R2>passive-interface Embedded-Service-Engine0/0
R2>passive-interface GigabitEthernet0/0
R2>passive-interface GigabitEthernet0/1
R2>show ip interface brief
R2>
R2>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up
Vlan1 unassigned YES unset administratively down down
R2>
R2>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up
Vlan1 unassigned YES unset administratively down down
R2>
R2>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up
Vlan1 unassigned YES unset administratively down down
R2>

```

- b. Verifique la conectividad entre las computadoras.
 ¿Es posible hacer ping de la PC-A a la PC-B? **NO**
 ¿Por qué?
No hay ruta que llegue a pc-b,

```

PC-A
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Request timed out.
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
  
```

¿Es posible hacer ping de la PC-A a la PC-C? **NO**

¿Por qué?

R1 y R3 no tienen ruta hacia la subnet específica en el router remoto,

```

PC-A
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.3
Pinging 172.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Ping statistics for 172.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
  
```

¿Es posible hacer ping de la PC-C a la PC-B? **NO**

¿Por qué? PC-B no participa en "rip" La LAN donde esta PC-B, no participa en ruta.

```

PC-C
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
  
```

¿Es posible hacer ping de la PC-C a la PC-A? **NO**

¿Por qué?

No, porque R1 y R3 no tienen rutas, hacia la subnet específica, remota. No tiene ruta "rip" específica

```

PC-C
Physical  Config  Desktop  Attributes  Software/Services

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Request timed out.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

c. Verifique que RIPv2 se ejecute en los routers.

Puede usar los comandos **debug ip rip**, **show ip protocols** y **show run** para confirmar que RIPv2 esté en ejecución. A continuación, se muestra el resultado del comando **show ip protocols** para el R1.

```

R1# show ip protocols
Variable
Reasons:
  Show ip protocols
  Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 3 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0        2      2
  Serial0/0/1        2      2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    172.30.0.0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance    Last Update
    10.1.1.1         120         00:00:28
  Distance: (default is 120)
  RIP

```

R1# show ip protocols

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 7 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Redistributing: rip

Default version control: **send version 2, receive 2**

Interface Send Recv Triggered RIP Key-chain

```

Serial0/0/0      2 2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance    Last Update
  10.1.1.2         120
Distance: (default is 120)
  
```

Al emitir el comando **debug ip rip** en el R2, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?

```

show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 7 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
   Interface      Send Recv Triggered RIP  Max-hops
  Serial0/0/1      2      2
  Serial0/0/0      2      2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance    Last Update
    10.1.1.2         120         00:00:19
  10.1.1.1         120         00:00:19
  
```

La depuración del protocolo RIP está activada

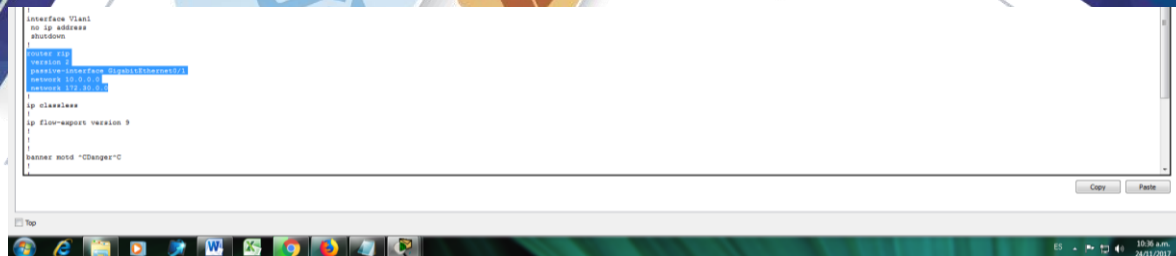
Cuando haya terminado de observar los resultados de la depuración, emita el comando **undebug all** en la petición de entrada del modo EXEC privilegiado.

Se ha desactivado toda la depuración posible

```

undebug all
All possible debugging has been turned off
  
```

Al emitir el comando **show run** en el R3, ¿qué información se proporciona que confirma que RIPv2 está en ejecución?



router rip

version 2

passive-interface GigabitEthernet0/1

network 10.0.0.0

network 172.30.0.0

- d. Examinar el sumarización automática de las rutas.

Las LAN conectadas al R1 y el R3 se componen de redes no contiguas. El R2 muestra dos rutas de igual costo a la red 172.30.0.0/16 en la tabla de routing. El R2 solo muestra la dirección de red principal con clase 172.30.0.0 y no muestra ninguna de las subredes de esta red.

R2# show ip route

<Output Omitted>

```

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.2/32 is directly connected, Serial0/0/0
C    10.2.2.0/30 is directly connected, Serial0/0/1
L    10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
      [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.0/24 is directly connected, GigabitEthernet0/0
L    209.165.201.1/32 is directly connected, GigabitEthernet0/0

```

El R1 solo muestra sus propias subredes para la red 172.30.0.0. El R1 no tiene ninguna ruta para las subredes 172.30.0.0 en el R3.

R1# show ip route

<Output Omitted>

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0

```


R1# show ip route

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IS - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
C    10.1.1.1/32 is directly connected, Serial0/0/0
R    10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
R    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.30.10.0/24 is directly connected, GigabitEthernet0/1
L    172.30.10.1/32 is directly connected, GigabitEthernet0/1
R    172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
R
```

<Output Omitted>

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0

172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0

R3# show ip route

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IS - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.2.2.0/30 is directly connected, Serial0/0/1
C    10.2.2.1/32 is directly connected, Serial0/0/1
R    10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
R    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.30.30.0/24 is directly connected, GigabitEthernet0/1
L    172.30.30.1/32 is directly connected, GigabitEthernet0/1
R    172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
R
```

<Output Omitted>

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.1/32 is directly connected, Serial0/0/1

R 10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1

172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.30.30.0/24 is directly connected, GigabitEthernet0/1

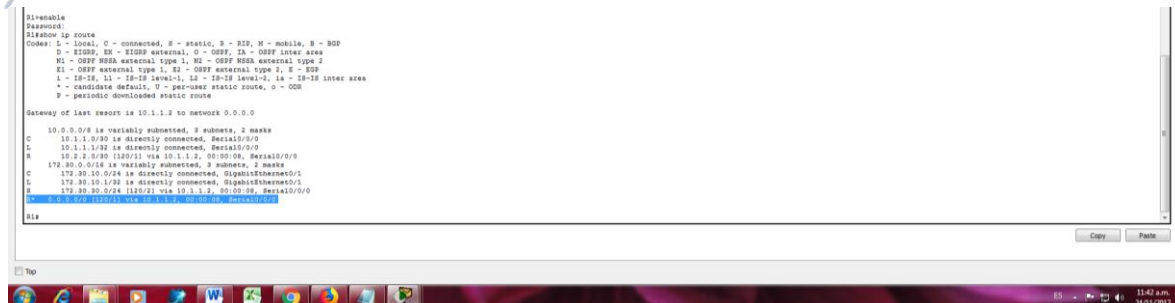
L 172.30.30.1/32 is directly connected, GigabitEthernet0/1

R 172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1

Paso 5. Verificar la configuración de enrutamiento.

k. Consulte la tabla de routing en el R1.

R1# show ip route



```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IS - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
  C   10.1.1.0/30 is directly connected, Serial0/0/0
  L   10.1.1.1/32 is directly connected, Serial0/0/0
  R   10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
  C   172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
  C   172.30.10.0/24 is directly connected, GigabitEthernet0/1
  L   172.30.10.1/32 is directly connected, GigabitEthernet0/1
  R   172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0
  S   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
  
```

<Output Omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0

172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.30.10.0/24 is directly connected, GigabitEthernet0/1

L 172.30.10.1/32 is directly connected, GigabitEthernet0/1

R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0

¿Cómo se puede saber, a partir de la tabla de routing, que la red dividida en subredes que comparten el R1 y el R3 tiene una ruta para el tráfico de Internet?

Hay un Gateway, de ultimo alcance, una puerta de enlace, que nos conecta ha internet, y la ruta por defecto que se muestra en la tabla de ruteo esta aprendida por "rip"

I. Consulte la tabla de routing en el R2.

```

R2#enable
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IS - IS-IS inter area
       * - candidate default, U - per-user static route, s - ODR
       D - periodic downloaded static route

Gateway of last resort is 209.165.201.2 to network 0.0.0.0

R 0.0.0.0/0 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/24 is directly connected, Serial0/0/0
C 10.1.1.2/24 is directly connected, Serial0/0/0
C 10.2.2.0/24 is directly connected, Serial0/0/1
C 10.2.2.2/24 is directly connected, Serial0/0/1
S 172.30.0.0/24 is subnetted, 2 subnets
R 172.30.0.0/24 (120/1) via 10.1.1.1, 00:00:03, Serial0/0/0
R 172.30.30.0/24 (120/1) via 10.2.2.1, 00:00:10, Serial0/0/1
C 209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.201.0/24 is directly connected, GigabitEthernet0/0
L 209.165.201.1/32 is directly connected, GigabitEthernet0/0
  
```

¿En qué forma se proporciona la ruta para el tráfico de Internet en la tabla de routing?

R2 tiene una ruta estatica por defecto 0.0.0.0 via 209.165.201.2 directamente conectada a la G0/0

Paso 6. Verifique la conectividad.

m. Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2.

¿Tuvieron éxito los pings? si

n. Verifique que los hosts dentro de la red dividida en subredes tengan posibilidad de conexión entre sí haciendo ping entre la PC-C y la PC-A.

¿Tuvieron éxito los pings? SI

Nota: quizá sea necesario deshabilitar el firewall de las computadoras.

Parte 3: configurar IPv6 en los dispositivos

En la parte 3, configurará todas las interfaces con direcciones IPv6 y verificará la conectividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

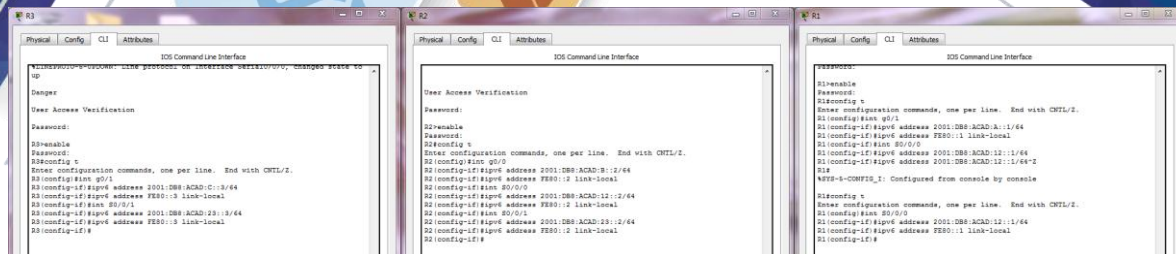
Paso 1. configurar los equipos host.

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

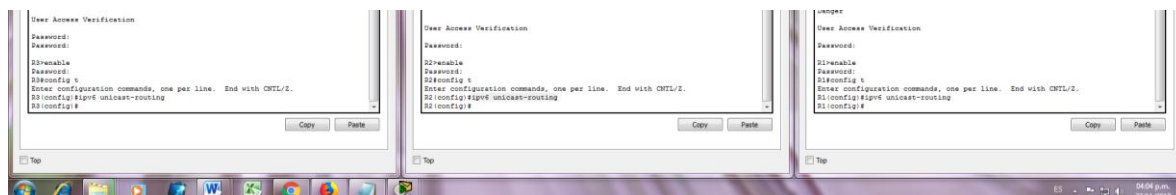
Paso 2. configurar IPv6 en los routers.

Nota: la asignación de una dirección IPv6 además de una dirección IPv4 en una interfaz se conoce como “dual-stacking” (o apilamiento doble). Esto se debe a que las pilas de protocolos IPv4 e IPv6 están activas.

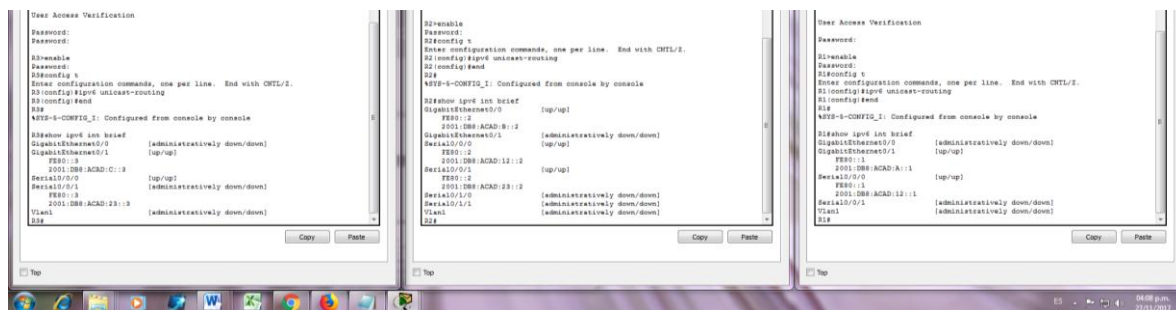
- o. Para cada interfaz del router, asigne la dirección global y la dirección link local de la tabla de direccionamiento.



p. Habilite el routing IPv6 en cada router.



q. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace. Escriba el comando en el espacio que se incluye a continuación.



- r. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.
- s. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

Parte 4: configurar y verificar el routing RIPng

En la parte 4, configurará el routing RIPng en todos los routers, verificará que las tablas de routing estén correctamente actualizadas, configurará y distribuirá una ruta predeterminada, y verificará la conectividad de extremo a extremo.

Paso 1. configurar el routing RIPng.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción network se eliminó en RIPng. En cambio, el routing RIPng se habilita en el nivel de la interfaz y se identifica por un nombre de proceso pertinente en el nivel local, ya que se pueden crear varios procesos con RIPng.

- t. Emita el comando **ipv6 rip Test1 enable** para cada interfaz en el R1 que participará en el routing RIPng, donde **Test1** es el nombre de proceso pertinente en el nivel local.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```

- u. Configure RIPng para las interfaces seriales en el R2, con **Test2** como el nombre de proceso. No lo configure para la interfaz G0/0
- v. Configure RIPng para cada interfaz en el R3, con **Test3** como el nombre de proceso.
- w. Verifique que RIPng se esté ejecutando en los routers.

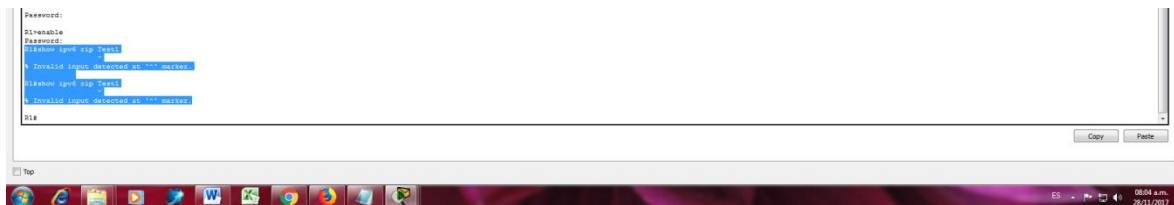
Los comandos **show ipv6 protocols**, **show run**, **show ipv6 rip database** y **show ipv6 rip nombre de proceso** se pueden usar para confirmar que se esté ejecutando RIPng. En el R1, emita el comando **show ipv6 protocols**.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
Interfaces:
  Serial0/0/0
  GigabitEthernet0/1
Redistribution:
  None
```

¿En qué forma se indica RIPng en el resultado?

RIPng is listed by process name

- x. Emita el comando **show ipv6 rip Test1**. No lo soporta el comando **Cisco Pack Traer**



```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 1, trigger updates 0
```

Full Advertisement 0, Delayed Events 0

Interfaces:

GigabitEthernet0/1

Serial0/0/0

Redistribution:

None

¿Cuáles son las similitudes entre RIPv2 y RIPv6?

Ambas tienen la distancia administrativa de 120, usan el conteo de saltos como la métrica, y envían actualizaciones cada 30 segundos.

y. Inspeccione la tabla de routing IPv6 en cada router. Escriba el comando apropiado que se usa para ver la tabla de routing en el espacio a continuación.

En el R1, ¿cuántas rutas se descubrieron mediante RIPv6? 2

En el R2, ¿cuántas rutas se descubrieron mediante RIPv6? 2

En el R3, ¿cuántas rutas se descubrieron mediante RIPv6? 2

z. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? **NO**

¿Es posible hacer ping de la PC-A a la PC-C? **NO**

¿Es posible hacer ping de la PC-C a la PC-B? **NO**

¿Es posible hacer ping de la PC-C a la PC-A? **NO**

Paso 2. configurar y volver a distribuir una ruta predeterminada.

aa. Desde el R2, cree una ruta estática predeterminada a la red:: 0/64 con el comando **ipv6 route** y la dirección IP de la interfaz de salida G0/0. Esto reenvía todo tráfico de dirección de destino desconocida a la interfaz G0/0

del R2 hacia la PC-B y simula Internet. Escriba el comando que utilizó en el espacio a continuación.

bb.ipv6 route ::/0 2001:db8:acad:b::b

cc. Las rutas estáticas se pueden incluir en las actualizaciones RIPng mediante el comando **ipv6 rip nombre de proceso default-information originate** en el modo de configuración de interfaz. Configure los enlaces seriales en el R2 para enviar la ruta predeterminada en actualizaciones RIPng.

R2(config)# int s0/0/0

R2(config-rtr)# ipv6 rip Test2 default-information originate

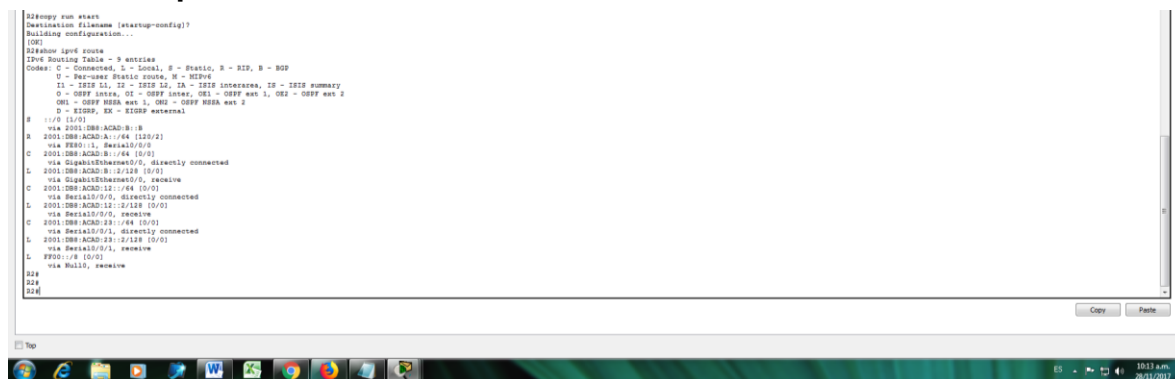
R2(config)# int s0/0/1

R2(config-rtr)# ipv6 rip Test2 default-information originate

Paso 3. Verificar la configuración de enrutamiento.

dd. Consulte la tabla de routing IPv6 en el router R2.

R2# show ipv6 route



```

R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external

S ::/64 [1/0]
  via 2001:DB8:ACAD:B::B
R 2001:DB8:ACAD:A::/64 [120/2]
  via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:B::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:B::/64 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:B::/64 [0/0]
  via Serial0/0/0, receive
L 2001:DB8:ACAD:B::/64 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:B::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:B::/64 [0/0]
  via Serial0/0/1, receive
S FE80::/64 [0/0]
  via Null0, receive

```

IPv6 Routing Table - 10 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

S ::/64 [1/0]

via 2001:DB8:ACAD:B::B

R 2001:DB8:ACAD:A::/64 [120/2]

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:B::/64 [0/0]

via ::, GigabitEthernet0/1

- L 2001:DB8:ACAD:B::2/128 [0/0]
via ::, GigabitEthernet0/1
- R 2001:DB8:ACAD:C::/64 [120/2]
via FE80::3, Serial0/0/1
- C 2001:DB8:ACAD:12::/64 [0/0]
via ::, Serial0/0/0
- L 2001:DB8:ACAD:12::2/128 [0/0]
via ::, Serial0/0/0
- C 2001:DB8:ACAD:23::/64 [0/0]
via ::, Serial0/0/1
- L 2001:DB8:ACAD:23::2/128 [0/0]
via ::, Serial0/0/1
- L FF00::/8 [0/0]
via ::, Null0

¿Cómo se puede saber, a partir de la tabla de routing, que el R2 tiene una ruta para el tráfico de Internet?

```

R2#show ip route
IPV6 Routing Table - R2#12345
Codes: C - Connected, L - Local, B - Static, S - RIPv6, B - BGP
       O - OSPFv3 External, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS Interarea, IS - ISIS Summary
       O - OSPFv3 Area, O1 - OSPFv3 Inter, O2 - OSPFv3 ext 1, O3 - OSPFv3 ext 2
       D - EIGRP, EX - EIGRP External
R2#
R 2001:DB8:ACAD:B::/64 [120/2]
  via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:B::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:12::/64 [0/0]
  via Serial0/0/0, receive
L 2001:DB8:ACAD:12::2/128 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::2/128 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
224

```

Tiene una ruta por defecto estatica, que se muestra en R2.

ee. Consulte las tablas de routing del R1 y el R3.

¿Cómo se proporciona la ruta para el tráfico de Internet en sus tablas de enrutamiento?

La tabla de ruteo se muestra en RIPv6, con una métrica de 2

Paso 4. Verifique la conectividad.

Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 2001:DB8:ACAD:B::B/64.

¿Tuvieron éxito los pings? Si

Reflexión

1. ¿Por qué desactivaría la sumarización automática para RIPv6?

Para que los router no sumaricen, las rutas hacia la clase mayor y así puede haber continuidad entre redes discontinuas.

2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3?

— Aprendiero de las actualizaciones de rip recibidas desde el router donde fue configurada de la ruta por defecto, R2

3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPvng?

RIPv2 se configura notificando redes y RIPvng se configura con las interfaces

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

8.2.4.5 Práctica de laboratorio: configuración de OSPFv2 básico de área única

Topología

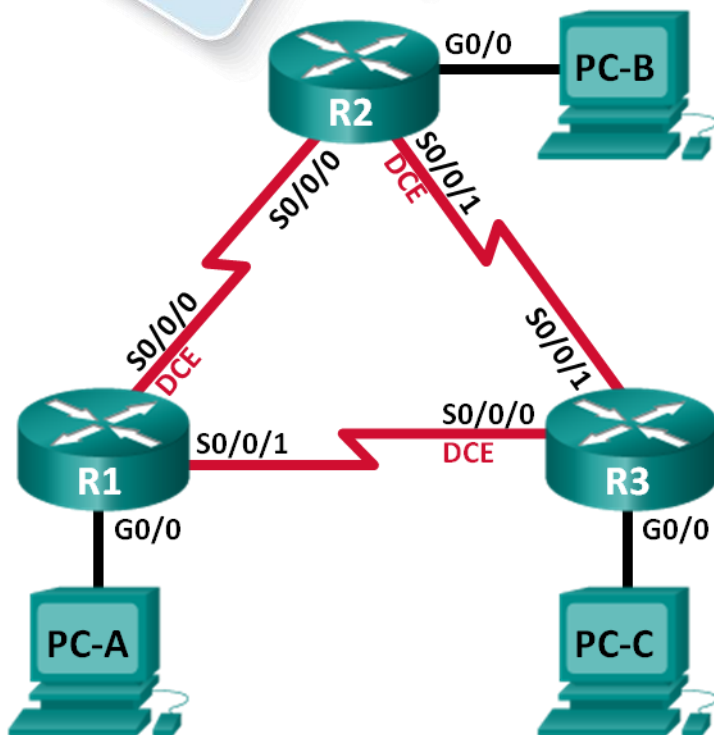


Tabla de direccionamiento

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 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	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

Objetivos

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

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6. OSPF detecta cambios en la topología, como fallas de enlace, y converge en una nueva estructura de routing sin bucles muy



rápidamente. Computa cada ruta con el algoritmo de Dijkstra, un algoritmo SPF (Shortest Path First).

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv2, cambiará las asignaciones de ID de router, configurará interfaces pasivas, ajustará las métricas de OSPF y utilizará varios comandos de CLI para ver y verificar la información de routing OSPF.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

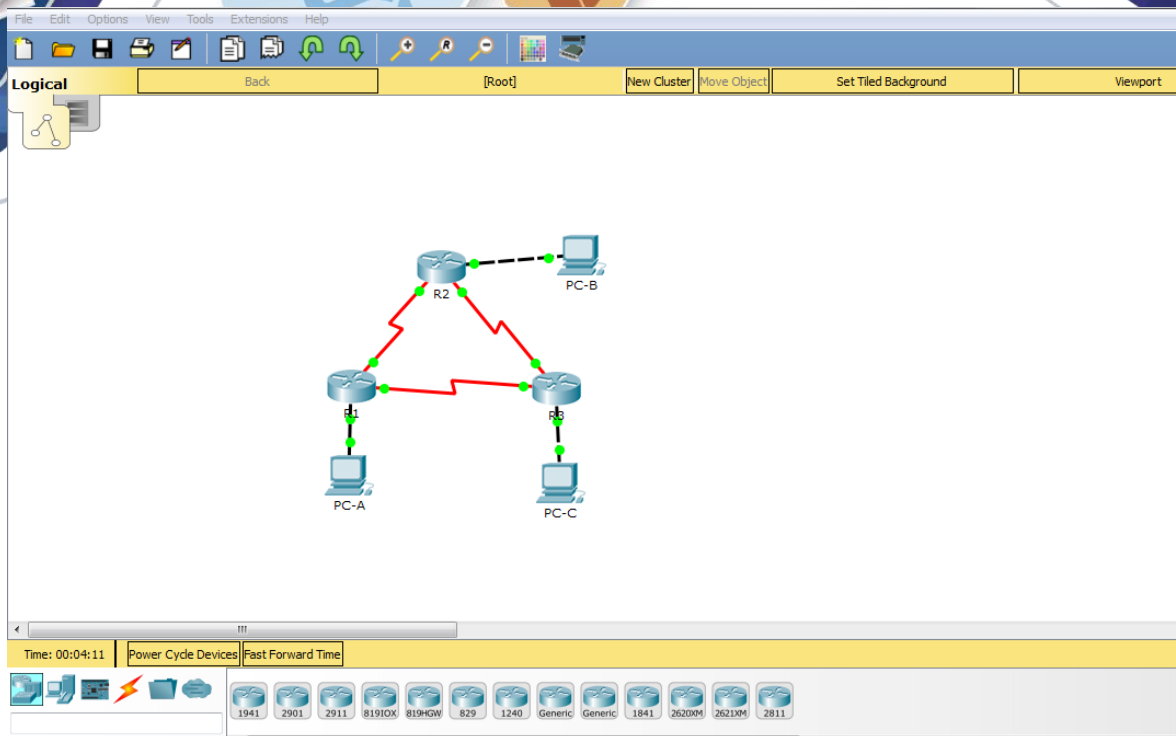
- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

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

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

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





Step 2: inicializar y volver a cargar los routers según sea necesario.

Step 3: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- f. Configure **logging synchronous** para la línea de consola.
- g. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.
- i. Copie la configuración en ejecución en la configuración de inicio

Step 4: configurar los equipos host.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
R1(config-if)#int s0/0/0
R1(config-if)#ip add 192.168.12.1 255.255.255.0
R1(config-if)#ip add 192.168.12.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#int s0/0/1
R1(config-if)#ip add 192.168.13.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#int s0/0/0
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
  
```

Copy Paste

Top

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "R2". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main content area displays the following commands and their outputs:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int g0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)#int s0/0/0
R2(config-if)#ip add 192.168.12.2 255.255.255.252
R2(config-if)#no shutdown

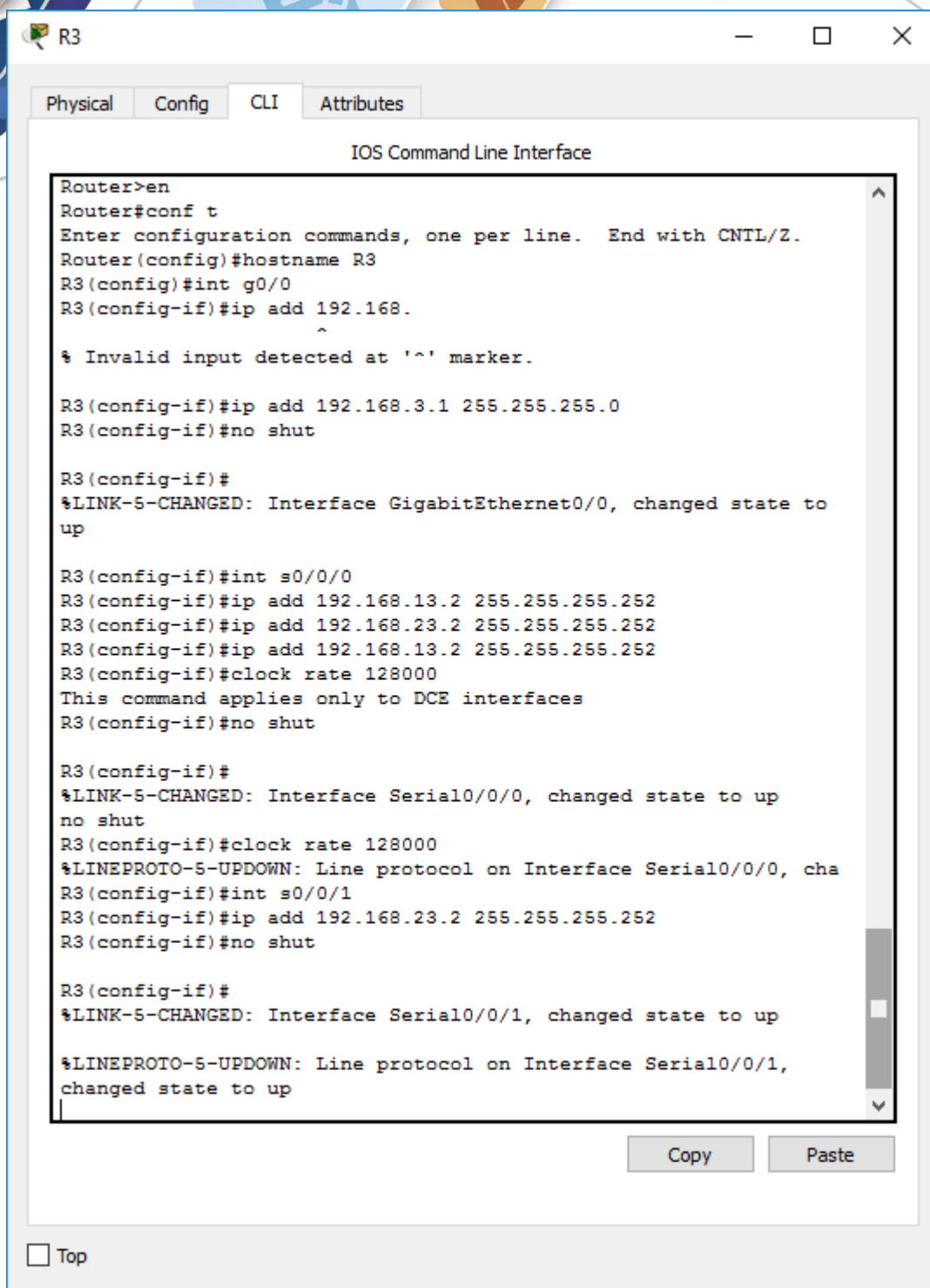
R2(config-if)#
%LINK-5-CHANGED: Interface Serial10/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/0,
changed state to up

R2(config-if)#int s0/0/1
R2(config-if)#ip add 192.168.23.1 255.255.255.252
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to down
R2(config-if)#
R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" button with a small square icon to its left.



```

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/0
R3(config-if)#ip add 192.168.
      ^
% Invalid input detected at '^' marker.

R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

R3(config-if)#int s0/0/0
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#ip add 192.168.23.2 255.255.255.252
R3(config-if)#ip add 192.168.13.2 255.255.255.252
R3(config-if)#clock rate 128000
This command applies only to DCE interfaces
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
no shut
R3(config-if)#clock rate 128000
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, cha
R3(config-if)#int s0/0/1
R3(config-if)#ip add 192.168.23.2 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
  
```

Copy Paste

Top

Step 5: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPF. Verifique y resuelva los problemas, si es necesario.

Part 2: Configurar y verificar el enrutamiento OSPF

En la parte 2, configurará el routing OSPFv2 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente. Después de verificar OSPF, configurará la autenticación de OSPF en los enlaces para mayor seguridad.

Step 1: Configure el protocolo OSPF en R1.

- a. Use el comando **router ospf** en el modo de configuración global para habilitar OSPF en el R1.

```
R1(config)# router ospf 1
```

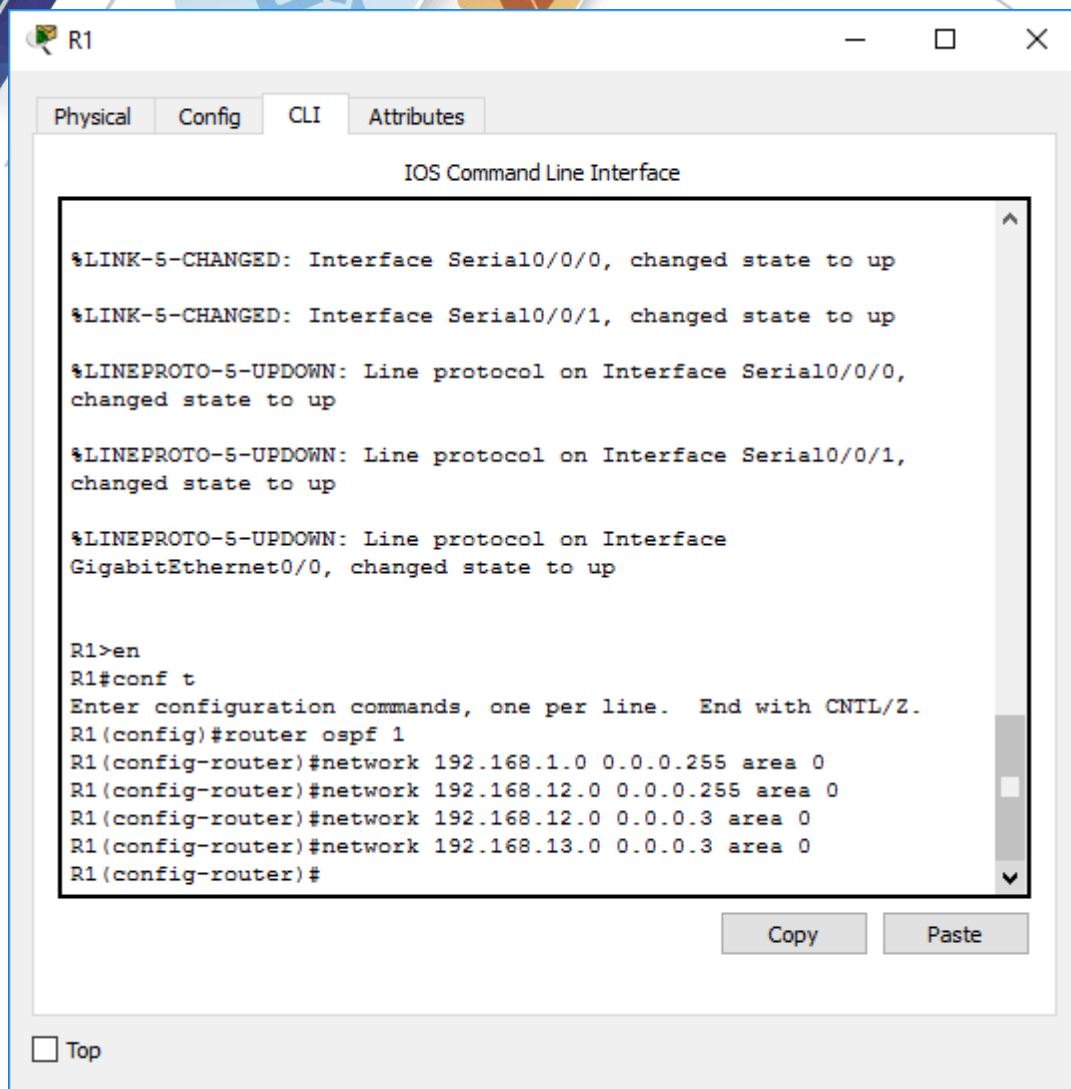
Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

- b. Configure las instrucciones **network** para las redes en el R1. Utilice la ID de área 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
```

```
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```



The screenshot shows a terminal window for router R1. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```

IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.3 area 0
R1(config-router)#network 192.168.13.0 0.0.0.3 area 0
R1(config-router)#
  
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

Step 2: Configure OSPF en el R2 y el R3.

Use el comando **router ospf** y agregue las instrucciones **network** para las redes en el R2 y el R3. Cuando el routing OSPF está configurado en el R2 y el R3, se muestran mensajes de adyacencia de vecino en el R1.

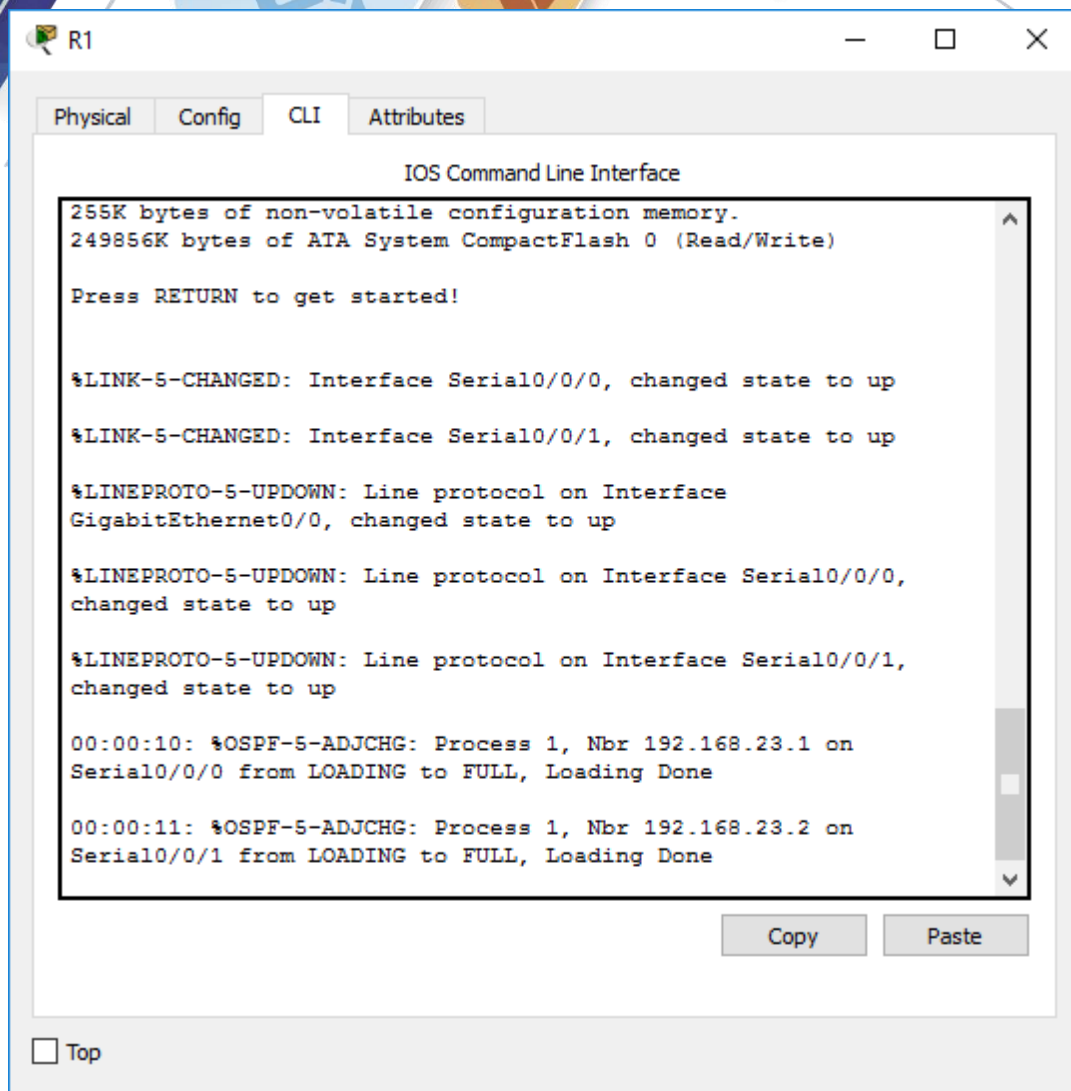
R1#

00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R1#

00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R1#



Step 3: verificar los vecinos OSPF y la información de routing.

- a. Emita el comando **show ip ospf neighbor** para verificar que cada router indique a los demás routers en la red como vecinos.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.23.2	0	FULL/ -	00:00:33	192.168.13.2	Serial0/0/1
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

00:00:11: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on
Serial0/0/1 from LOADING to FULL, Loading Done

R1>ENABLE
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
192.168.23.1	0	FULL/ -	00:00:30	192.168.12.2
192.168.23.2	0	FULL/ -	00:00:38	192.168.13.2

R1#

Copy Paste

Top

R2

Physical Config CLI Attributes

IOS Command Line Interface

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on
Serial0/0/1 from LOADING to FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2>en
R2#show ip ospf neighbor
  
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
192.168.13.1	0	FULL/ -	00:00:35	192.168.12.1
Serial0/0/0				
192.168.23.2	0	FULL/ -	00:00:35	192.168.23.2
Serial0/0/1				

R2#

Copy Paste

Top

```

R3
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on
Serial0/0/1 from LOADING to FULL, Loading Done

00:00:11: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3>en
R3#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.13.1     0    FULL/ -         00:00:35   192.168.13.1
Serial0/0/0
192.168.23.1     0    FULL/ -         00:00:32   192.168.23.1
Serial0/0/1
R3#
  
```

- b. Emita el comando **show ip route** para verificar que todas las redes aparezcan en la tabla de routing de todos los routers.

R1# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

- C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
- L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
- O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
- O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
- 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.12.0/30 is directly connected, Serial0/0/0
- L 192.168.12.1/32 is directly connected, Serial0/0/0
- 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.13.0/30 is directly connected, Serial0/0/1
- L 192.168.13.1/32 is directly connected, Serial0/0/1
- 192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
[110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

R1

Physical Config CLI Attributes

IOS Command Line Interface

```

Serial0/0/0
192.168.23.2    0    FULL/ -    00:00:38    192.168.13.2
Serial0/0/1
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 01:03:43,
Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 01:03:43,
Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 01:03:43,
Serial0/0/0
                               [110/128] via 192.168.13.2, 01:03:43,
Serial0/0/1

R1#
  
```

Copy Paste

Top

R2

Physical Config CLI Attributes

IOS Command Line Interface

```

192.168.23.2 0 FULL/ - 00:00:35 192.168.23.2
Serial0/0/1
R2#show ip route show ip route ^Z
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

O   192.168.1.0/24 [110/65] via 192.168.12.1, 01:04:58,
Serial0/0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.2.0/24 is directly connected, GigabitEthernet0/0
L   192.168.2.1/32 is directly connected, GigabitEthernet0/0
O   192.168.3.0/24 [110/65] via 192.168.23.2, 01:04:58,
Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/30 is directly connected, Serial0/0/0
L   192.168.12.2/32 is directly connected, Serial0/0/0
    192.168.13.0/30 is subnetted, 1 subnets
O   192.168.13.0/30 [110/128] via 192.168.23.2, 01:04:58,
Serial0/0/1
                                     [110/128] via 192.168.12.1, 01:04:58,
Serial0/0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.23.0/30 is directly connected, Serial0/0/1
L   192.168.23.1/32 is directly connected, Serial0/0/1

R2#
  
```

Copy Paste

Top

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
Serial0/0/0
192.168.23.1 0 FULL/ - 00:00:32 192.168.23.1
Serial0/0/1
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.1.0/24 [110/65] via 192.168.13.1, 01:05:11,
Serial0/0/0
O 192.168.2.0/24 [110/65] via 192.168.23.1, 01:05:21,
Serial0/0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0
L 192.168.3.1/32 is directly connected, GigabitEthernet0/0
192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0/30 [110/128] via 192.168.13.1, 01:05:11,
Serial0/0/0
[110/128] via 192.168.23.1, 01:05:11,
Serial0/0/1
192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.13.0/30 is directly connected, Serial0/0/0
L 192.168.13.2/32 is directly connected, Serial0/0/0
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.23.0/30 is directly connected, Serial0/0/1
L 192.168.23.2/32 is directly connected, Serial0/0/1
R3#
Copy Paste
 Top
  
```

¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

Step 4: verificar la configuración del protocolo OSPF.

El comando **show ip protocols** es una manera rápida de verificar información fundamental de configuración de OSPF. Esta información incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 192.168.13.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
192.168.1.0 0.0.0.255 area 0
```

```
192.168.12.0 0.0.0.3 area 0
```

```
192.168.13.0 0.0.0.3 area 0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update
192.168.23.2	110	00:19:16
192.168.23.1	110	00:20:03

```
Distance: (default is 110)
```

The screenshot shows a Cisco IOS Command Line Interface window for router R1. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the output of the 'show ip protocols' command. The output shows that OSPF is configured with ID 192.168.13.1, and lists the networks in area 0 along with their routing information sources.

```

R1# show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1     110          00:09:29
    192.168.23.1     110          00:09:29
    192.168.23.2     110          00:09:30
  Distance: (default is 110)

R1#
  
```

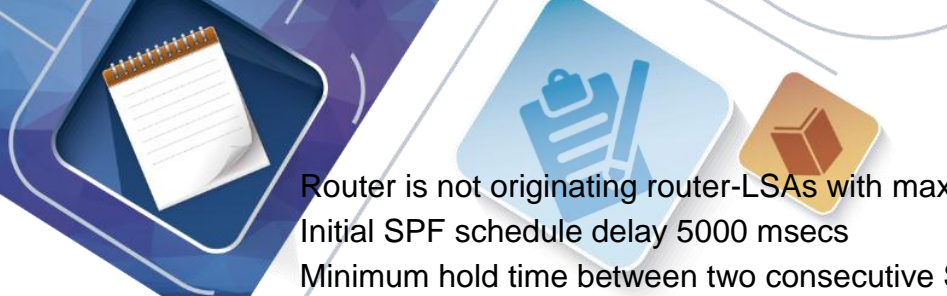
Step 5: verificar la información del proceso OSPF.

Use el comando **show ip ospf** para examinar la ID del proceso OSPF y la ID del router. Este comando muestra información de área OSPF y la última vez que se calculó el algoritmo SPF.

R1# **show ip ospf**

```


Routing Process "ospf 1" with ID 192.168.13.1
Start time: 00:20:23.260, Time elapsed: 00:25:08.296
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  
```



Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 sec
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 sec
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:22:53.756 ago
SPF algorithm executed 7 times
Area ranges are
Number of LSA 3. Checksum Sum 0x019A61
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0



```

R1#show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x00b0a6
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R1#
  
```

Step 6: verificar la configuración de la interfaz OSPF.

- a. Emita el comando **show ip ospf interface brief** para ver un resumen de las interfaces con OSPF habilitado.

```

R1# show ip ospf interface brief
Interface  PID  Area      IP Address/Mask  Cost  State  Nbrs F/C
Se0/0/1   1    0         192.168.13.1/30  64    P2P    1/1
Se0/0/0   1    0         192.168.12.1/30  64    P2P    1/1
Gi0/0     1    0         192.168.1.1/24   1     DR     0/0
  
```

- b. Para obtener una lista detallada de todas las interfaces con OSPF habilitado, emita el comando **show ip ospf interface**.

```

R1# show ip ospf interface
Serial0/0/1 is up, line protocol is up
  
```

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
 Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT,
 Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 oob-resync timeout 40
 Hello due in 00:00:01

Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 3/3, flood queue length 0
 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
 Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT,
 Cost: 64

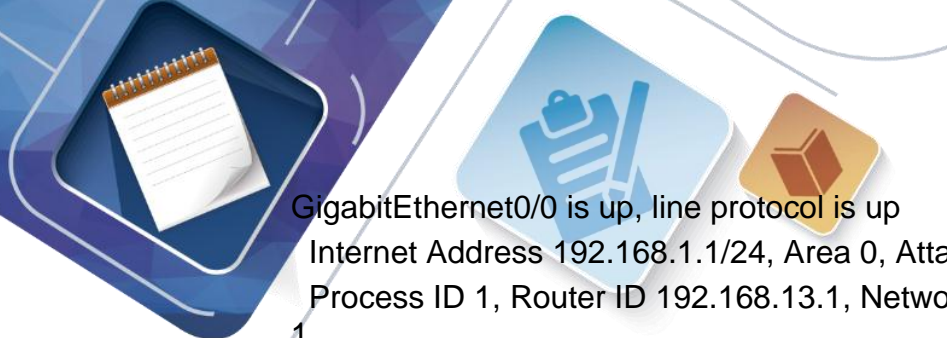
Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 oob-resync timeout 40
 Hello due in 00:00:03

Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 192.168.23.1

Suppress hello for 0 neighbor(s)



GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost:
1

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	1	no	no	Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40

Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0


Next 0x0(0)/0x0(0)

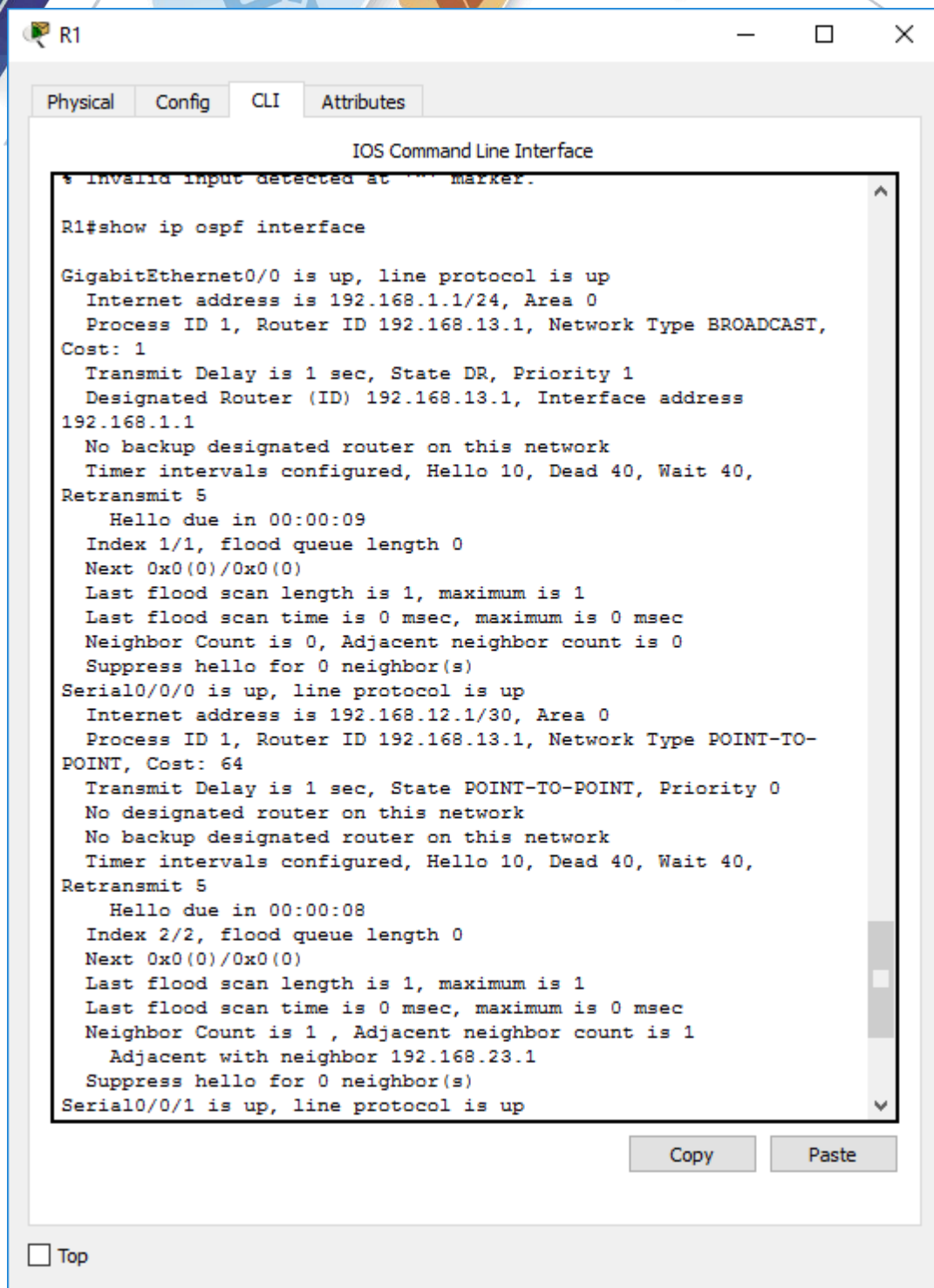
Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)





```

R1
Physical Config CLI Attributes
IOS Command Line Interface
* Invalid input detected at ... marker.

R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.13.1, Interface address
192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 192.168.13.1, Network Type POINT-TO-
POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:08
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.1
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  
```

Copy Paste

Top

Step 7: Verificar la conectividad de extremo a extremo.

Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

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

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
  
```

Part 3: cambiar las asignaciones de ID del router

El ID del router OSPF se utiliza para identificar de forma única el router en el dominio de enrutamiento OSPF. Los routers Cisco derivan la ID del router en una de estas tres formas y con la siguiente prioridad:

- 1) Dirección IP configurada con el comando de OSPF **router-id**, si la hubiera
- 2) Dirección IP más alta de cualquiera de las direcciones de loopback del router, si la hubiera
- 3) Dirección IP activa más alta de cualquiera de las interfaces físicas del router

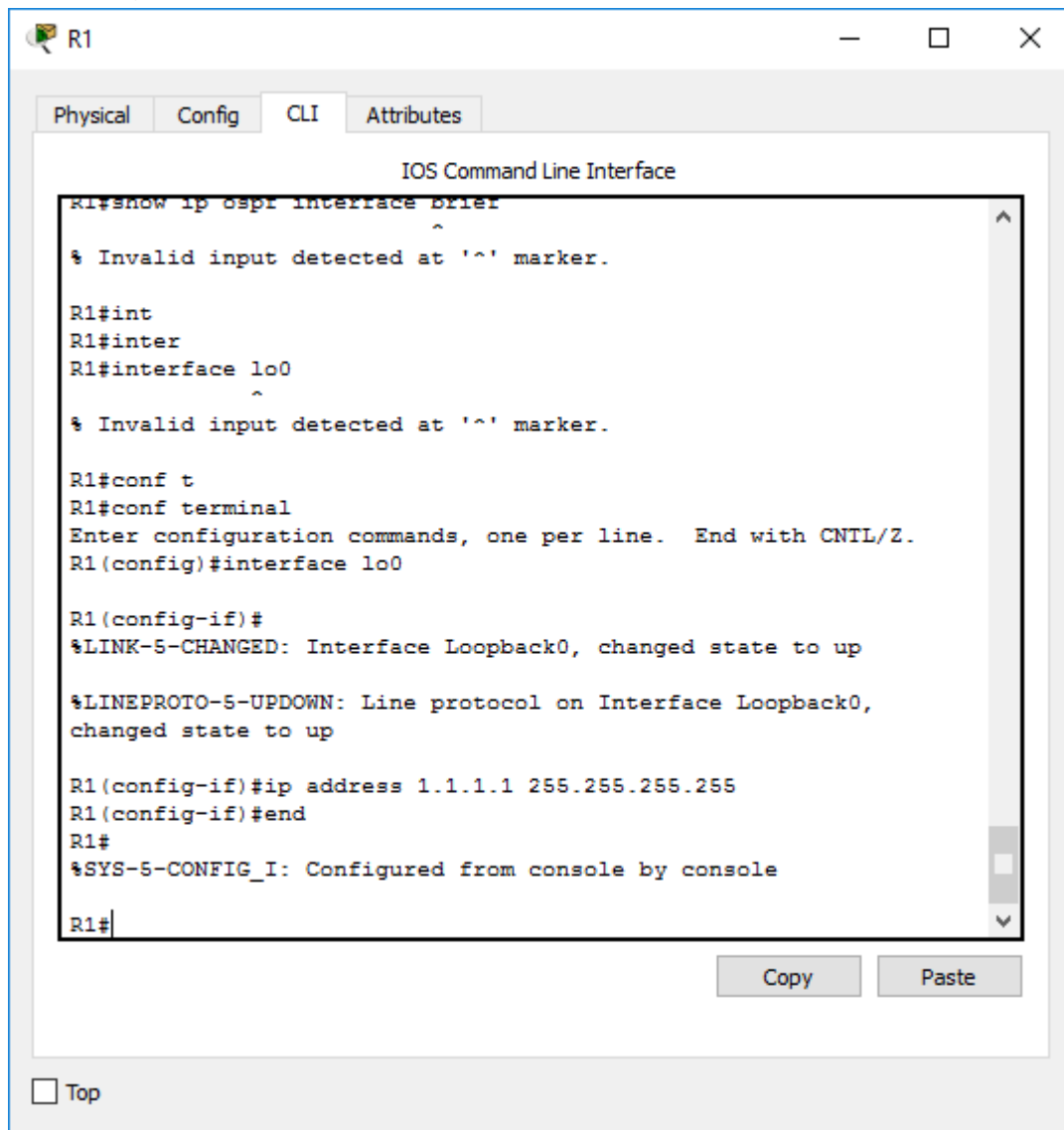
Dado que no se ha configurado ningún ID o interfaz de loopback en los tres routers, el ID de router para cada ruta se determina según la dirección IP más alta de cualquier interfaz activa.

En la parte 3, cambiará la asignación de ID del router OSPF con direcciones de loopback. También usará el comando **router-id** para cambiar la ID del router.

Step 1: Cambie las ID de router con direcciones de loopback.

- a. Asigne una dirección IP al loopback 0 en el R1.

```
R1(config)# interface lo0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```



- b. Asigne direcciones IP al loopback 0 en el R2 y el R3. Utilice la dirección IP 2.2.2.2/32 para el R2 y 3.3.3.3/32 para el R3.

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface lo0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

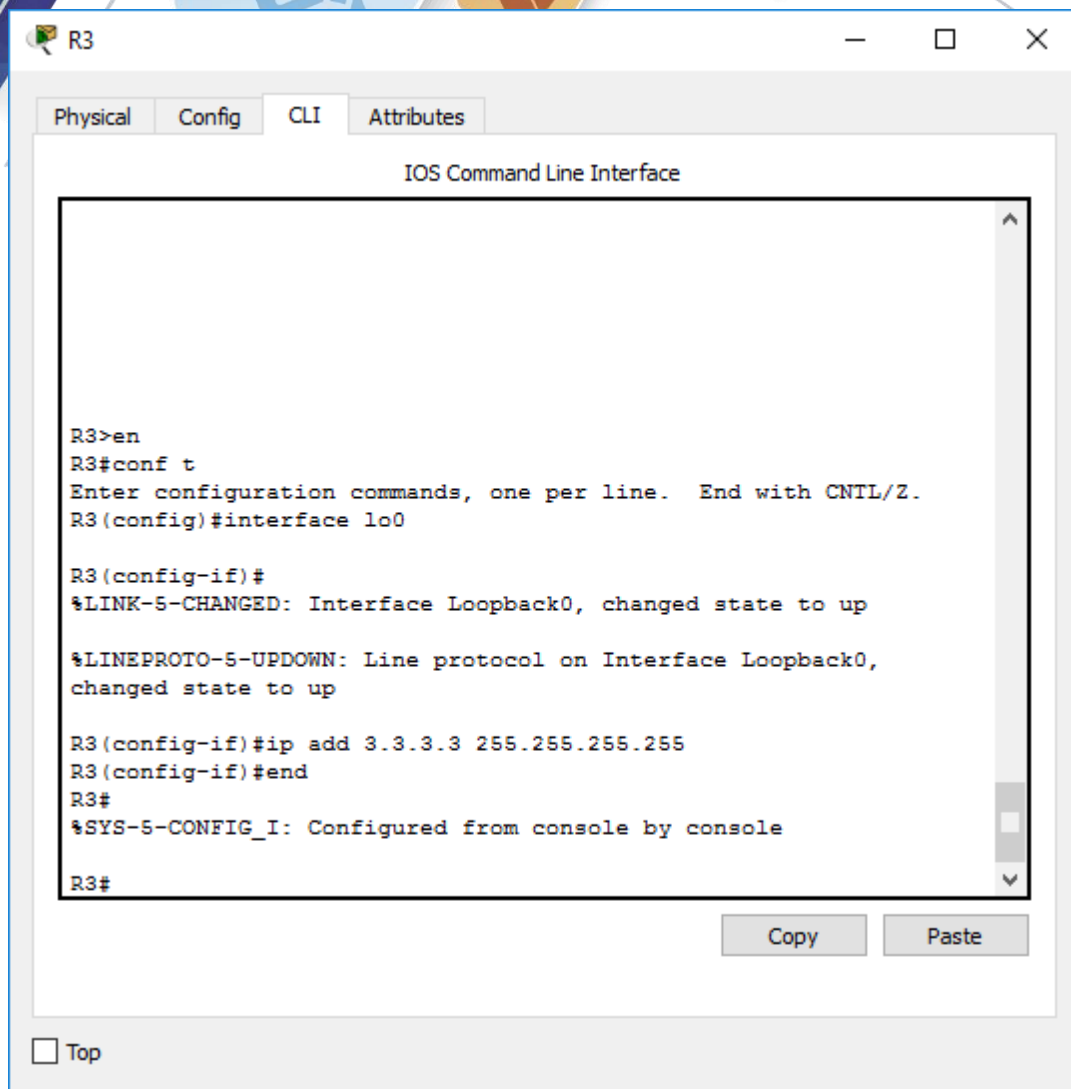
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

R2(config-if)#ip add 1.1.1.1 255.255.255.255
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```

Copy Paste

Top



The screenshot shows a window titled 'R3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface lo0

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

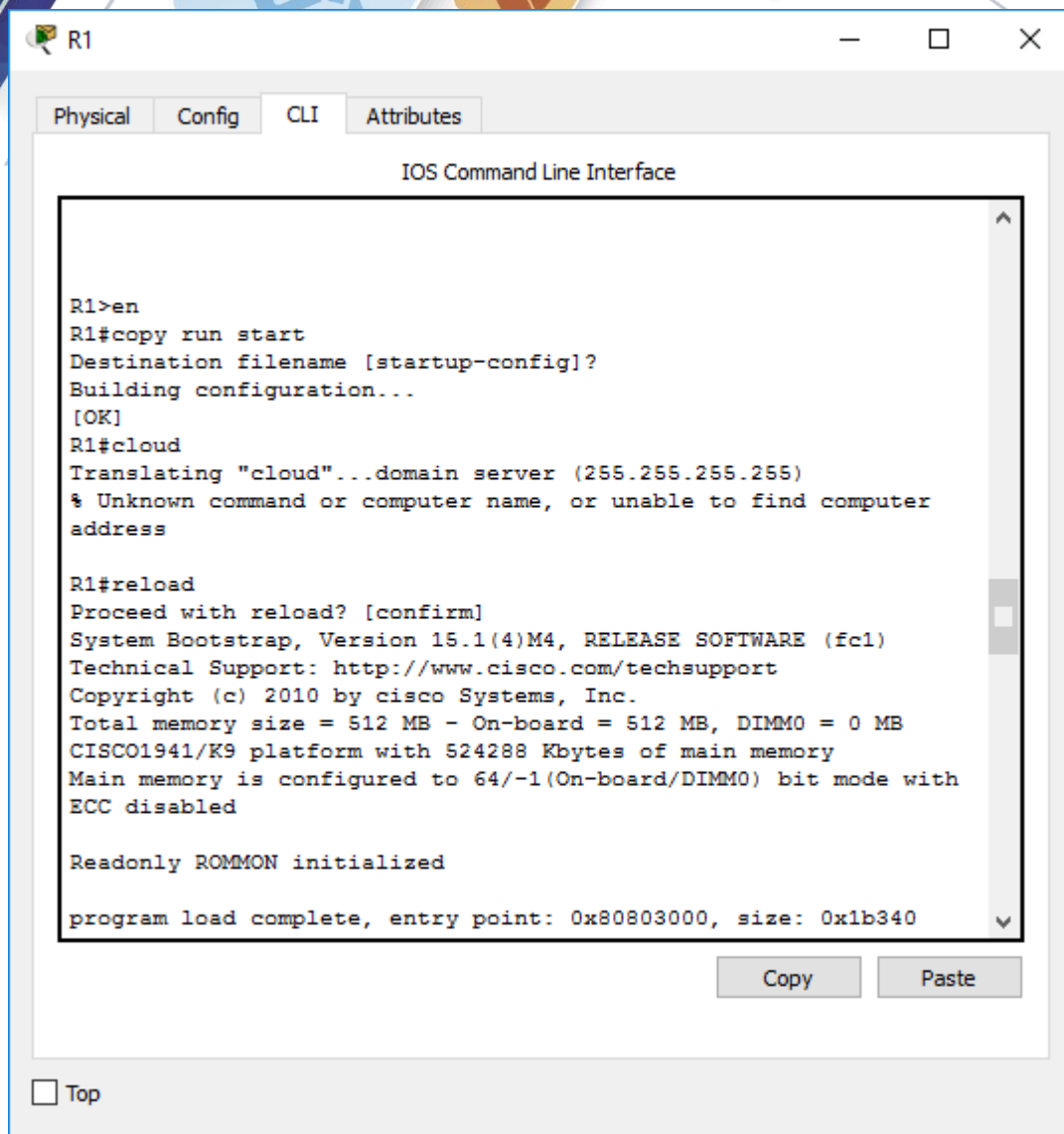
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

R3(config-if)#ip add 3.3.3.3 255.255.255.255
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with an unchecked checkbox.

- c. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.



The screenshot shows a terminal window for a Cisco router named 'R1'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The title bar reads 'R1'. The main content area is titled 'IOS Command Line Interface' and contains the following text:

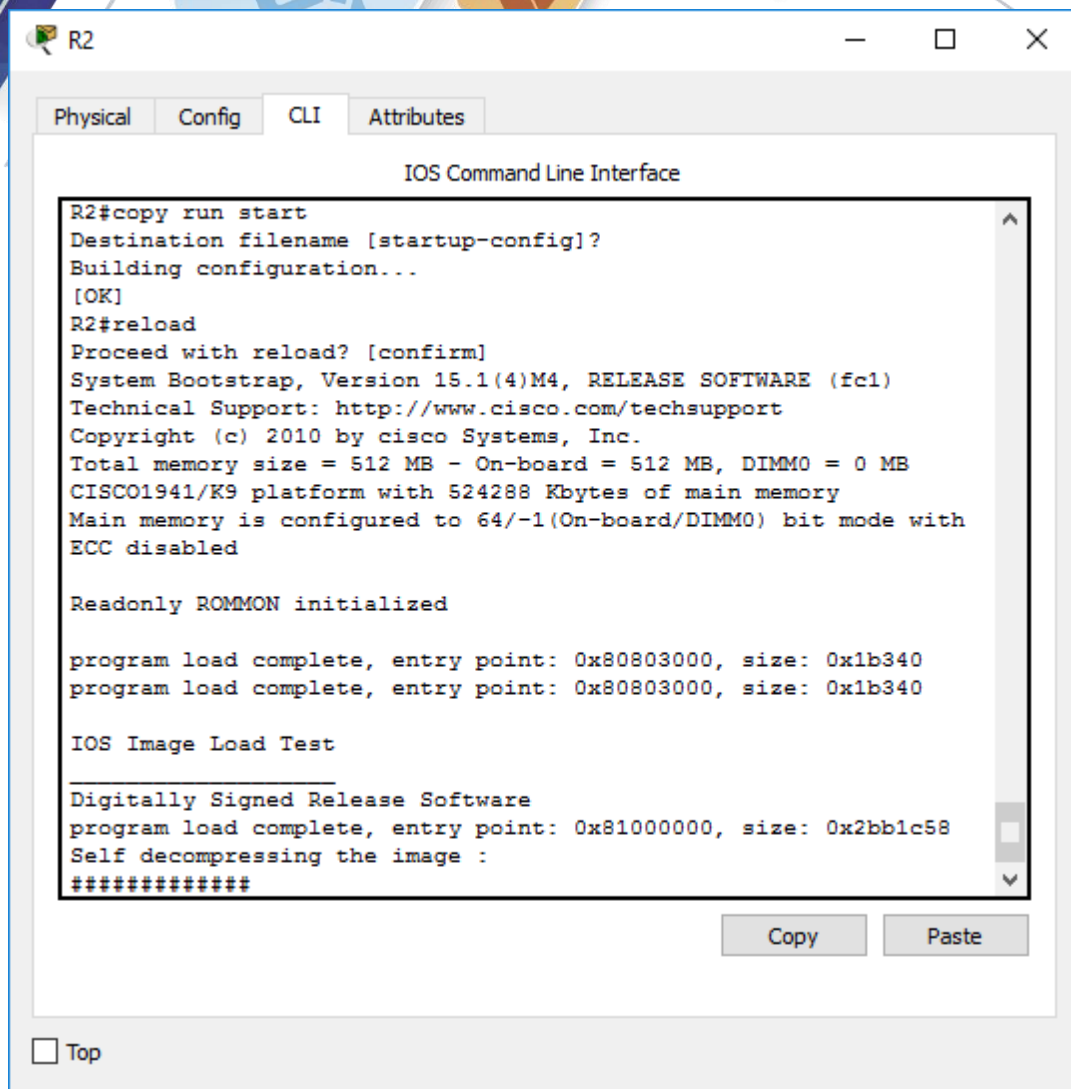
```
R1>en
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#cloud
Translating "cloud"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
```

At the bottom of the terminal area, there are 'Copy' and 'Paste' buttons. Below the terminal area, there is a checkbox labeled 'Top' which is currently unchecked.



The screenshot shows a terminal window for a Cisco router named 'R2'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The title bar reads 'R2'. The main content area is titled 'IOS Command Line Interface' and contains the following text:

```
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
*****
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with an unchecked checkbox.

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#####
Copy Paste
 Top

```

- d. Debe volver a cargar los routers para restablecer la ID del router a la dirección de loopback. Emita el comando **reload** en los tres routers. Presione Enter para confirmar la recarga.
- e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

3.3.3.3	110	00:01:00
---------	-----	----------

2.2.2.2	110	00:01:14
---------	-----	----------

Distance: (default is 110)

R1

Physical Config CLI Attributes

IOS Command Line Interface

00:11:30: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done

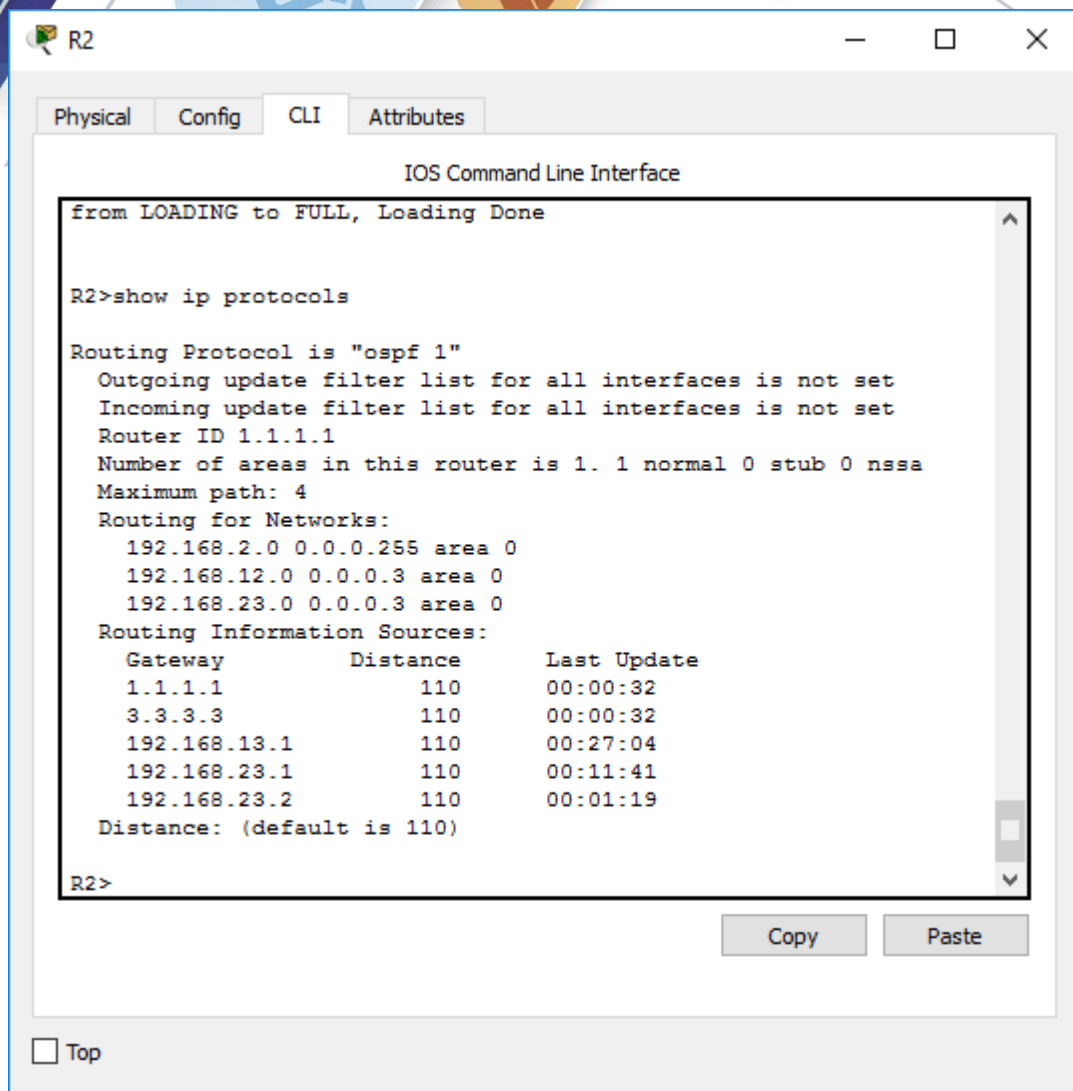
R1>show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.1.0 0.0.0.255 area 0
192.168.12.0 0.0.0.255 area 0
192.168.12.0 0.0.0.3 area 0
192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:00:06
3.3.3.3 110 00:00:06
192.168.13.1 110 00:26:38
192.168.23.1 110 00:11:15
192.168.23.2 110 00:00:53
Distance: (default is 110)

R1>

Copy Paste

Top



The screenshot shows a Cisco IOS CLI window titled "R2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The output of the command "show ip protocols" is shown in a scrollable text area. The output indicates that OSPF is running on the router with Router ID 1.1.1.1, 4 areas, and four information sources. Below the text area are "Copy" and "Paste" buttons, and a "Top" button at the bottom left.

```
from LOADING to FULL, Loading Done

R2>show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:32
    3.3.3.3          110          00:00:32
    192.168.13.1     110          00:27:04
    192.168.23.1     110          00:11:41
    192.168.23.2     110          00:01:19
  Distance: (default is 110)

R2>
```

```

R3>show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.0 0.0.0.255 area 0
    192.168.13.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:51
    3.3.3.3          110          00:00:51
    192.168.13.1    110          00:27:23
    192.168.23.1    110          00:12:00
    192.168.23.2    110          00:01:38
  Distance: (default is 110)

R3>
  
```

- f. Emita el comando **show ip ospf neighbor** para mostrar los cambios de ID de router de los routers vecinos.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

R1#

R1

Physical Config CLI Attributes

IOS Command Line Interface

```

Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  192.168.1.0 0.0.0.255 area 0
  192.168.12.0 0.0.0.255 area 0
  192.168.12.0 0.0.0.3 area 0
  192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
  Gateway          Distance      Last Update
  1.1.1.1           110          00:00:06
  3.3.3.3           110          00:00:06
  192.168.13.1     110          00:26:38
  192.168.23.1     110          00:11:15
  192.168.23.2     110          00:00:53
  Distance: (default is 110)

R1>show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
1.1.1.1          0    EXSTART/ -      00:00:32   192.168.12.2
Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:31   192.168.13.2
Serial0/0/1
R1>
  
```

Copy Paste

Top

R2

Physical Config CLI Attributes

IOS Command Line Interface

```

Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.2.0 0.0.0.255 area 0
 192.168.12.0 0.0.0.3 area 0
 192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway      Distance    Last Update
 1.1.1.1      110        00:00:32
 3.3.3.3      110        00:00:32
 192.168.13.1 110        00:27:04
 192.168.23.1 110        00:11:41
 192.168.23.2 110        00:01:19
Distance: (default is 110)

R2>show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address
Interface
1.1.1.1        0   EXSTART/ -      00:00:30   192.168.12.1
Serial0/0/0
3.3.3.3        0   FULL/ -         00:00:32   192.168.23.2
Serial0/0/1
R2>
  
```

Copy Paste

Top

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.3.0 0.0.0.255 area 0
 192.168.13.0 0.0.0.3 area 0
 192.168.23.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway      Distance    Last Update
 1.1.1.1      110        00:00:51
 3.3.3.3      110        00:00:51
 192.168.13.1 110        00:27:23
 192.168.23.1 110        00:12:00
 192.168.23.2 110        00:01:38
Distance: (default is 110)

R3>show ip ospf neighbor

Neighbor ID   Pri  State           Dead Time   Address
Interface
1.1.1.1       0    FULL/ -         00:00:34   192.168.13.1
Serial0/0/0
1.1.1.1       0    FULL/ -         00:00:34   192.168.23.1
Serial0/0/1
R3>
  
```

Step 2: cambiar la ID del router R1 con el comando router-id.

El método de preferencia para establecer la ID del router es mediante el comando **router-id**.

- a. Emita el comando **router-id 11.11.11.11** en el R1 para reasignar la ID del router. Observe el mensaje informativo que aparece al emitir el comando **router-id**.

R1(config)# **router ospf 1**

R1(config-router)# **router-id 11.11.11.11**

Reload or use "clear ip ospf process" command, for this to take effect

R1(config)# **end**

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id
% Incomplete command.
R1(config-router)#router-id 11.11.11.11
R1(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect

R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
c
% Ambiguous command: "c"
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R1#
00:28:14: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from EXSTART to DOWN, Neighbor Down: Adjacency forced to reset

00:28:14: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from EXSTART to DOWN, Neighbor Down: Interface down or detached

00:28:14: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:28:14: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached

R1#
00:28:25: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

R1#
Copy Paste
 Top

```

- b. Recibirá un mensaje informativo en el que se le indique que debe volver a cargar el router o usar el comando **clear ip ospf process** para que se aplique el cambio. Emita el comando **clear ip ospf process** en los tres routers. Escriba **yes** (sí) como respuesta al mensaje de verificación de restablecimiento y presione Enter.

- c. Establezca la ID del router R2 **22.22.22.22** y la ID del router R3 **33.33.33.33**. Luego, use el comando **clear ip ospf process** para restablecer el proceso de routing de OSPF.

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 22.22.22.22
R2(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect

R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R2#
00:19:29: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:19:29: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

00:19:29: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:19:29: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached

R2#|
```

Copy Paste

Top

The screenshot shows a Cisco IOS Command Line Interface window for router R3. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```

R3>
00:19:01: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on
Serial0/0/1 from LOADING to FULL, Loading Done
en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 33.33.33.33
R3(config-router)#Reload or use "clear ip ospf process" command,
for this to take effect

R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R3#
00:19:53: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:19:53: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

00:19:53: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Adjacency forced to
reset

00:19:53: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached

R3#
  
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

- d. Emita el comando **show ip protocols** para verificar que la ID del router R1 haya cambiado.

R1# **show ip protocols**

*** IP Routing is NSF aware ***



Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 11.11.11.11

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
33.33.33.33	110	00:00:19
22.22.22.22	110	00:00:31
3.3.3.3	110	00:00:41
2.2.2.2	110	00:00:41

Distance: (default is 110)



```

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:20:47
    3.3.3.3          110          00:02:10
    11.11.11.11     110          00:01:10
    22.22.22.22     110          00:01:10
    33.33.33.33     110          00:01:10
    192.168.13.1    110          00:47:19
    192.168.23.1    110          00:31:56
    192.168.23.2    110          00:21:34
  Distance: (default is 110)

R1#
  
```

- e. Emita el comando **show ip ospf neighbor** en el R1 para verificar que se muestren las nuevas ID de los routers R2 y R3.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

The screenshot shows a Cisco IOS CLI window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The main content is the 'IOS Command Line Interface' showing the following text:

```

maximum path: 4
Routing for Networks:
 192.168.1.0 0.0.0.255 area 0
 192.168.12.0 0.0.0.255 area 0
 192.168.12.0 0.0.0.3 area 0
 192.168.13.0 0.0.0.3 area 0
Routing Information Sources:
 Gateway         Distance      Last Update
 1.1.1.1          110           00:20:47
 3.3.3.3          110           00:02:10
11.11.11.11       110           00:01:10
22.22.22.22       110           00:01:10
33.33.33.33       110           00:01:10
192.168.13.1      110           00:47:19
192.168.23.1      110           00:31:56
192.168.23.2      110           00:21:34
Distance: (default is 110)

R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
22.22.22.22     0    FULL/ -         00:00:36   192.168.12.2
Serial0/0/0
33.33.33.33     0    FULL/ -         00:00:35   192.168.13.2
Serial0/0/1
R1#

```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

Part 4: configurar las interfaces pasivas de OSPF

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 4, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPF para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 1: configurar una interfaz pasiva.

- a. Emita el comando **show ip ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo.

Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.

R1# **show ip ospf interface g0/0**

```
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0      1    no     no      Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

The screenshot shows a Cisco IOS CLI window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show ip ospf neighbor', which returns the following output:

```
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
22.22.22.22     0    FULL/ -         00:00:36   192.168.12.2
Serial0/0/0
33.33.33.33     0    FULL/ -         00:00:35   192.168.13.2
Serial0/0/1
R1#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:03
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R1#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

- b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```


- c. Vuelva a emitir el comando **show ip ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

```
R1# show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
 Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
 Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
 Topology-MTID  Cost  Disabled  Shutdown  Topology Name
 0          1    no       no       Base
```




Transmit Delay is 1 sec, State DR, Priority 1



Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1

No backup designated router on this network



Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40

No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0


Next 0x0(0)/0x0(0)

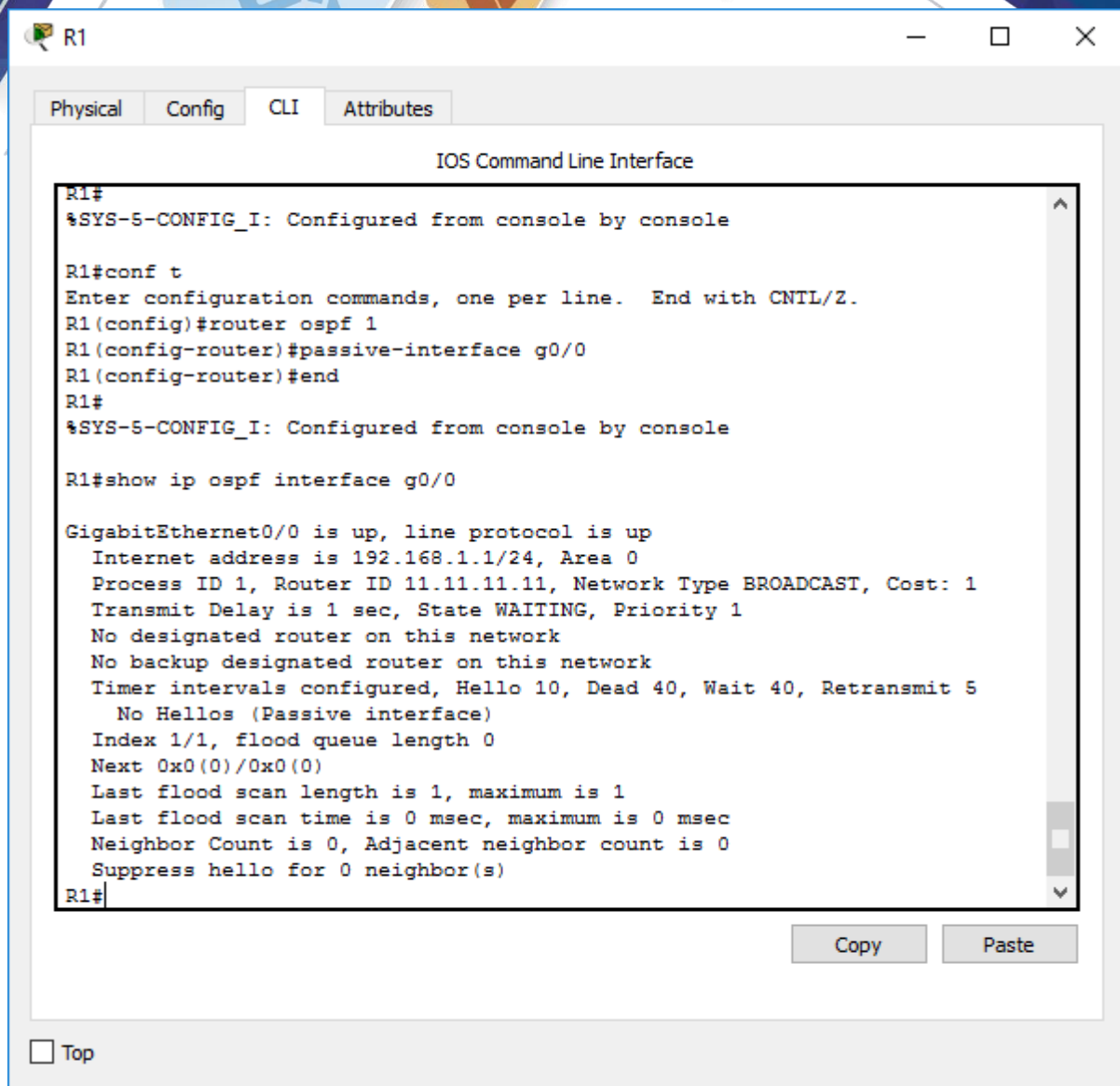
Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)





```

R1
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
  
```

- d. Emita el comando **show ip route** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 192.168.1.0/24.

R2# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override



Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets

C 2.2.2.2 is directly connected, Loopback0

O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, GigabitEthernet0/0

L 192.168.2.1/32 is directly connected, GigabitEthernet0/0

O 192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/30 is directly connected, Serial0/0/0

L 192.168.12.2/32 is directly connected, Serial0/0/0

192.168.13.0/30 is subnetted, 1 subnets

O 192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
[110/128] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/30 is directly connected, Serial0/0/1

L 192.168.23.1/32 is directly connected, Serial0/0/1



R2

Physical Config CLI Attributes

IOS Command Line Interface

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

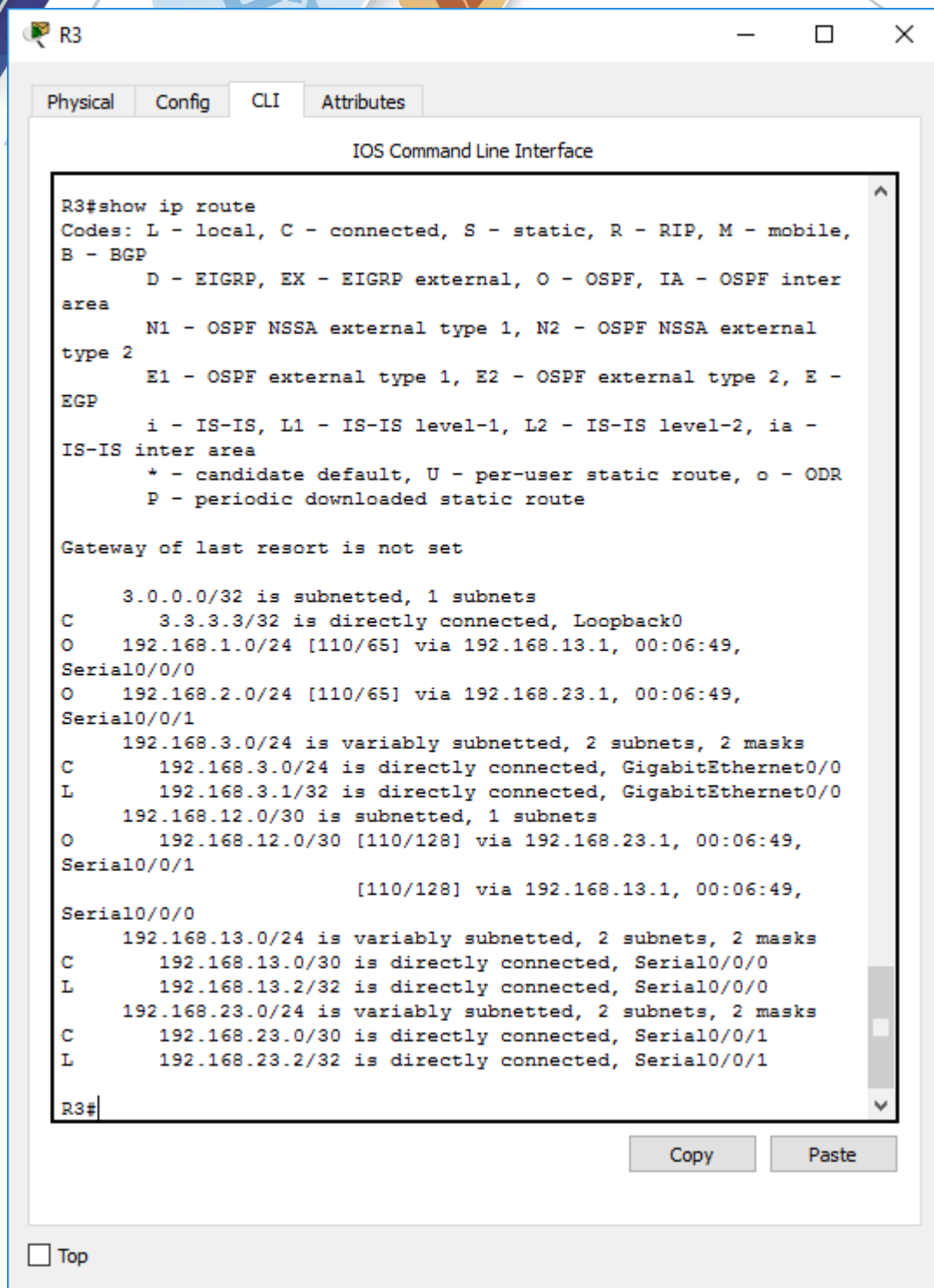
Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
O       192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:26,
Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/65] via 192.168.23.2, 00:05:21,
Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0/30 [110/128] via 192.168.12.1, 00:06:26,
Serial0/0/0
                                      [110/128] via 192.168.23.2, 00:06:26,
Serial0/0/1
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1

R2#
  
```

Copy Paste

Top



```

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

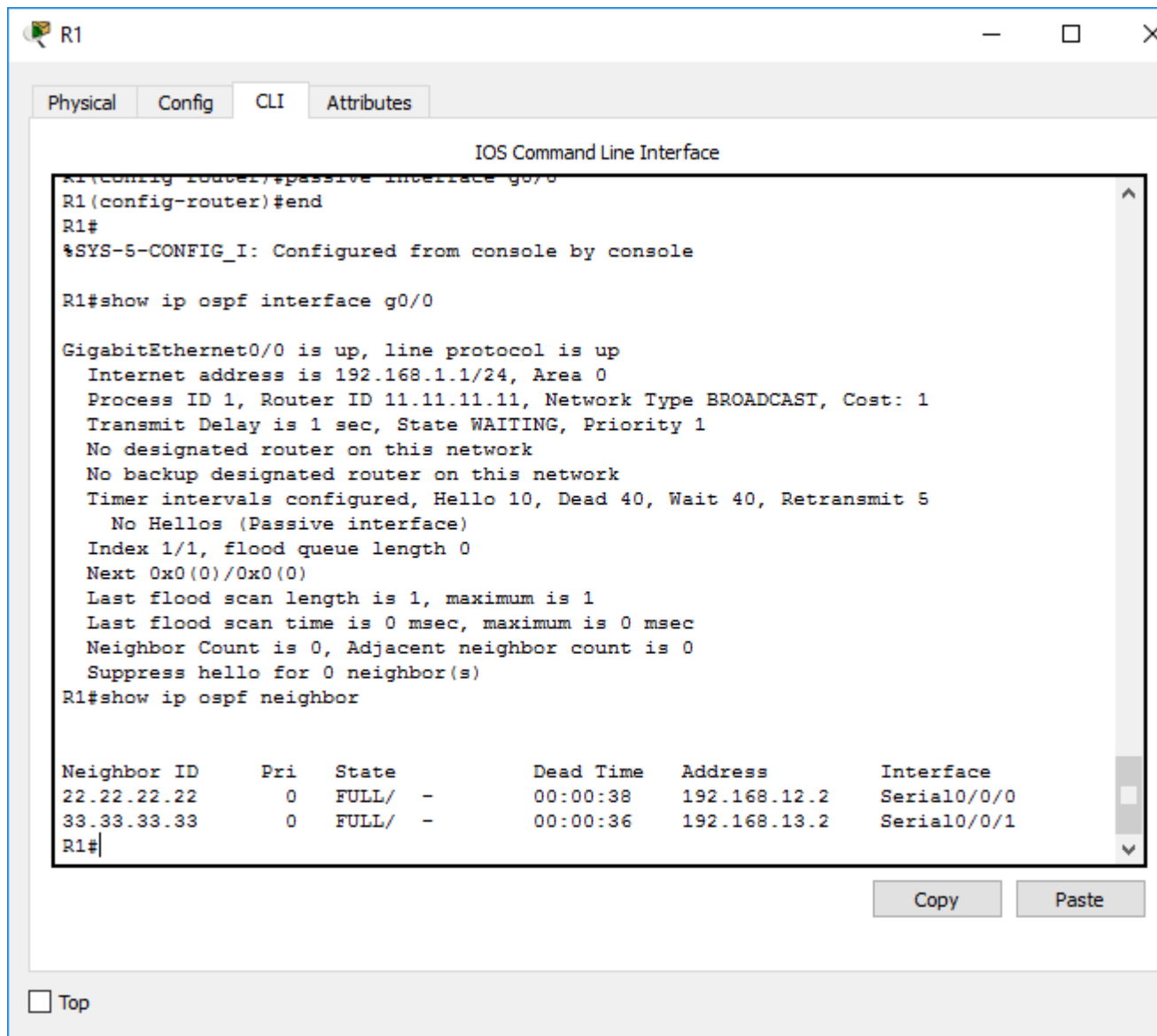
      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3/32 is directly connected, Loopback0
O   192.168.1.0/24 [110/65] via 192.168.13.1, 00:06:49,
Serial0/0/0
O   192.168.2.0/24 [110/65] via 192.168.23.1, 00:06:49,
Serial0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
      192.168.12.0/30 is subnetted, 1 subnets
O   192.168.12.0/30 [110/128] via 192.168.23.1, 00:06:49,
Serial0/0/1
                               [110/128] via 192.168.13.1, 00:06:49,
Serial0/0/0
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/30 is directly connected, Serial0/0/0
L        192.168.13.2/32 is directly connected, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.23.0/30 is directly connected, Serial0/0/1
L        192.168.23.2/32 is directly connected, Serial0/0/1
R3#
  
```

Step 2: establecer la interfaz pasiva como la interfaz predeterminada en un router.

- a. Emita el comando **show ip ospf neighbor** en el R1 para verificar que el R2 aparezca como un vecino OSPF.

R1# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0



IOS Command Line Interface

```

R1(config-router)#passive interface g0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
22.22.22.22     0    FULL/ -         00:00:38   192.168.12.2 Serial0/0/0
33.33.33.33     0    FULL/ -         00:00:36   192.168.13.2 Serial0/0/1
R1#
  
```

- b. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPF como pasivas de manera predeterminada.

R2(config)# router ospf 1

R2(config-router)# passive-interface default

R2(config-router)#

*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

R2
— □ ×

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
C    1.1.1.1/32 is directly connected, Loopback0
O    192.168.1.0/24 [110/65] via 192.168.12.1, 00:06:26, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/0
L    192.168.2.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.23.2, 00:05:21, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.2/32 is directly connected, Serial0/0/0
     192.168.13.0/30 is subnetted, 1 subnets
O    192.168.13.0/30 [110/128] via 192.168.12.1, 00:06:26, Serial0/0/0
     [110/128] via 192.168.23.2, 00:06:26, Serial0/0/1
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.1/32 is directly connected, Serial0/0/1

R2#router ospf 1
^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#passive-interface default
R2(config-router)#
00:28:16: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:28:16: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

R2(config-router)#

```

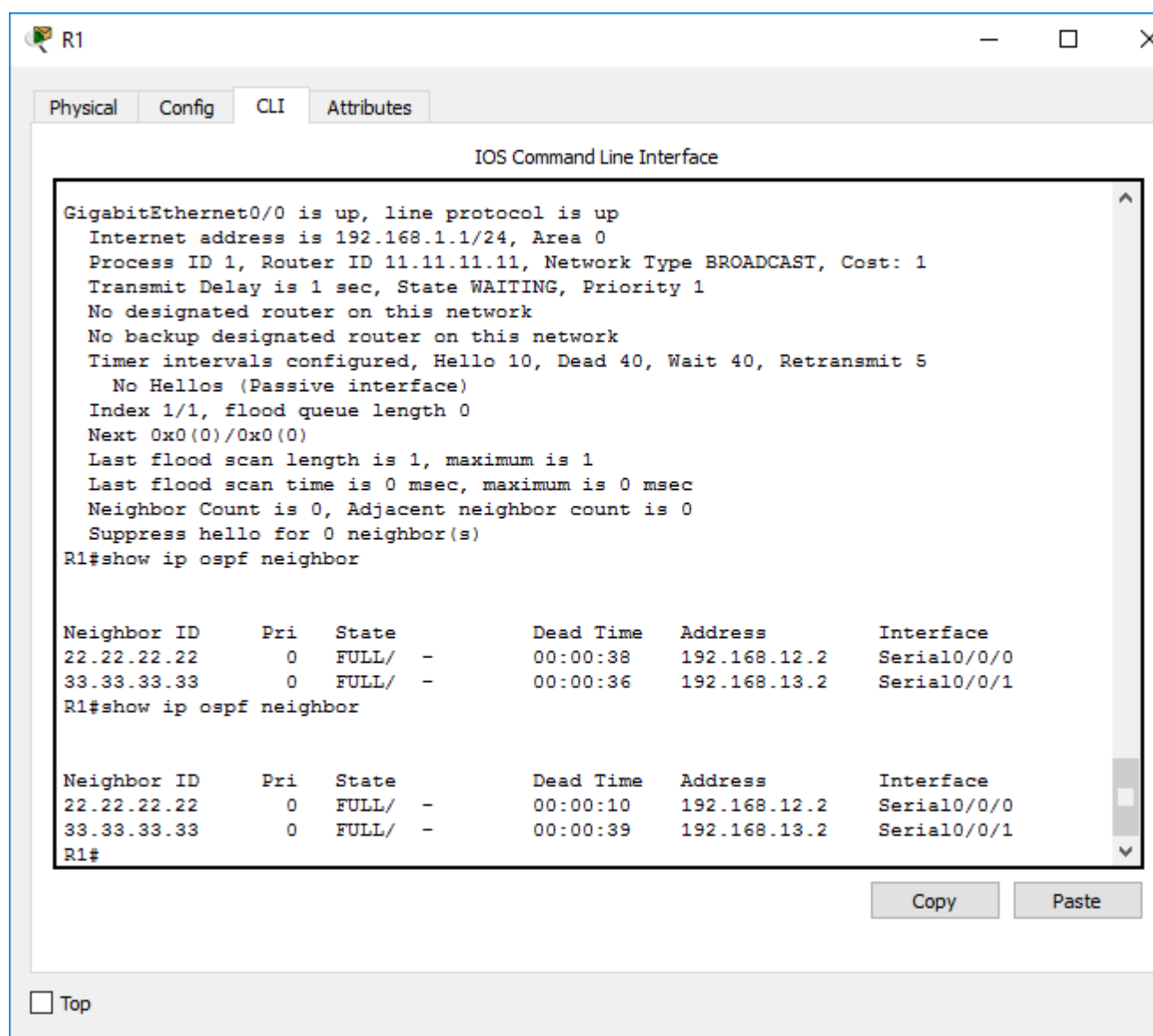
Copy
Paste

Top

- c. Vuelva a emitir el comando **show ip ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto haya caducado, el R2 ya no se mostrará como un vecino OSPF.

R1# **show ip ospf neighbor**

```
Neighbor ID   Pri  State           Dead Time  Address      Interface
33.33.33.33   0    FULL/ -         00:00:34  192.168.13.2 Serial0/0/1
```



IOS Command Line Interface

```
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R1#show ip ospf neighbor

Neighbor ID   Pri  State           Dead Time  Address      Interface
22.22.22.22   0    FULL/ -         00:00:38  192.168.12.2 Serial0/0/0
33.33.33.33   0    FULL/ -         00:00:36  192.168.13.2 Serial0/0/1
R1#show ip ospf neighbor

Neighbor ID   Pri  State           Dead Time  Address      Interface
22.22.22.22   0    FULL/ -         00:00:10  192.168.12.2 Serial0/0/0
33.33.33.33   0    FULL/ -         00:00:39  192.168.13.2 Serial0/0/1
R1#
```

Copy Paste

Top

- d. Emita el comando **show ip ospf interface S0/0/0** en el R2 para ver el estado de OSPF de la interfaz S0/0/0.

R2# **show ip ospf interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement



Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT,
Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40

No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0


Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

R2(config-router)#show ip ospf interface S0/0/0
^
% Invalid input detected at '^' marker.

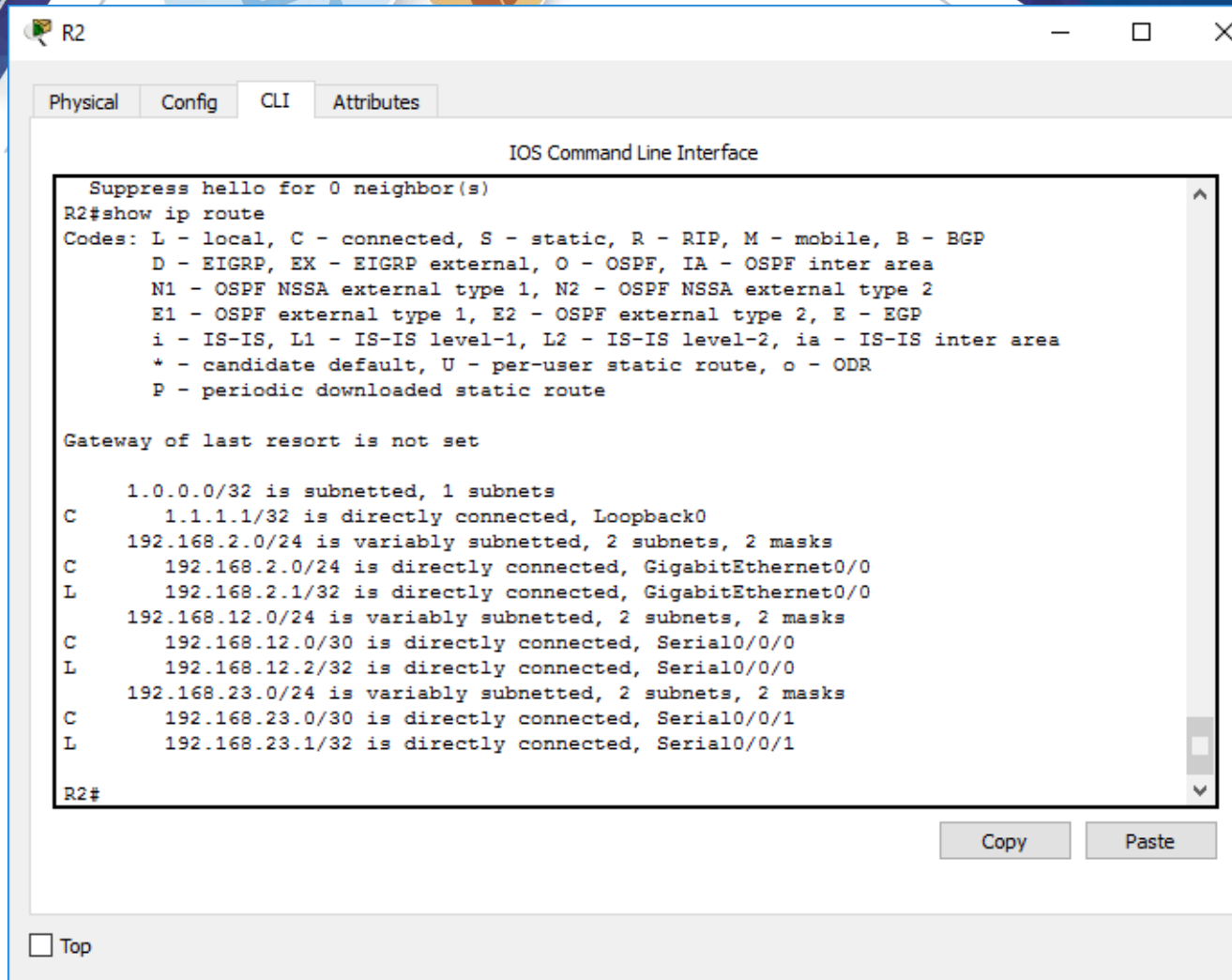
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip ospf interface S0/0/0

Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.2/30, Area 0
 Process ID 1, Router ID 22.22.22.22, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Suppress hello for 0 neighbor(s)
R2#
Copy Paste
 Top

```

- e. Si todas las interfaces en el R2 son pasivas, no se anuncia ninguna información de routing. En este caso, el R1 y el R3 ya no deberían tener una ruta a la red 192.168.2.0/24. Esto se puede verificar mediante el comando **show ip route**.



R2

Physical Config CLI Attributes

IOS Command Line Interface

```

Suppress hello for 0 neighbor(s)
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.2/32 is directly connected, Serial0/0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/30 is directly connected, Serial0/0/1
L       192.168.23.1/32 is directly connected, Serial0/0/1

R2#

```

Copy Paste

Top

- f. En el R2, emita el comando **no passive-interface** para que el router envíe y reciba actualizaciones de routing OSPF. Después de introducir este comando, verá un mensaje informativo que explica que se estableció una adyacencia de vecino con el R1.

R2(config)# **router ospf 1**

R2(config-router)# **no passive-interface s0/0/0**

R2(config-router)#

*Apr 3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done

```

R2
Physical Config CLI Attributes
IOS Command Line Interface
192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.23.0/30 is directly connected, Serial0/0/1
L    192.168.23.1/32 is directly connected, Serial0/0/1

R2#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no passive-interface
      ^
% Invalid input detected at '^' marker.

R2(config)#no passive-interface
      ^
% Invalid input detected at '^' marker.

R2(config)#no passive-interface s0/0/0
      ^
% Invalid input detected at '^' marker.

R2(config)#router ospf 1
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
00:30:41: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done
Copy Paste
 Top

```

- g. Vuelva a emitir los comandos **show ip route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 192.168.2.0/24.
- ¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? **s0/0/0**
 - ¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3? **129**
 - ¿El R2 aparece como vecino OSPF en el R1? **_si**
 - ¿El R2 aparece como vecino OSPF en el R3? **No**
 - ¿Qué indica esta información? **El trafico haci la red 2 desde r3 puede ser ruteado, pero atraves del r1.**

R1

Physical Config CLI Attributes

IOS Command Line Interface

```

R1#
00:39:12: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired

00:39:12: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

00:41:04: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/0 from LOADING to
FULL, Loading Done

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1/32 is directly connected, Loopback0
C       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:00:28, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:10:19, Serial0/0/1
C       192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
L       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
C       192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
L       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
O       192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:00:28, Serial0/0/0
                [110/128] via 192.168.13.2, 00:00:28, Serial0/0/1

R1#
  
```

Copy Paste

Top

- h. Cambie la interfaz S0/0/1 en el R2 para permitir que anuncie las rutas OSPF. Registre los comandos utilizados a continuación.

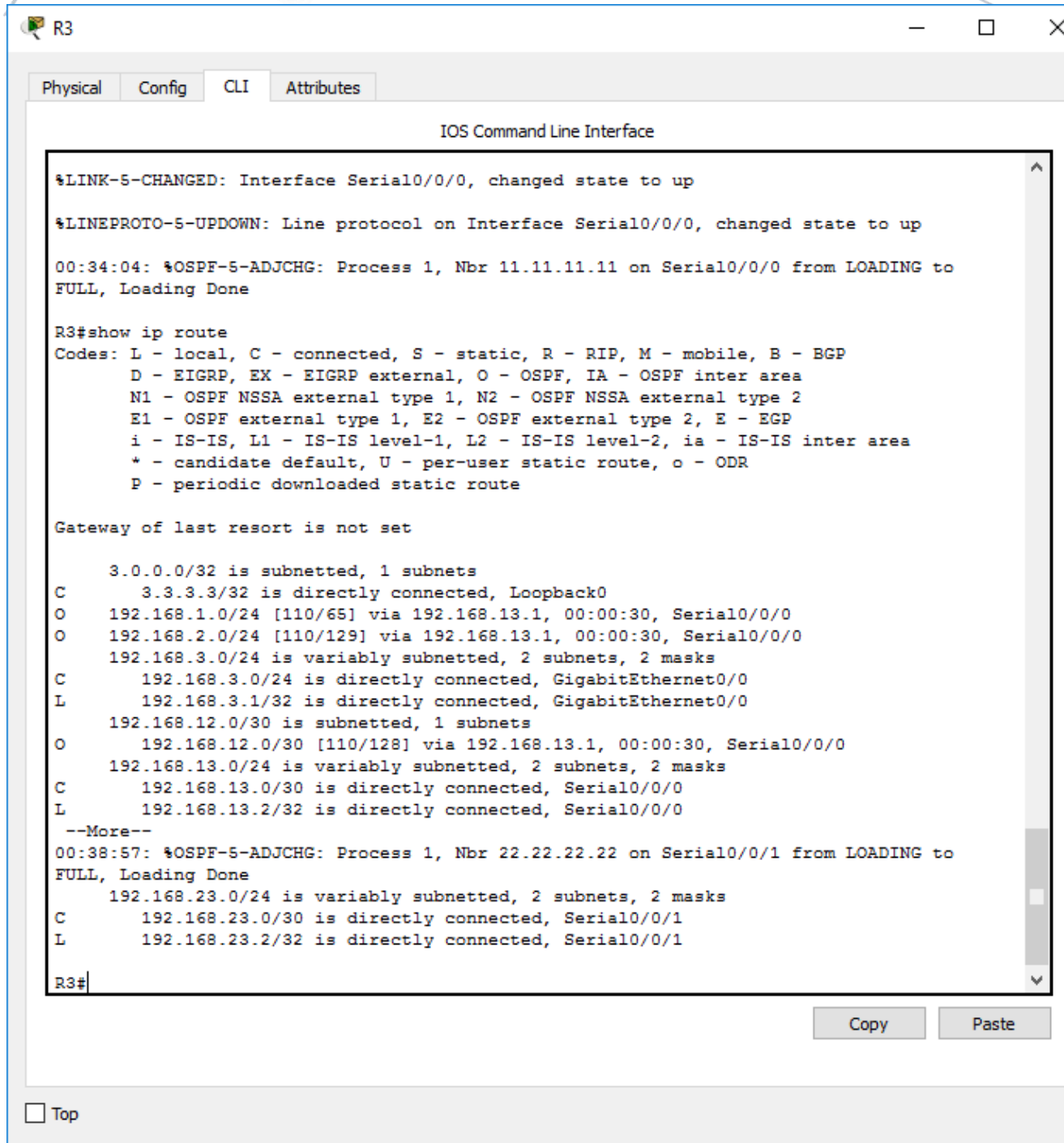
No passive interface s/0/0/1

- i. Vuelva a emitir el comando **show ip route** en el R3.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? **s0/0/1**

¿Cuál es la métrica de costo acumulado para la red 192.168.2.0/24 en el R3 y cómo se calcula? **65**

¿El R2 aparece como vecino OSPF del R3? **Si**



```

R3
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

00:34:04: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 3.0.0.0/32 is subnetted, 1 subnets
 C       3.3.3.3/32 is directly connected, Loopback0
 O       192.168.1.0/24 [110/65] via 192.168.13.1, 00:00:30, Serial0/0/0
 O       192.168.2.0/24 [110/129] via 192.168.13.1, 00:00:30, Serial0/0/0
 192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
 C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
 L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
 192.168.12.0/30 is subnetted, 1 subnets
 O       192.168.12.0/30 [110/128] via 192.168.13.1, 00:00:30, Serial0/0/0
 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
 C       192.168.13.0/30 is directly connected, Serial0/0/0
 L       192.168.13.2/32 is directly connected, Serial0/0/0
--More--
00:38:57: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/1 from LOADING to FULL, Loading Done
 192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
 C       192.168.23.0/30 is directly connected, Serial0/0/1
 L       192.168.23.2/32 is directly connected, Serial0/0/1

R3#
Copy Paste
 Top
  
```

Part 5: cambiar las métricas de OSPF

En la parte 3, cambiará las métricas de OSPF con los comandos **auto-cost**, **reference-bandwidth**, **bandwidth** e **ip ospf cost**.

Nota: en la parte 1, se deberían haber configurado todas las interfaces DCE con una frecuencia de reloj de 128000.

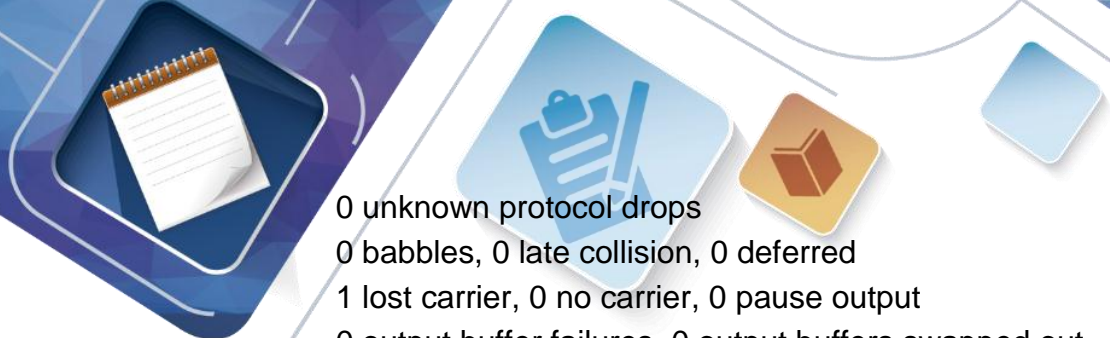
Step 1: cambiar el ancho de banda de referencia en los routers.

El ancho de banda de referencia predeterminado para OSPF es 100 Mb/s (velocidad Fast Ethernet). Sin embargo, la mayoría de los dispositivos de infraestructura moderna tienen enlaces con una velocidad superior a 100 Mb/s. Debido a que la métrica de costo de OSPF debe ser un número entero, todos los enlaces con velocidades de transmisión de 100 Mb/s o más tienen un costo de 1. Esto da como resultado interfaces Fast Ethernet, Gigabit Ethernet y 10G Ethernet con el mismo costo. Por eso, se debe cambiar el ancho de banda de referencia a un valor más alto para admitir redes con enlaces más rápidos que 100 Mb/s.

- a. Emita el comando **show interface** en el R1 para ver la configuración del ancho de banda predeterminado para la interfaz G0/0.

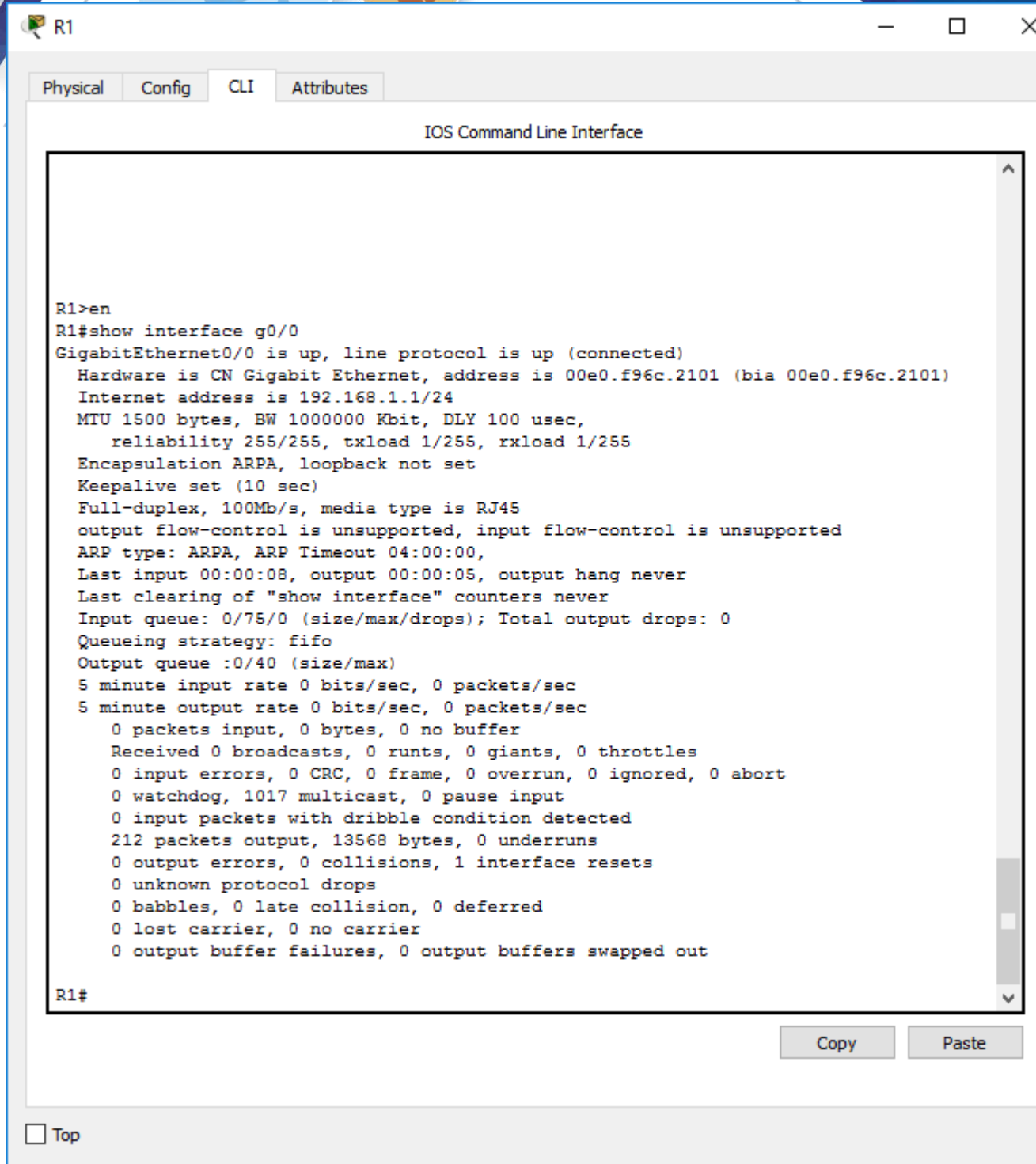
R1# show interface g0/0

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia
c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:31, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
  279 packets output, 89865 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
```



0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
1 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

Nota: si la interfaz del equipo host solo admite velocidad Fast Ethernet, la configuración de ancho de banda de G0/0 puede diferir de la que se muestra arriba. Si la interfaz del equipo host no admite velocidad de gigabit, es probable que el ancho de banda se muestre como 100 000 Kbit/s.



The screenshot shows a terminal window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show interface g0/0' and the output is as follows:

```

R1>en
R1#show interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00e0.f96c.2101 (bia 00e0.f96c.2101)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
    0 input packets with dribble condition detected
    212 packets output, 13568 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

R1#
  
```

At the bottom of the terminal window, there are 'Copy' and 'Paste' buttons, and a 'Top' button with a checkbox.

- b. Emita el comando **show ip route ospf** en el R1 para determinar la ruta a la red 192.168.3.0/24.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

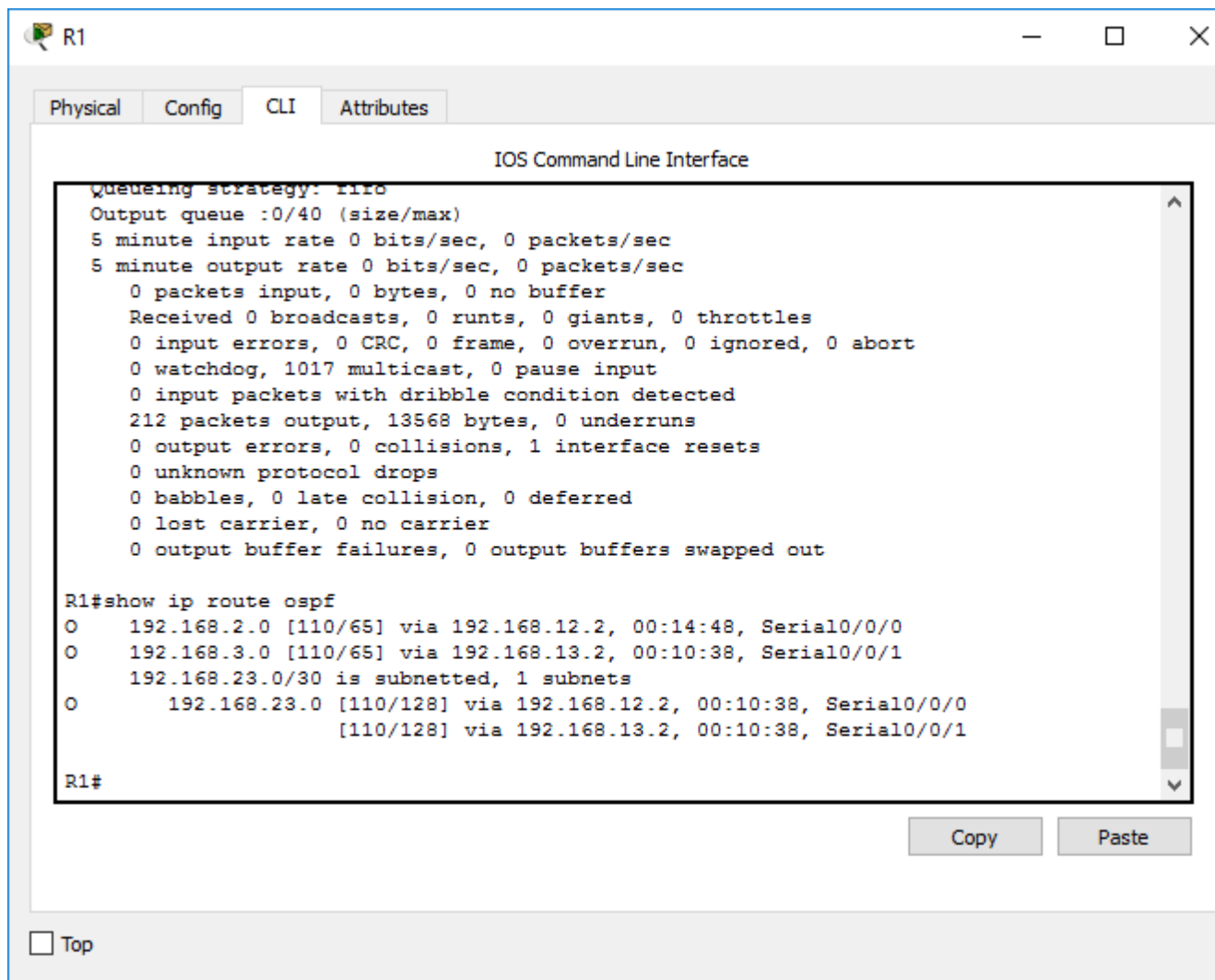
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

- 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
- 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
[110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

Nota: el costo acumulado del R1 a la red 192.168.3.0/24 es 65.



```

R1#show ip route ospf
O   192.168.2.0 [110/65] via 192.168.12.2, 00:14:48, Serial0/0/0
O   192.168.3.0 [110/65] via 192.168.13.2, 00:10:38, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.12.2, 00:10:38, Serial0/0/0
        [110/128] via 192.168.13.2, 00:10:38, Serial0/0/1

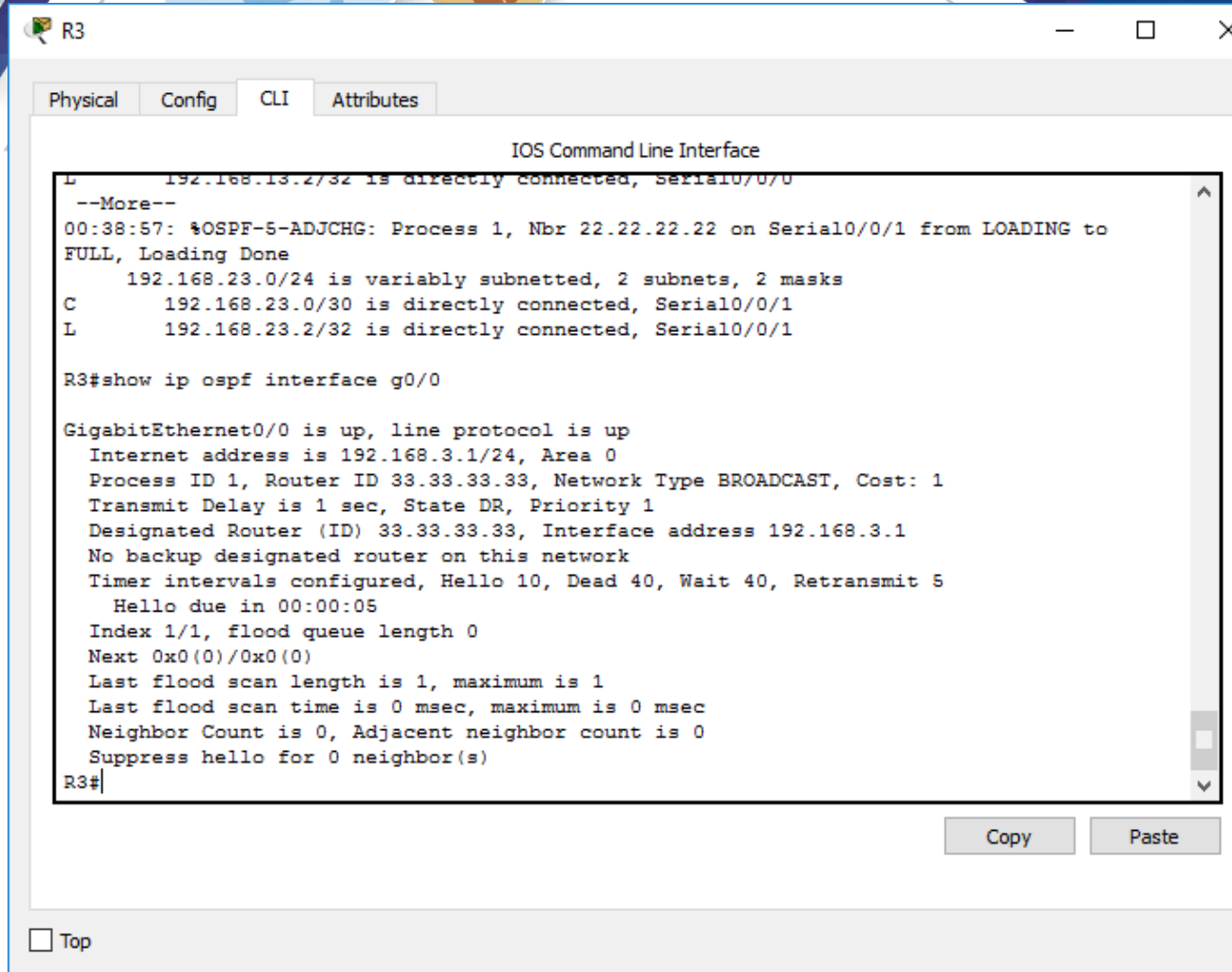
R1#
  
```

Queuing strategy: fifo
 Output queue :0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 watchdog, 1017 multicast, 0 pause input
 0 input packets with dribble condition detected
 212 packets output, 13568 bytes, 0 underruns
 0 output errors, 0 collisions, 1 interface resets
 0 unknown protocol drops
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out

- c. Emita el comando **show ip ospf interface** en el R3 para determinar el costo de routing para G0/0.

R3# **show ip ospf interface g0/0**

```
GigabitEthernet0/0 is up, line protocol is up
Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
  0      1    no      no      Base
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```



```

R3
Physical Config CLI Attributes
IOS Command Line Interface
L 192.168.13.2/32 is directly connected, Serial0/0/0
--More--
00:38:57: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on Serial0/0/1 from LOADING to
FULL, Loading Done
C 192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.23.0/30 is directly connected, Serial0/0/1
L 192.168.23.2/32 is directly connected, Serial0/0/1

R3#show ip ospf interface g0/0

GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.1/24, Area 0
Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
R3#
Copy Paste
 Top
  
```

- d. Emita el comando **show ip ospf interface s0/0/1** en el R1 para ver el costo de routing para S0/0/1.

R1# **show ip ospf interface s0/0/1**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost:

64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40

Hello due in 00:00:04

Supports Link-local Signaling (LLS)

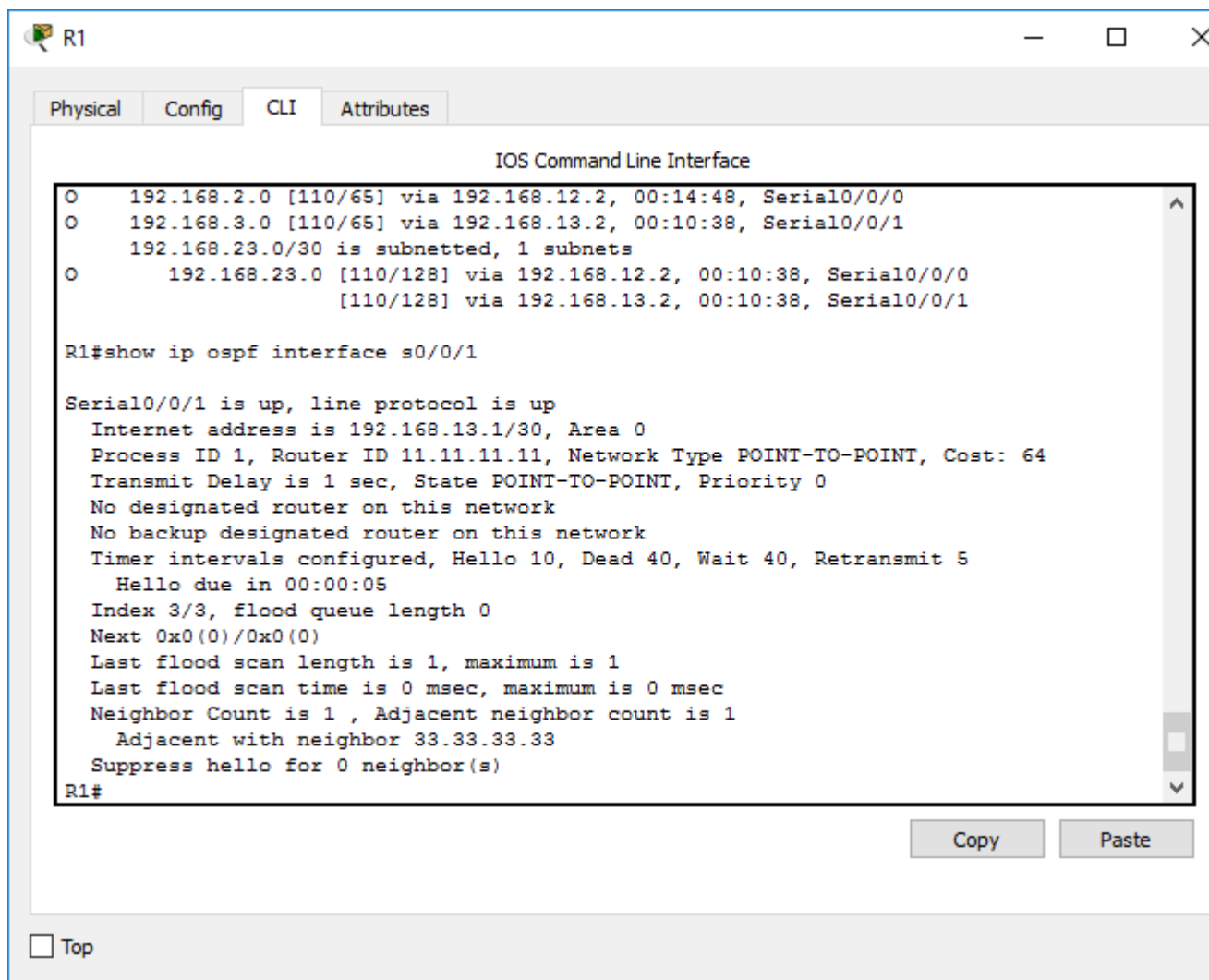
Cisco NSF helper support enabled

```

IETF NSF helper support enabled
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.23.2
Suppress hello for 0 neighbor(s)

```

La suma de los costos de estas dos interfaces es el costo acumulado de la ruta a la red 192.168.3.0/24 en el R3 ($1 + 64 = 65$), como puede observarse en el resultado del comando **show ip route**.



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
O 192.168.2.0 [110/65] via 192.168.12.2, 00:14:48, Serial0/0/0
O 192.168.3.0 [110/65] via 192.168.13.2, 00:10:38, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O   192.168.23.0 [110/128] via 192.168.12.2, 00:10:38, Serial0/0/0
   [110/128] via 192.168.13.2, 00:10:38, Serial0/0/1

R1#show ip ospf interface s0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 33.33.33.33
  Suppress hello for 0 neighbor(s)
R1#

```

- e. Emita el comando **auto-cost reference-bandwidth 10000** en el R1 para cambiar la configuración de ancho de banda de referencia predeterminado. Con esta configuración, las interfaces de 10 Gb/s tendrán un costo de 1, las

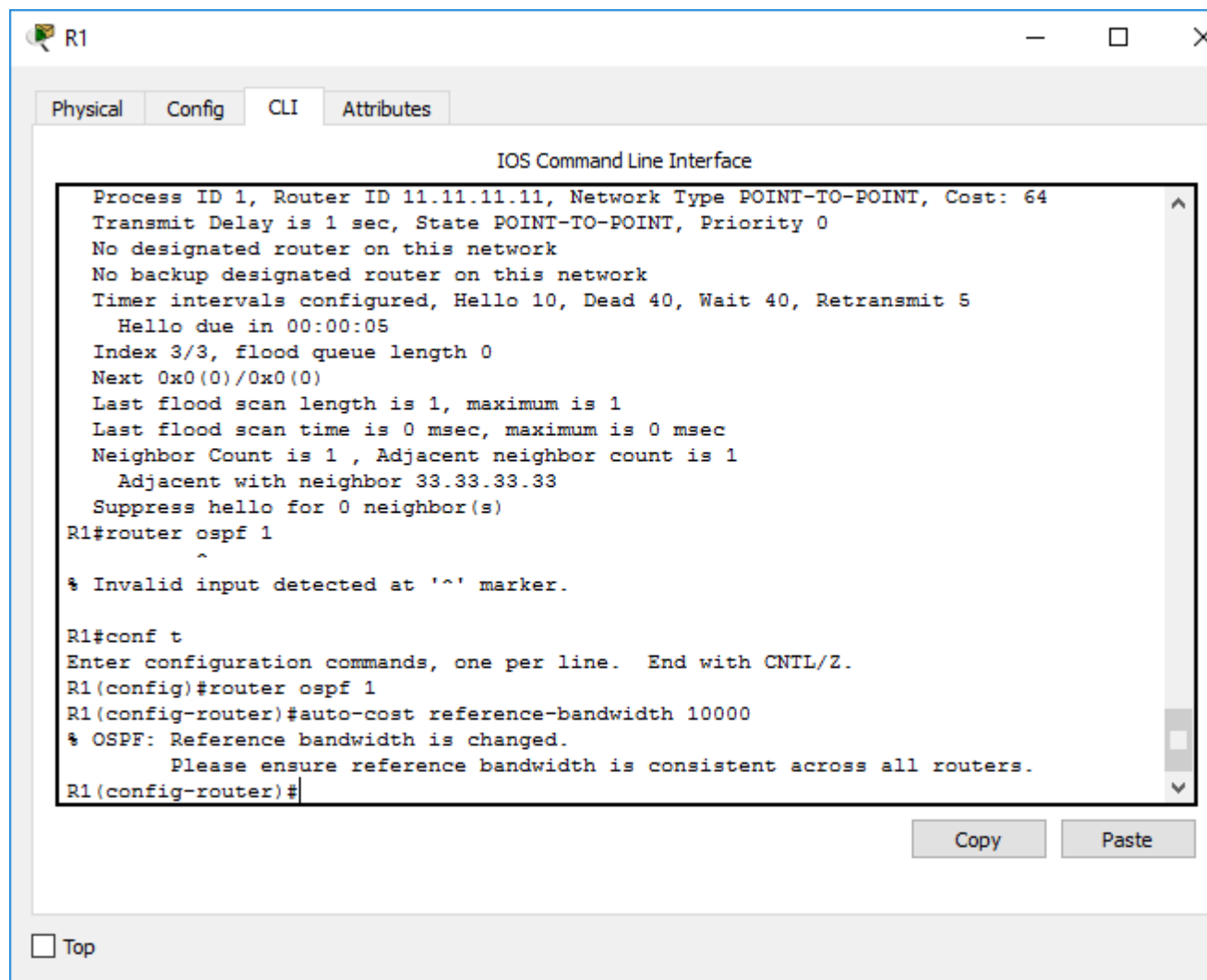
interfaces de 1 Gb/s tendrán un costo de 10, y las interfaces de 100 Mb/s tendrán un costo de 100.

```
R1(config)# router ospf 1
```

```
R1(config-router)# auto-cost reference-bandwidth 10000
```

```
% OSPF: Reference bandwidth is changed.
```

Please ensure reference bandwidth is consistent across all routers.



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 33.33.33.33
  Suppress hello for 0 neighbor(s)
R1#router ospf 1
  ^
% Invalid input detected at '^' marker.

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
  Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#
  
```

- f. Emita el comando **auto-cost reference-bandwidth 10000** en los routers R2 y R3.

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
00:30:41: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
00:39:43: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from LOADING to FULL, Loading Done

R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

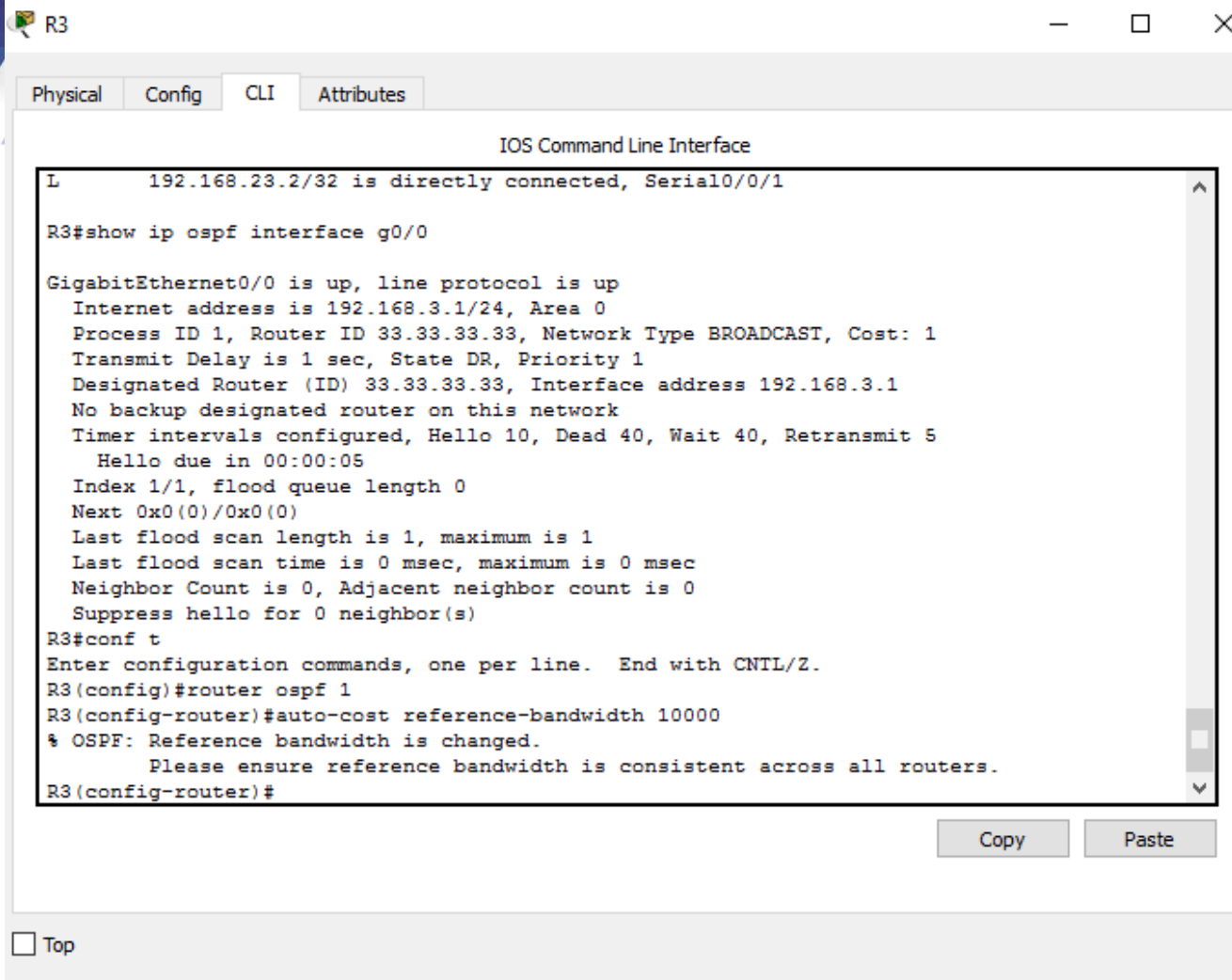
R2#conf t
^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#
```

Copy Paste

Copy to Clipboard

Top



```


R3
Physical Config CLI Attributes
IOS Command Line Interface
L 192.168.23.2/32 is directly connected, Serial0/0/1
R3#show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.3.1/24, Area 0
 Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:05
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
   Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#
Copy Paste
 Top
  
```

- g. Vuelva a emitir el comando **show ip ospf interface** para ver el nuevo costo de G0/0 en el R3 y de S0/0/1 en el R1.

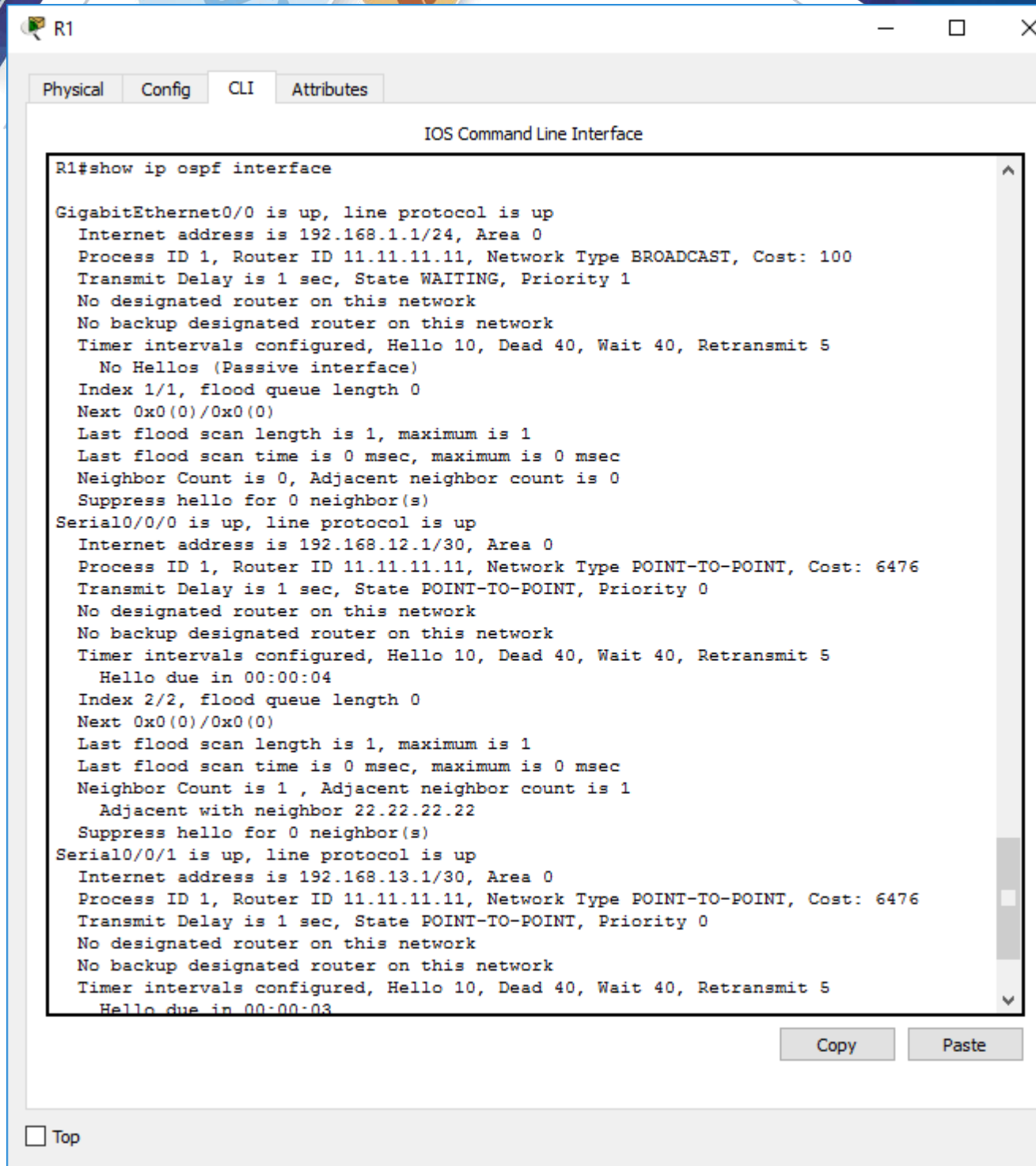
R3# show ip ospf interface g0/0

```

GigabitEthernet0/0 is up, line protocol is up
 Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
 Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
 Topology-MTID Cost Disabled Shutdown Topology Name
   0 10 no no Base
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   oob-resync timeout 40
   Hello due in 00:00:02
 Supports Link-local Signaling (LLS)
  
```



Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)



R1

Physical Config CLI Attributes

IOS Command Line Interface

```
R1#show ip ospf interface

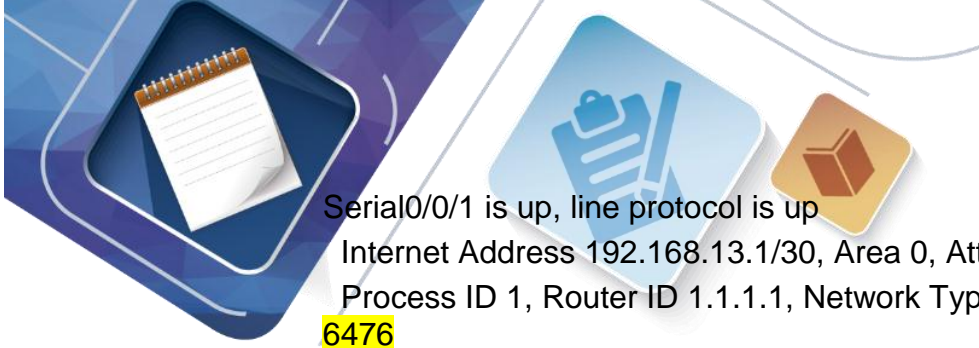
GigabitEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 100
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.1/30, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 22.22.22.22
 Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.13.1/30, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
```

Copy Paste

Top

Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo será diferente del que se muestra en el resultado. Por ejemplo, el costo será de 100 para la velocidad Fast Ethernet (100 Mb/s).

R1# **show ip ospf interface s0/0/1**



Serial0/0/1 is up, line protocol is up
Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost:
6476

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	6476	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40

Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

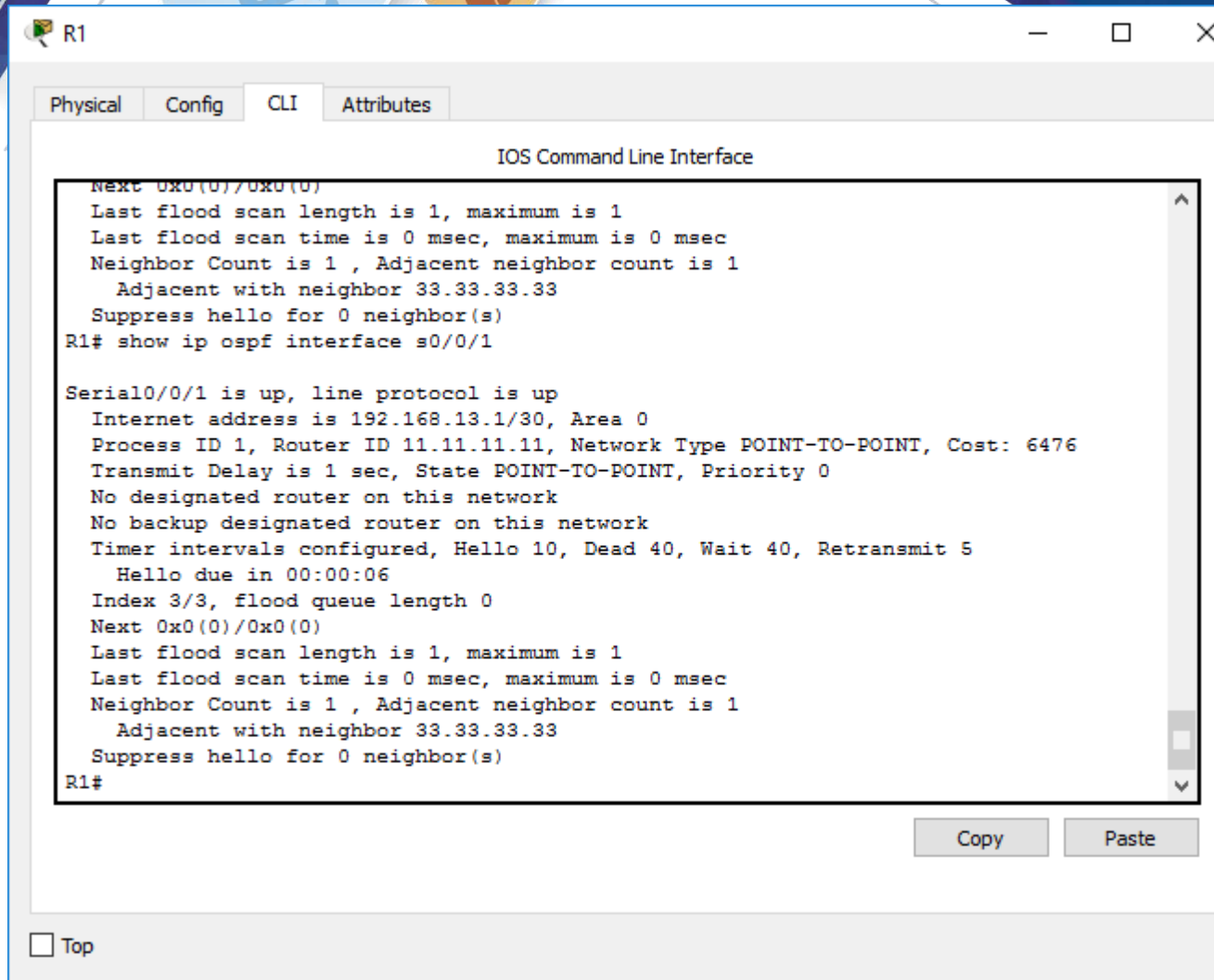
Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)



- h. Vuelva a emitir el comando **show ip route ospf** para ver el nuevo costo acumulado de la ruta 192.168.3.0/24 ($10 + 6476 = 6486$).

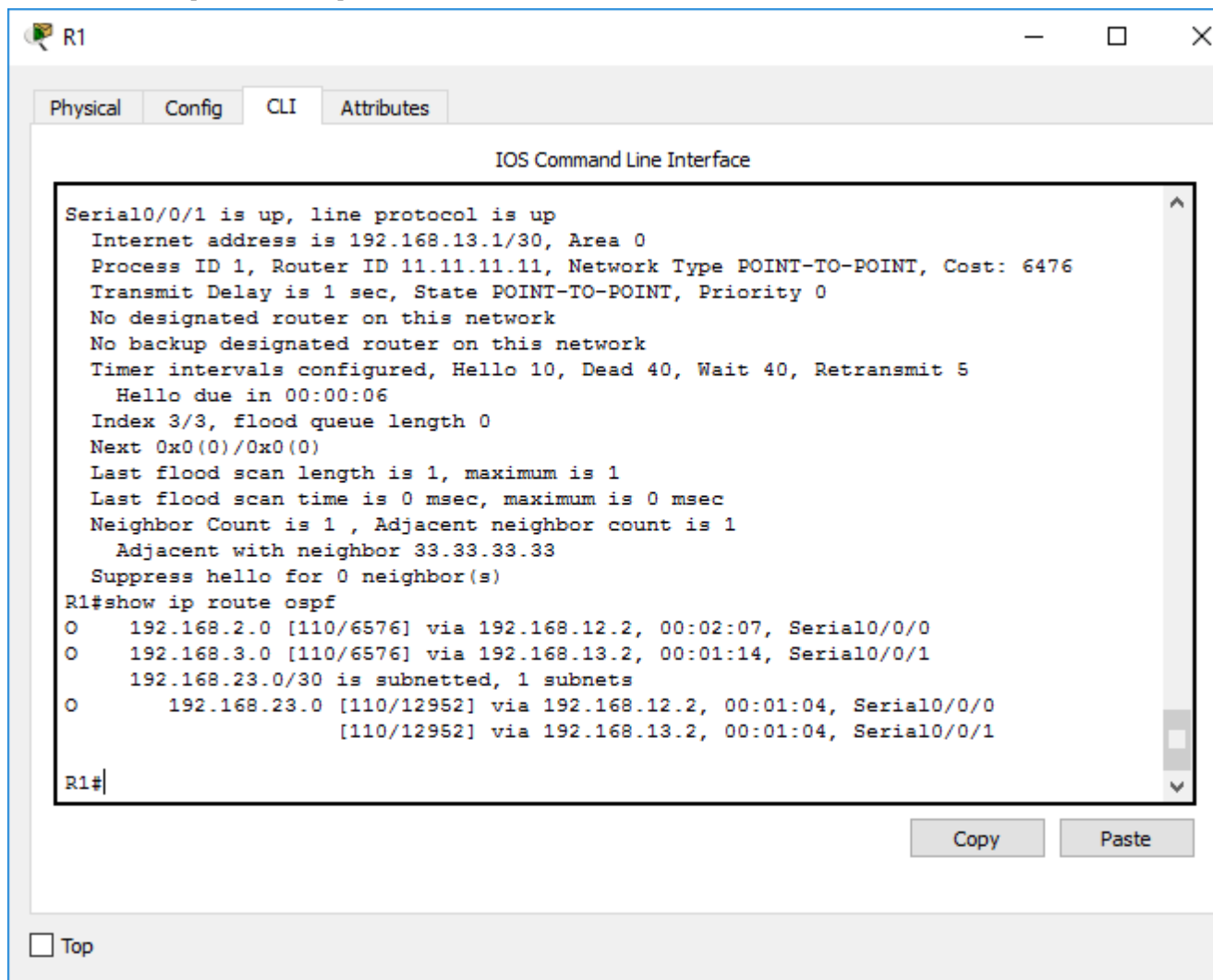
Nota: si el dispositivo conectado a la interfaz G0/0 no admite velocidad de Gigabit Ethernet, el costo total será diferente del que se muestra en el resultado. Por ejemplo, el costo acumulado será 6576 si G0/0 está funcionando con velocidad Fast Ethernet (100 Mb/s).

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

- 192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
- 192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
- 192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
[110/12952] via 192.168.12.2, 00:05:17, Serial0/0/



```

R1
Physical Config CLI Attributes
IOS Command Line Interface

Serial0/0/1 is up, line protocol is up
Internet address is 192.168.13.1/30, Area 0
Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 33.33.33.33
Suppress hello for 0 neighbor(s)
R1#show ip route ospf
O 192.168.2.0 [110/6576] via 192.168.12.2, 00:02:07, Serial0/0/0
O 192.168.3.0 [110/6576] via 192.168.13.2, 00:01:14, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/12952] via 192.168.12.2, 00:01:04, Serial0/0/0
      [110/12952] via 192.168.13.2, 00:01:04, Serial0/0/1

R1#
Copy Paste
 Top
  
```

Nota: cambiar el ancho de banda de referencia en los routers de 100 a 10 000 cambió los costos acumulados de todas las rutas en un factor de 100, pero el costo de cada enlace y ruta de interfaz ahora se refleja con mayor precisión.

- i. Para restablecer el ancho de banda de referencia al valor predeterminado, emita el comando **auto-cost reference-bandwidth 100** en los tres routers.

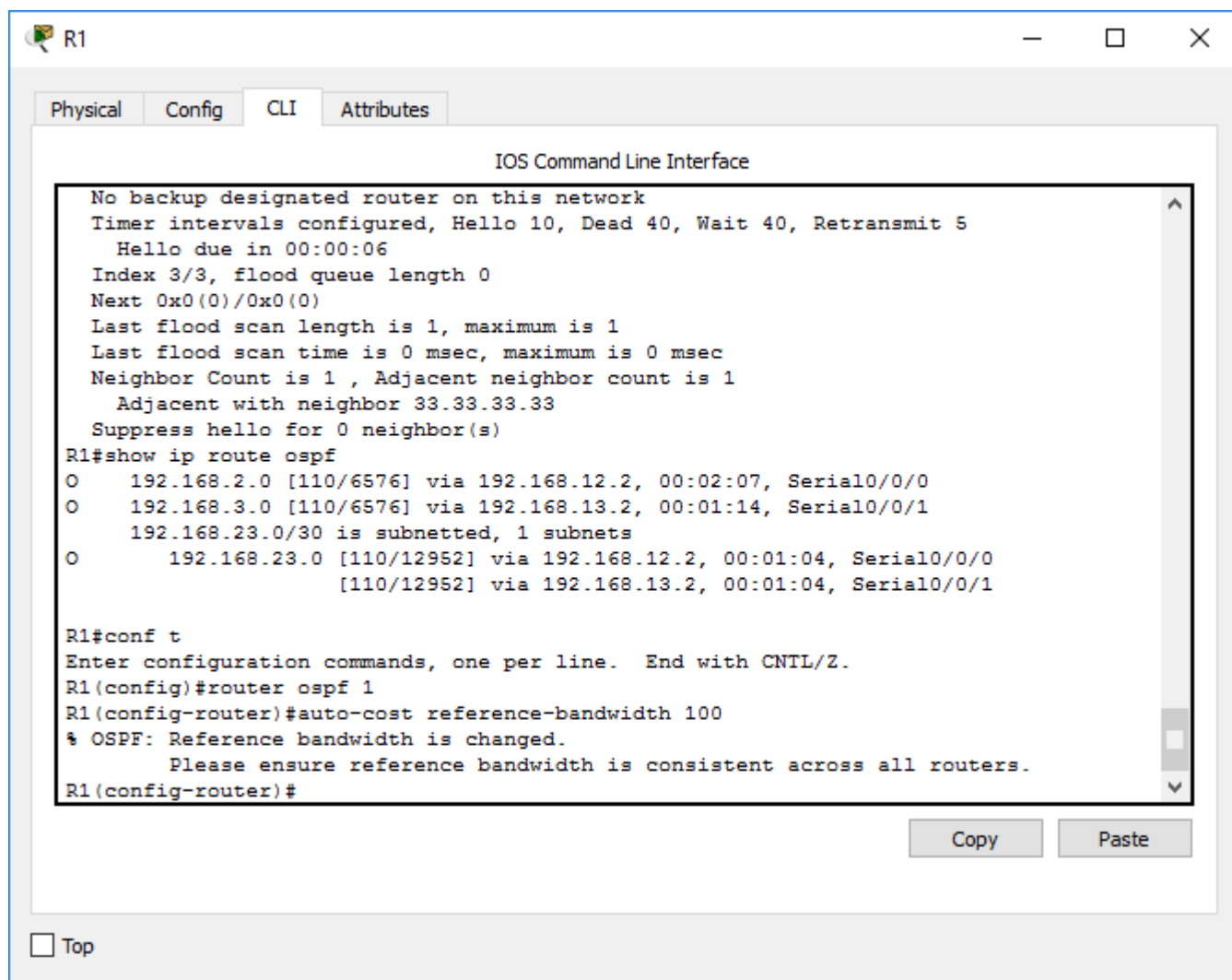
R1(config)# router ospf 1

R1(config-router)# **auto-cost reference-bandwidth 100**

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

¿Por qué querría cambiar el ancho de banda de referencia OSPF predeterminado? Los equipos soportan velocidad en enlaces mayores a 100mbs. Para obtener un costo mas exacto es necesario incrementar el ancho de banda soportado



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 33.33.33.33
  Suppress hello for 0 neighbor(s)
R1#show ip route ospf
O   192.168.2.0 [110/6576] via 192.168.12.2, 00:02:07, Serial0/0/0
O   192.168.3.0 [110/6576] via 192.168.13.2, 00:01:14, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.12.2, 00:01:04, Serial0/0/0
        [110/12952] via 192.168.13.2, 00:01:04, Serial0/0/1

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
  Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#
  
```

Step 2: cambiar el ancho de banda de una interfaz.

En la mayoría de los enlaces seriales, la métrica del ancho de banda será 1544 Kbits de manera predeterminada (la de un T1). Si esta no es la velocidad real del enlace serial, se deberá cambiar la configuración del ancho de banda para que coincida con la velocidad real, a fin de permitir que el costo de la ruta se calcule correctamente en OSPF. Use el comando **bandwidth** para ajusta la configuración del ancho de banda de una interfaz.

Nota: un concepto erróneo habitual es suponer que con el comando **bandwidth** se cambia el ancho de banda físico, o la velocidad, del enlace. El comando modifica la métrica de ancho de banda que utiliza OSPF para calcular los costos de routing, pero no modifica el ancho de banda real (la velocidad) del enlace.

- a. Emita el comando **show interface s0/0/0** en el R1 para ver la configuración actual del ancho de banda de S0/0/0. Aunque la velocidad de enlace/frecuencia de reloj en esta interfaz estaba configurada en 128 Kb/s, el ancho de banda todavía aparece como 1544 Kb/s.

R1# **show interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD **Serial**

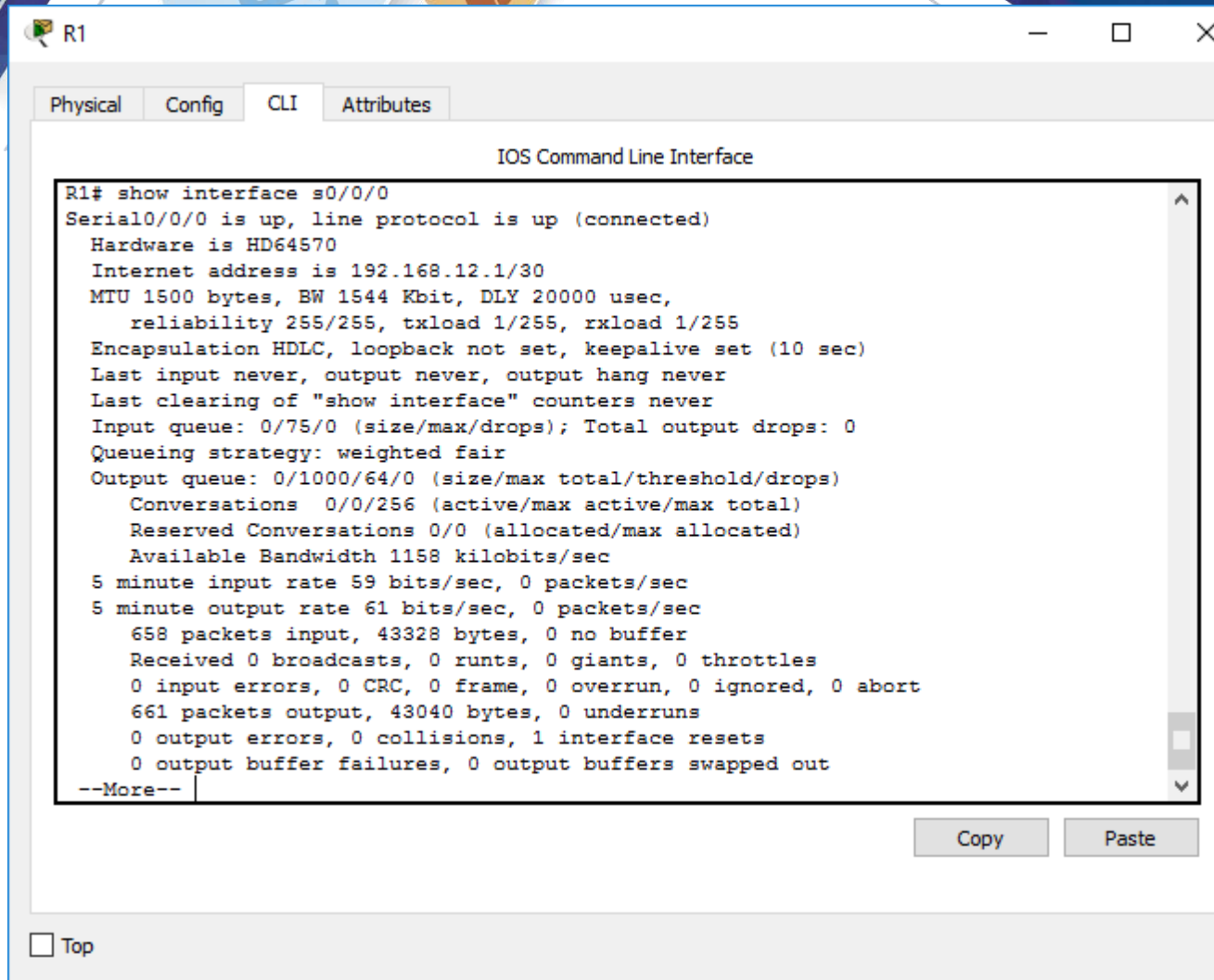
Internet address is 192.168.12.1/30

MTU 1500 bytes, **BW 1544** Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set

Keepalive set (10 sec)

<Output Omitted>



R1

Physical Config CLI Attributes

IOS Command Line Interface

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.12.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 59 bits/sec, 0 packets/sec
5 minute output rate 61 bits/sec, 0 packets/sec
658 packets input, 43328 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
661 packets output, 43040 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
--More--
```

Copy Paste

Top

- b. Emita el comando **show ip route ospf** en el R1 para ver el costo acumulado de la ruta a la red 192.168.23.0/24 con S0/0/0. Observe que hay dos rutas con el mismo costo (128) a la red 192.168.23.0/24, una a través de S0/0/0 y otra a través de S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

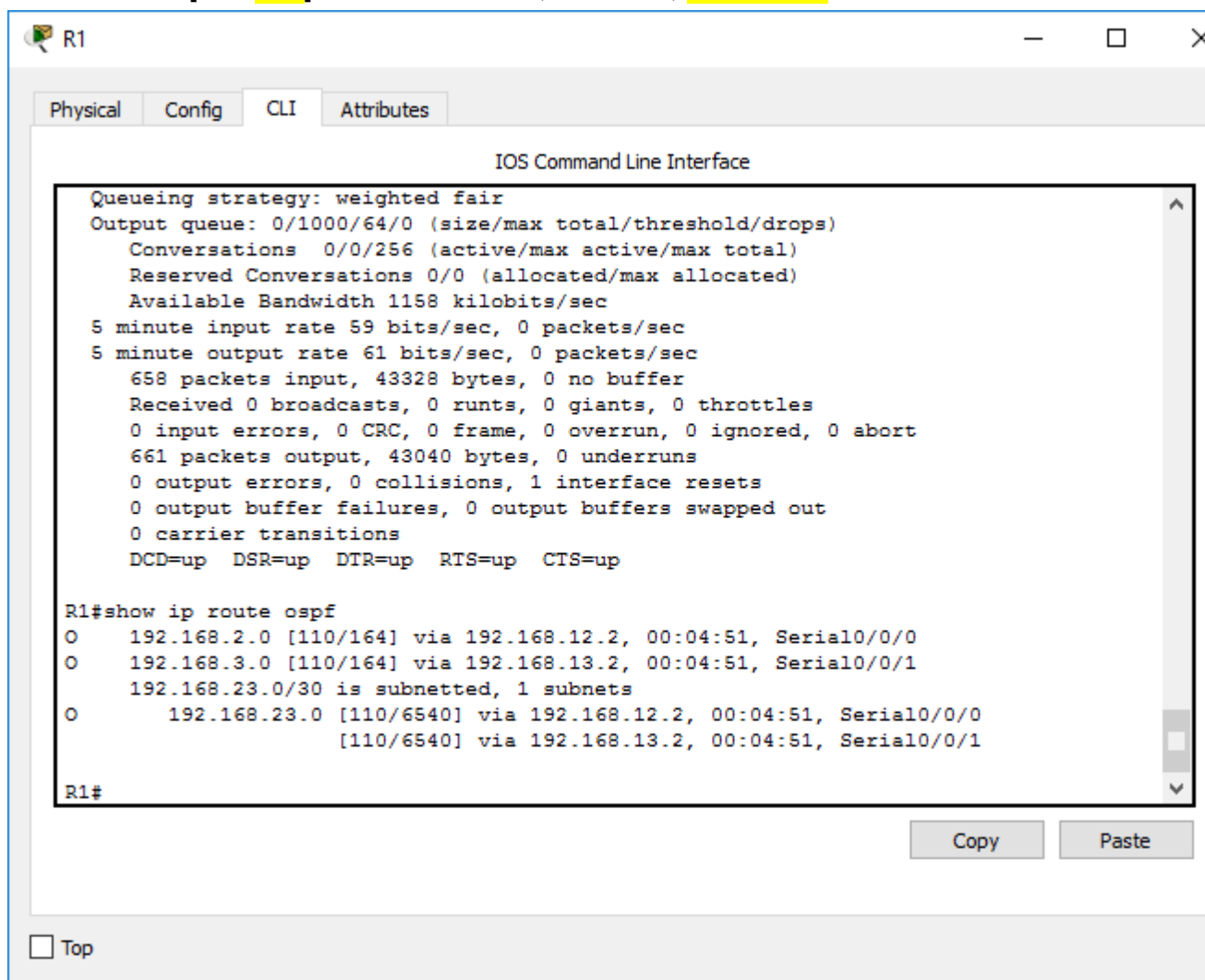
ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

- O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
[110/128] via 192.168.12.2, 00:00:42, Serial0/0/0



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 59 bits/sec, 0 packets/sec
5 minute output rate 61 bits/sec, 0 packets/sec
658 packets input, 43328 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
661 packets output, 43040 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

R1#show ip route ospf
O 192.168.2.0 [110/164] via 192.168.12.2, 00:04:51, Serial0/0/0
O 192.168.3.0 [110/164] via 192.168.13.2, 00:04:51, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/6540] via 192.168.12.2, 00:04:51, Serial0/0/0
      [110/6540] via 192.168.13.2, 00:04:51, Serial0/0/1

R1#
Copy Paste
 Top
  
```

- c. Emita el comando **bandwidth 128** para establecer el ancho de banda en S0/0/0 en 128 Kb/s.
R1(config)# **interface s0/0/0**
R1(config-if)# **bandwidth 128**
- d. Vuelva a emitir el comando **show ip route ospf**. En la tabla de routing, ya no se muestra la ruta a la red 192.168.23.0/24 a través de la interfaz S0/0/0. Esto es porque la mejor ruta, la que tiene el costo más bajo, ahora es a través de S0/0/1.
R1# **show ip route ospf**
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

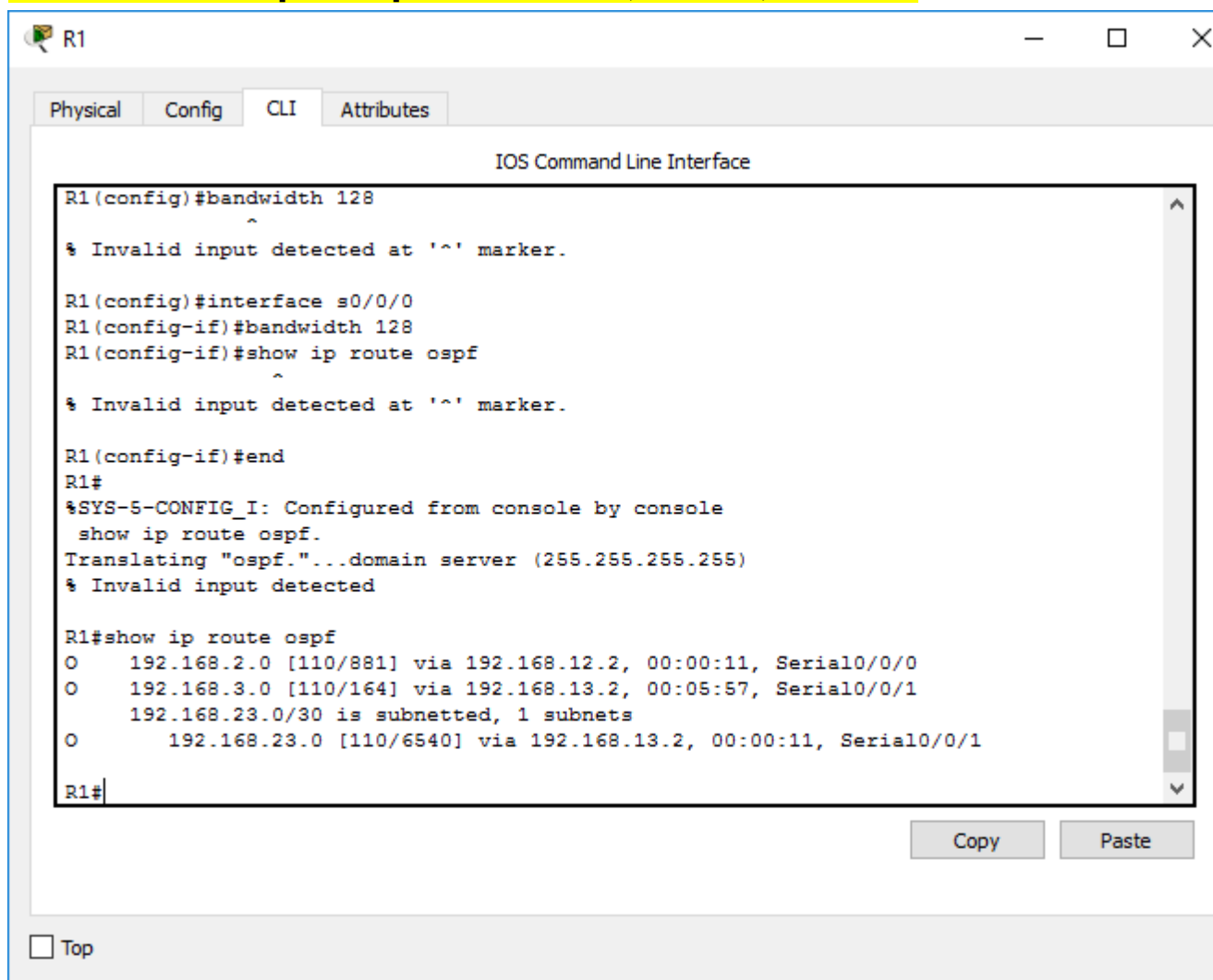
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#bandwidth 128
^
% Invalid input detected at '^' marker.

R1(config)#interface s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#show ip route ospf
^
% Invalid input detected at '^' marker.

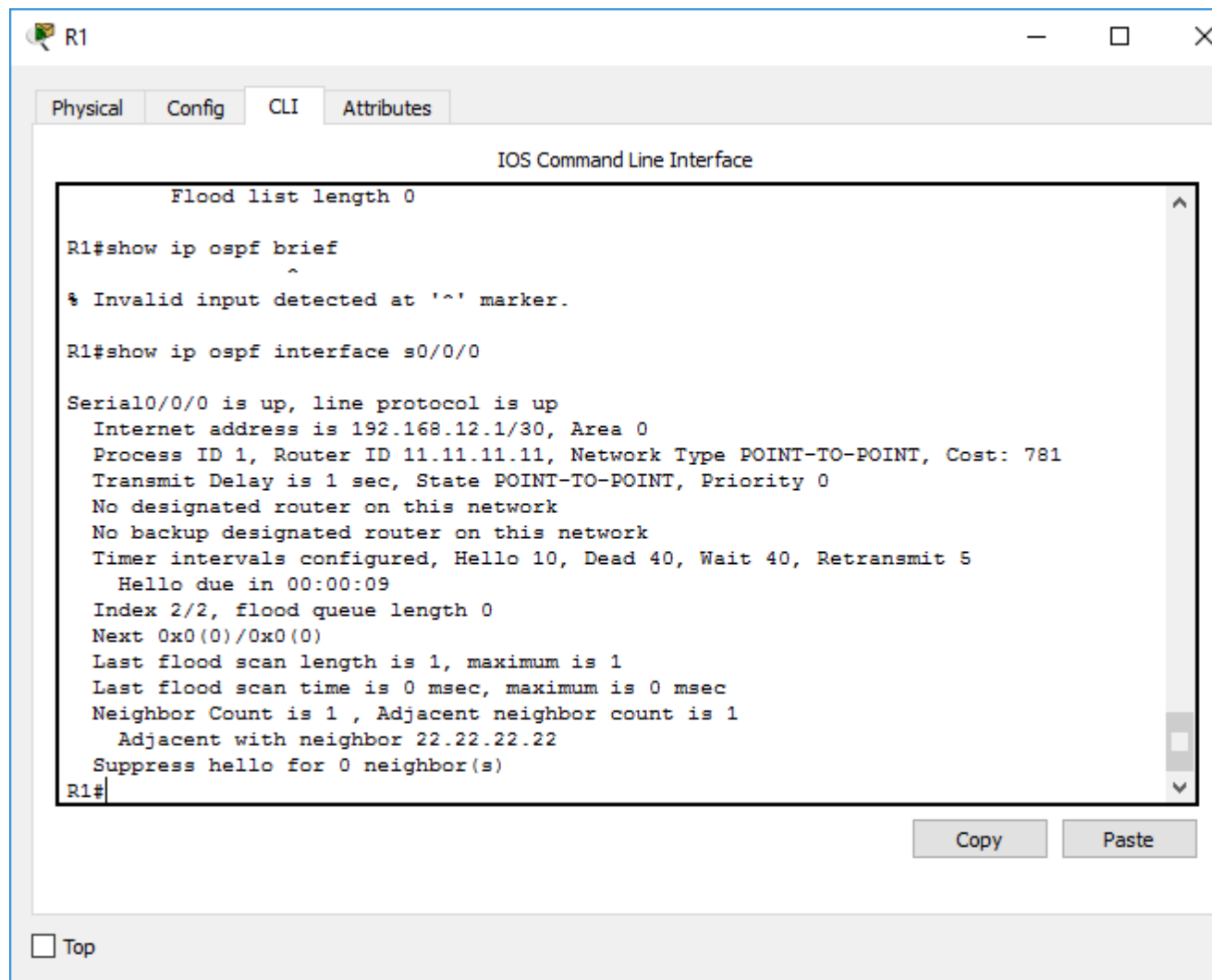
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
show ip route ospf.
Translating "ospf"...domain server (255.255.255.255)
% Invalid input detected

R1#show ip route ospf
O   192.168.2.0 [110/881] via 192.168.12.2, 00:00:11, Serial0/0/0
O   192.168.3.0 [110/164] via 192.168.13.2, 00:05:57, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/6540] via 192.168.13.2, 00:00:11, Serial0/0/1
R1#
Copy Paste
 Top
  
```

- e. Emita el comando **show ip ospf interface brief**. El costo de S0/0/0 cambió de 64 a 781, que es una representación precisa del costo de la velocidad del enlace.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1	
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1	
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0	



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Flood list length 0
R1#show ip ospf brief
^
% Invalid input detected at '^' marker.
R1#show ip ospf interface s0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.12.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 22.22.22.22
  Suppress hello for 0 neighbor(s)
R1#
  
```

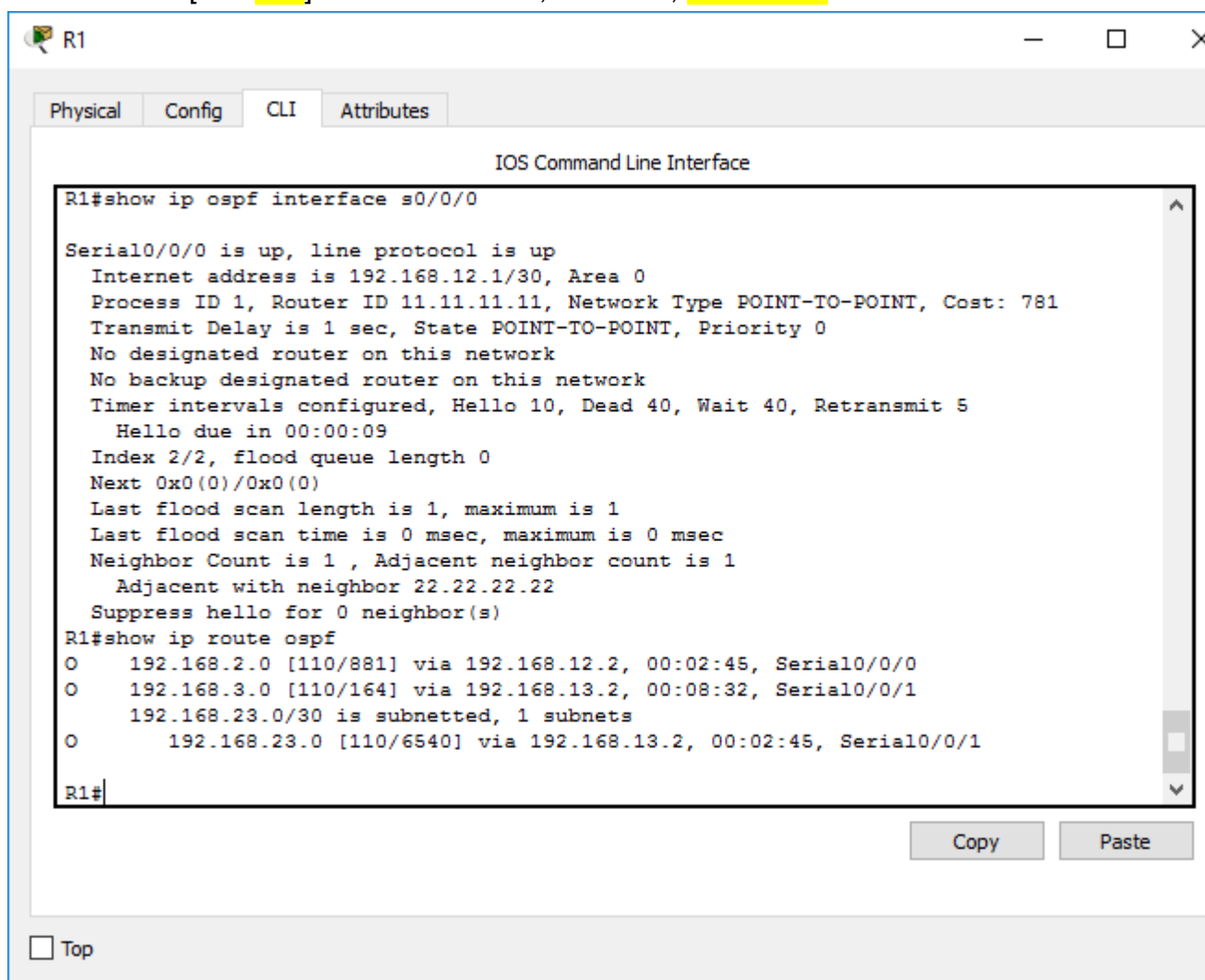
- f. Cambie el ancho de banda de la interfaz S0/0/1 a la misma configuración que S0/0/0 en el R1.
- g. Vuelva a emitir el comando **show ip route ospf** para ver el costo acumulado de ambas rutas a la red 192.168.23.0/24. Observe que otra vez hay dos rutas con el mismo costo (845) a la red 192.168.23.0/24: una a través de S0/0/0 y otra a través de S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

- O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
 192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
 [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0



The screenshot shows a Cisco IOS Command Line Interface window for router R1. The CLI shows the output of two commands: 'show ip ospf interface s0/0/0' and 'show ip route ospf'. The first command displays detailed OSPF interface statistics for Serial0/0/0, including its IP address (192.168.12.1/30), process ID (1), router ID (11.11.11.11), network type (POINT-TO-POINT), and cost (781). The second command displays the OSPF routing table, showing three entries: a local route for 192.168.2.0/24, a connected route for 192.168.3.0/24, and a static route for 192.168.23.0/24.

```

R1#show ip ospf interface s0/0/0

Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.12.1/30, Area 0
 Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 781
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:09
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
   Adjacent with neighbor 22.22.22.22
 Suppress hello for 0 neighbor(s)
R1#show ip route ospf
O   192.168.2.0 [110/881] via 192.168.12.2, 00:02:45, Serial0/0/0
O   192.168.3.0 [110/164] via 192.168.13.2, 00:08:32, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/6540] via 192.168.13.2, 00:02:45, Serial0/0/1
R1#
  
```

Explique la forma en que se calcularon los costos del R1 a las redes 192.168.3.0/24 y 192.168.23.0/30.

El costo para 192.168.3.0/24: $R1 S0 / 0/1 + R3 G0 / 0$ ($781 + 1 = 782$). El costo para 192.168.23.0/30: $R1 S0 / 0/1$ y $R3 S0 / 0/1$ ($781 + 64 = 845$).

- h. Emita el comando **show ip route ospf** en el R3. El costo acumulado de 192.168.1.0/24 todavía se muestra como 65. A diferencia del comando **clock rate**, el comando **bandwidth** se tiene que aplicar en ambos extremos de un enlace serial.

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

- O 192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
192.168.12.0/30 is subnetted, 1 subnets
- O 192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
[110/128] via 192.168.13.1, 00:30:58, Serial0/0/0

```

R3>end
Translating "end"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

R3>en
R3#show ip route ospf
O   192.168.1.0 [110/6477] via 192.168.13.1, 00:20:13, Serial0/0/0
O   192.168.2.0 [110/6576] via 192.168.23.1, 00:22:21, Serial0/0/1
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/12952] via 192.168.23.1, 00:20:03, Serial0/0/1

R3#
  
```

- i. Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología.
¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1?
¿Por qué?

1562. Cada enlace serie ahora tiene un costo de 781, y la ruta a la red 192.168.23.0/24 viaja sobre dos enlaces seriales. $781 + 781 = 1.562$.



Step 3: cambiar el costo de la ruta.

De manera predeterminada, OSPF utiliza la configuración de ancho de banda para calcular el costo de un enlace. Sin embargo, puede reemplazar este cálculo si configura manualmente el costo de un enlace mediante el comando **ip ospf cost**. Al igual que el comando **bandwidth**, el comando **ip ospf cost** solo afecta el lado del enlace en el que se aplicó.

- a. Emita el comando **show ip route ospf** en el R1.



R1# **show ip route ospf**



Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

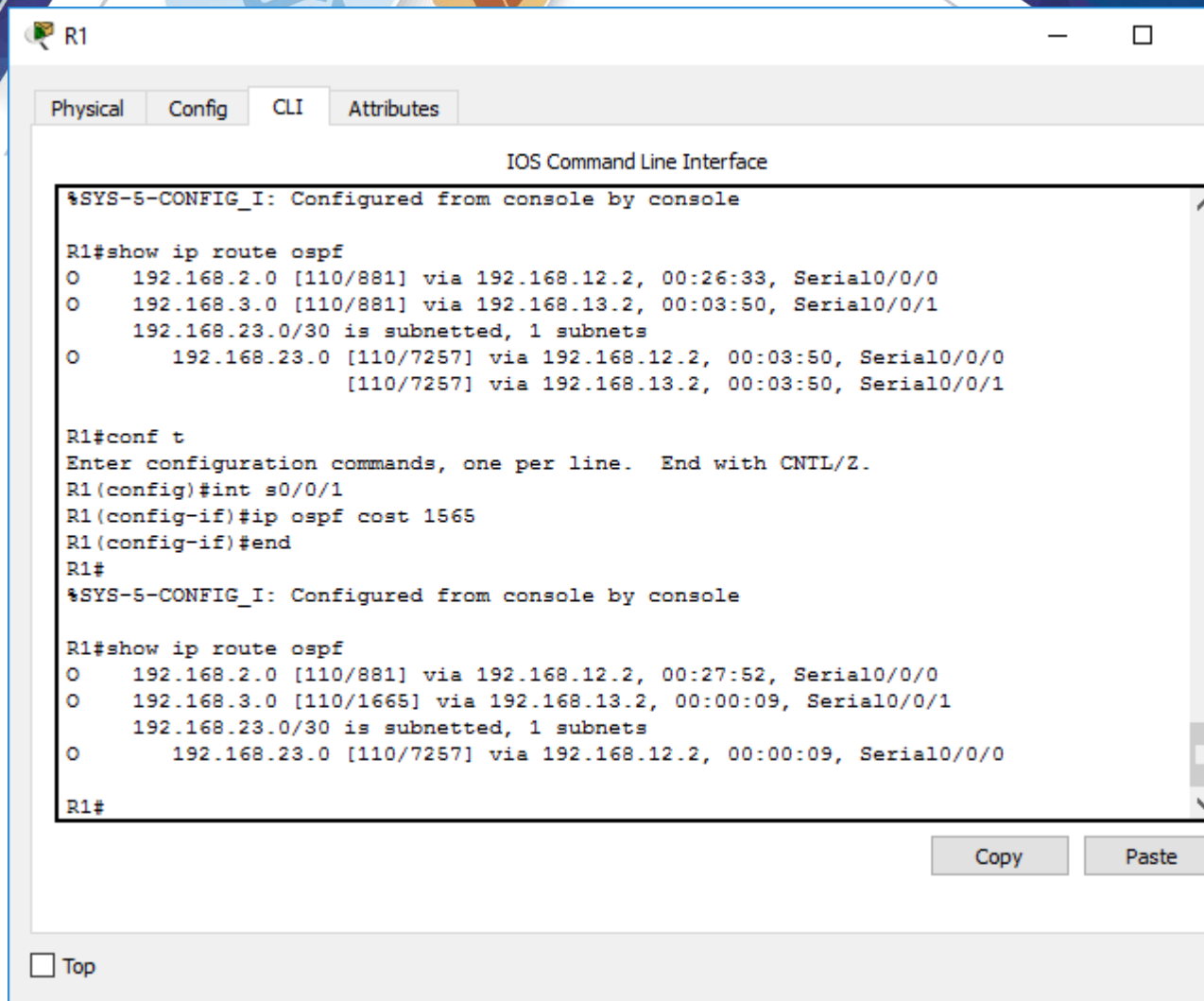
Gateway of last resort is not set

- O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
- O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1
- 192.168.23.0/30 is subnetted, 1 subnets
- O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
- [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

- b. Aplique el comando **ip ospf cost 1565** a la interfaz S0/0/1 en el R1. Un costo de 1565 es mayor que el costo acumulado de la ruta a través del R2, que es 1562.

R1(config)# **int s0/0/1**

R1(config-if)# **ip ospf cost 1565**



- c. Vuelva a emitir el comando **show ip route ospf** en el R1 para mostrar el efecto que produjo este cambio en la tabla de routing. Todas las rutas OSPF para el R1 ahora se enrutan a través del R2.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
 + - replicated route, % - next hop override

Gateway of last resort is not set

- 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
- 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
- 192.168.23.0/30 is subnetted, 1 subnets
- 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0

Nota: la manipulación de costos de enlace mediante el comando **ip ospf cost** es el método de preferencia y el más fácil para cambiar los costos de las rutas OSPF. Además de cambiar el costo basado en el ancho de banda, un administrador de red puede tener otros motivos para cambiar el costo de una ruta, como la preferencia por un proveedor de servicios específico o el costo monetario real de un enlace o de una ruta.

Explique la razón por la que la ruta a la red 192.168.3.0/24 en el R1 ahora atraviesa el R2.

OSPF elegirá la ruta con el menor costo acumulado.

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF? **Asignaciones de ID Router controlan el router designado (DR) y BDR (BDR) elección / proceso en una red de acceso múltiple.**
2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?
El proceso de elección DR / BDR es sólo un problema en una red multiacceso como Ethernet o Frame Relay.
3. ¿Por qué querría configurar una interfaz OSPF como pasiva?
Elimina innecesaria información de enrutamiento OSPF en esa interfaz, liberando ancho de banda

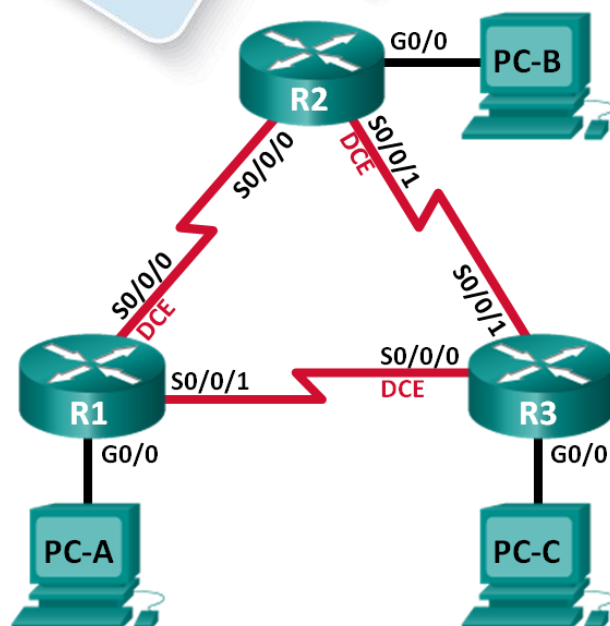
Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

8.3.3.6 Práctica de laboratorio: configuración de OSPFv3 básico de área única.

Topología



Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6.

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv3, asignará ID de router, configurará interfaces pasivas y utilizará varios comandos de CLI para ver y verificar la información de routing OSPFv3.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Gateway predeterminado
R1	G0/0	2001:DB8:ACAD:A::1/64 FE80::1 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:12::1/64 FE80::1 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:13::1/64 FE80::1 link-local	No aplicable
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	No aplicable
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	No aplicable
	S0/0/1 (DCE)	2001:DB8:ACAD:23::2/64 FE80::2 link-local	No aplicable
R3	G0/0	2001:DB8:ACAD:C::3/64 FE80::3 link-local	No aplicable
	S0/0/0 (DCE)	2001:DB8:ACAD:13::3/64 FE80::3 link-local	No aplicable
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	No aplicable
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Part 6: armar la red y configurar los parámetros básicos de los dispositivos

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

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

Step 2: inicializar y volver a cargar los routers según sea necesario.

Step 3: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de vty.
- Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- Configure **logging synchronous** para la línea de consola.
- Cifre las contraseñas de texto no cifrado.
- Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.
- Habilite el routing de unidifusión IPv6 en cada router.
- Copie la configuración en ejecución en la configuración de inicio

Step 4: configurar los equipos host.

Step 5: Probar la conectividad.

Los routers deben poder hacerse ping entre sí, y cada computadora debe poder hacer ping a su gateway predeterminado. Las computadoras no pueden hacer ping a otras computadoras hasta que no se haya configurado el routing OSPFv3. Verifique y resuelva los problemas, si es necesario.

Part 7: configurar el routing OSPFv3

En la parte 2, configurará el routing OSPFv3 en todos los routers de la red y, luego, verificará que las tablas de routing se hayan actualizado correctamente.

Step 1: asignar ID a los routers.

OSPFv3 sigue utilizando una dirección de 32 bits para la ID del router. Debido a que no hay direcciones IPv4 configuradas en los routers, asigne manualmente la ID del router mediante el comando **router-id**.

- a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

R1(config)# **ipv6 router ospf 1**

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#
```

Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

- b. Asigne la ID de router OSPFv3 **1.1.1.1** al R1.

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

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

- c. Inicie el proceso de routing de OSPFv3 y asigne la ID de router **2.2.2.2** al R2 y la ID de router **3.3.3.3** al R3.

```
R2(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R2(config-rtr)#router-id 2.2.2.2

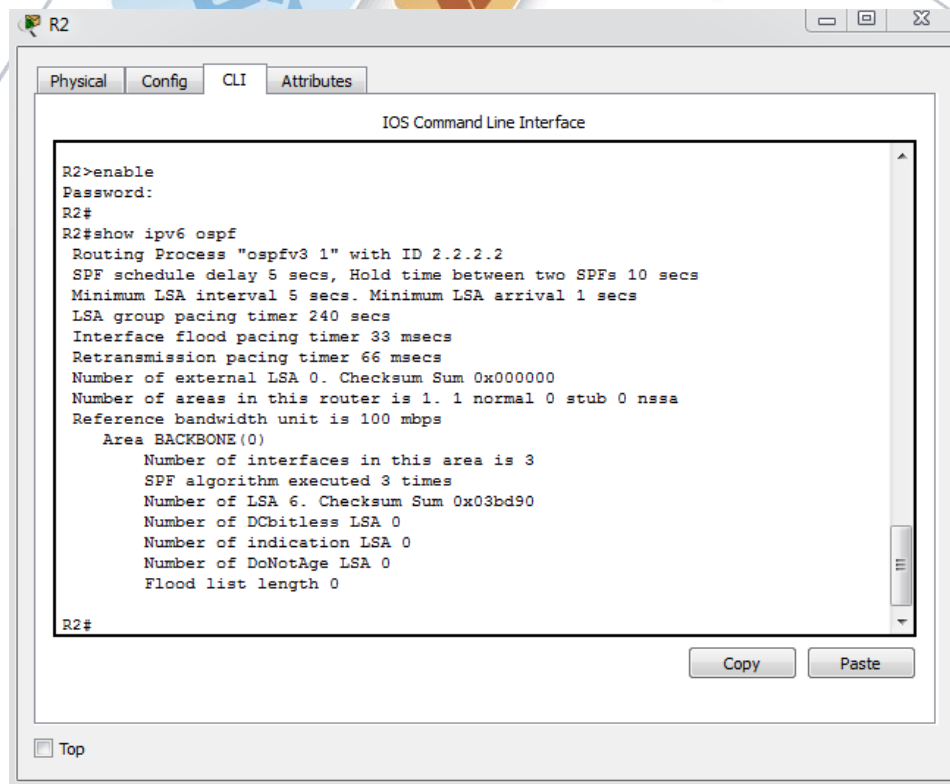
R3(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R3(config-rtr)#router-id 3.3.3.3
```

- d. Emita el comando **show ipv6 ospf** para verificar las ID de router de todos los routers.

R2# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 2.2.2.2

Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 <Output Omitted>



R2

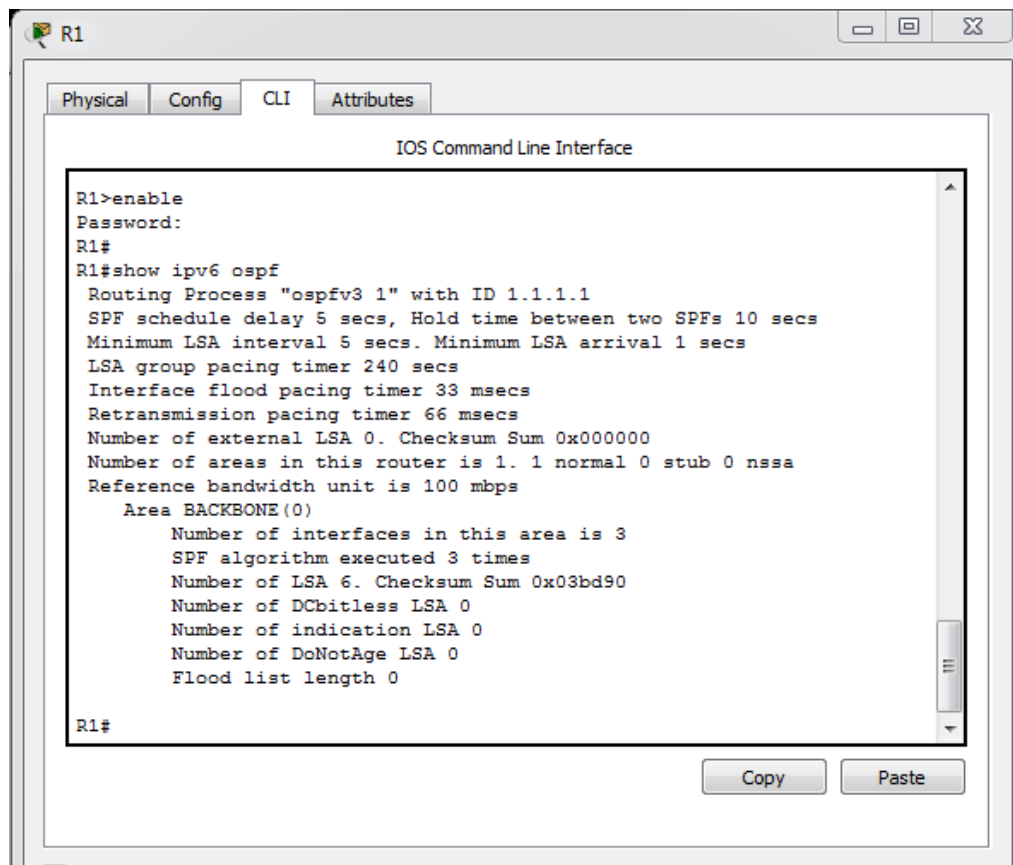
Physical Config CLI Attributes

IOS Command Line Interface

```
R2>enable
Password:
R2#
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    SPF algorithm executed 3 times
    Number of LSA 6. Checksum Sum 0x03bd90
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R2#
```

Copy Paste

Top



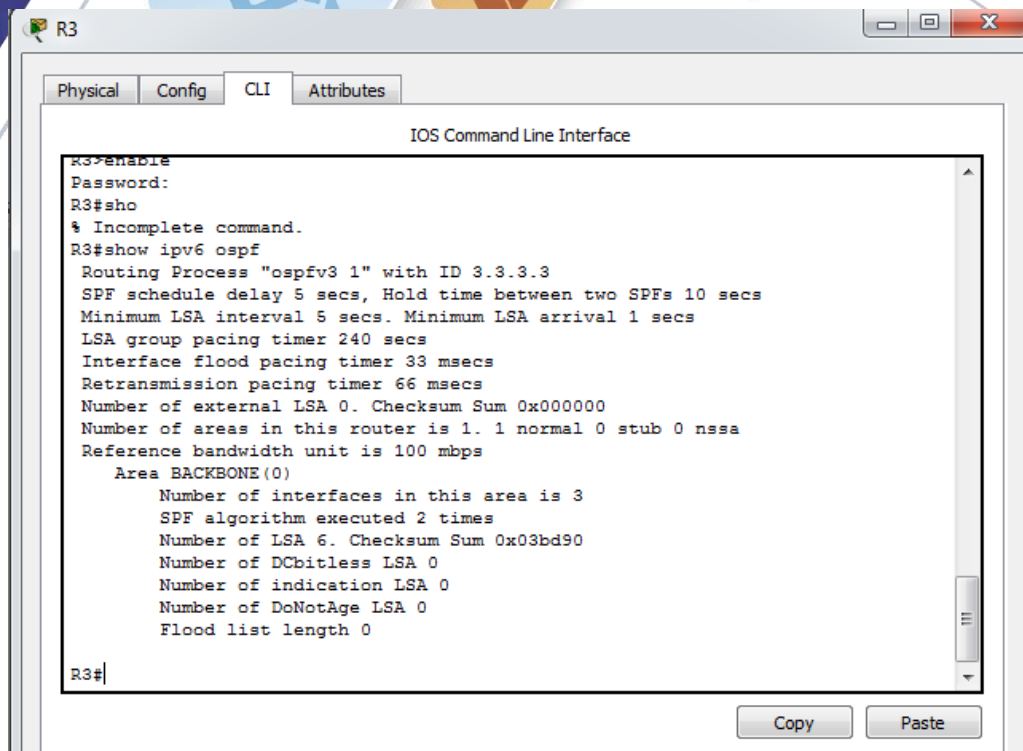
R1

Physical Config CLI Attributes

IOS Command Line Interface

```
R1>enable
Password:
R1#
R1#show ipv6 ospf
Routing Process "ospfv3 1" with ID 1.1.1.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    SPF algorithm executed 3 times
    Number of LSA 6. Checksum Sum 0x03bd90
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R1#
```

Copy Paste



Step 2: configurar OSPFv6 en el R1.

Con IPv6, es común tener varias direcciones IPv6 configuradas en una interfaz. La instrucción `network` se eliminó en OSPFv3. En cambio, el routing OSPFv3 se habilita en el nivel de la interfaz.

- a. Emita el comando `ipv6 ospf 1 area 0` para cada interfaz en el R1 que participará en el routing OSPFv3.

```
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
```

```
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 0
```

```
R3(config)#interface g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
```

Nota: la ID del proceso debe coincidir con la ID del proceso que usó en el paso 1a.

- b. Asigne las interfaces en el R2 y el R3 al área 0 de OSPFv3. Al agregar las interfaces al área 0, debería ver mensajes de adyacencia de vecino.

R1#

```
*Mar 19 22:14:43.251: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
```

R1#

```
*Mar 19 22:14:46.763: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
R1(config-if)#ipv6 ospf 1 area 0
01:04:09: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

R1(config-if)#ipv6 ospf 1 area 0

R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#
01:04:59: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

01:05:04: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-if)#
```

Step 3: verificar vecinos de OSPFv3.

Emita el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

R1# **show ipv6 ospf neighbor**

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	6	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:36	6	Serial0/0/0

```
R1#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	0	FULL/ -	00:00:31	3	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:36	3	Serial0/0/1

```
R1#
```

```
R1#
```

```
R2#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
1.1.1.1	0	FULL/ -	00:00:33	3	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:39	4	Serial0/0/1

```
R2#
```

```
R3#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
1.1.1.1	0	FULL/ -	00:00:39	4	Serial0/0/0
2.2.2.2	0	FULL/ -	00:00:31	4	Serial0/0/1

```
R3#
```

Step 4: verificar la configuración del protocolo OSPFv3.

El comando **show ipv6 protocols** es una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

R1# show ipv6 protocols

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "ospf 1"

Router ID 1.1.1.1

Number of areas: 1 normal, 0 stub, 0 nssa

Interfaces (Area 0):

Serial0/0/1

Serial0/0/0

GigabitEthernet0/0

Redistribution:

None

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0)
  GigabitEthernet0/0
  Serial0/0/0
  Serial0/0/1
```

```
R1#
```

```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/1
    Serial0/0/0
  Redistribution:
    None
```

R2#

```
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0)
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
```

R3#

Step 5: verificar las interfaces OSPFv3.

- Emita el comando **show ipv6 ospf interface** para mostrar una lista detallada de cada interfaz habilitada para OSPF.

R1# show ipv6 ospf interface

Serial0/0/1 is up, line protocol is up

Link Local Address FE80::1, Interface ID 7

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/3/3, flood queue length 0

Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 3.3.3.3

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 6

```

Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:00
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)

```

```

GigabitEthernet0/0 is up, line protocol is up
Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

- b. Para mostrar un resumen de las interfaces con OSPFv3 habilitado, emita el comando **show ipv6 ospf interface brief**.

R1# **show ipv6 ospf interface brief**

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/1	1	0	7	64	P2P	1/1	
Se0/0/0	1	0	6	64	P2P	1/1	
Gi0/0	1	0	3	1	DR	0/0	

Step 6: verificar la tabla de routing IPv6.

Emita el comando **show ipv6 route** para verificar que todas las redes aparezcan en la tabla de routing.

R2# show ipv6 route

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:B::/64 [0/0]

via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:B::2/128 [0/0]

via GigabitEthernet0/0, receive

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1

C 2001:DB8:ACAD:12::/64 [0/0]

via Serial0/0/0, directly connected

L 2001:DB8:ACAD:12::2/128 [0/0]

via Serial0/0/0, receive

O 2001:DB8:ACAD:13::/64 [110/128]

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:23::/64 [0/0]

via Serial0/0/1, directly connected

L 2001:DB8:ACAD:23::2/128 [0/0]

via Serial0/0/1, receive

L FF00::/8 [0/0]

via Null0, receive

```

R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:A::1/128 [0/0]
   via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/0, receive
O 2001:DB8:ACAD:C::/64 [110/65]
   via FE80::3, Serial0/0/1, receive
C 2001:DB8:ACAD:12::/64 [0/0]
   via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::1/128 [0/0]
   via Serial0/0/0, receive
C 2001:DB8:ACAD:13::/64 [0/0]
   via Serial0/0/1, directly connected
L 2001:DB8:ACAD:13::1/128 [0/0]
   via Serial0/0/1, receive
O 2001:DB8:ACAD:23::/64 [110/128]
   via FE80::3, Serial0/0/1, receive
   via FE80::2, Serial0/0/0, receive
L FF00::/8 [0/0]
   via Null0, receive
R1#

R2#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0, receive
C 2001:DB8:ACAD:B::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::2/128 [0/0]
   via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/65]
   via FE80::3, Serial0/0/1, receive
C 2001:DB8:ACAD:12::/64 [0/0]
   via Serial0/0/0, directly connected
L 2001:DB8:ACAD:12::2/128 [0/0]
   via Serial0/0/0, receive
O 2001:DB8:ACAD:13::/64 [110/128]
   via FE80::3, Serial0/0/1, receive
   via FE80::1, Serial0/0/0, receive
C 2001:DB8:ACAD:23::/64 [0/0]
   via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::2/128 [0/0]
   via Serial0/0/1, receive
L FF00::/8 [0/0]
   via Null0, receive
R2#

```

```

R3#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0, receive
O  2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/1, receive
C  2001:DB8:ACAD:C::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:C::3/128 [0/0]
   via GigabitEthernet0/0, receive
O  2001:DB8:ACAD:12::/64 [110/128]
   via FE80::1, Serial0/0/0, receive
   via FE80::2, Serial0/0/1, receive
C  2001:DB8:ACAD:13::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:ACAD:13::3/128 [0/0]
   via Serial0/0/0, receive
C  2001:DB8:ACAD:23::/64 [0/0]
   via Serial0/0/1, directly connected
L  2001:DB8:ACAD:23::3/128 [0/0]
   via Serial0/0/1, receive
L  FF00::/8 [0/0]
   via Null0, receive
R3#

```

¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

- show ipv6 route ospf

Step 7: Verificar la conectividad de extremo a extremo.

Se debería poder hacer ping entre todas las computadoras de la topología. Verifique y resuelva los problemas, si es necesario.

```

PC>ping 2001:DB8:ACAD:A::A

Pinging 2001:DB8:ACAD:A::A with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=6ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=26ms TTL=128
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=26ms TTL=128

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 26ms, Average = 14ms

```

```

PC>ping 2001:DB8:ACAD:B::B

Pinging 2001:DB8:ACAD:B::B with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::B: bytes=32 time=13ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B::B: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 4ms
  
```

```

PC>ping 2001:DB8:ACAD:C::C

Pinging 2001:DB8:ACAD:C::C with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::C: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

PC>
  
```

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

Part 8: configurar las interfaces pasivas de OSPFv3

El comando **passive-interface** evita que se envíen actualizaciones de routing a través de la interfaz de router especificada. Esto se hace comúnmente para reducir el tráfico en las redes LAN, ya que no necesitan recibir comunicaciones de protocolo de routing dinámico. En la parte 3, utilizará el comando **passive-interface** para configurar una única interfaz como pasiva. También configurará OSPFv3 para que todas las interfaces del router sean pasivas de manera predeterminada y, luego, habilitará anuncios de routing OSPF en interfaces seleccionadas.

Step 1: configurar una interfaz pasiva.

- a. Emita el comando **show ipv6 ospf interface g0/0** en el R1. Observe el temporizador que indica cuándo se espera el siguiente paquete de saludo.

Los paquetes de saludo se envían cada 10 segundos y se utilizan entre los routers OSPF para verificar que sus vecinos estén activos.

R1# show ipv6 ospf interface g0/0

```
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, local address FE80::1g
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

- b. Emita el comando **passive-interface** para cambiar la interfaz G0/0 en el R1 a pasiva.

R1(config)# ipv6 router ospf 1

R1(config-rtr)# passive-interface g0/0

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#
```

- c. Vuelva a emitir el comando **show ipv6 ospf interface g0/0** para verificar que la interfaz G0/0 ahora sea pasiva.

R1# show ipv6 ospf interface g0/0

```
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

No Hellos (Passive interface)

```

Wait time before Designated router selection 00:00:34
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
  
```

- d. Emita el comando **show ipv6 route ospf** en el R2 y el R3 para verificar que todavía haya disponible una ruta a la red 2001:DB8:ACAD:A::/64.

R2# show ipv6 route ospf

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1

O 2001:DB8:ACAD:13::/64 [110/128]

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

```

R2#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
  ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
  D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0
O  2001:DB8:ACAD:C::/64 [110/65]
   via FE80::3, Serial0/0/1
O  2001:DB8:ACAD:13::/64 [110/128]
   via FE80::1, Serial0/0/0
   via FE80::3, Serial0/0/1

R3#show ipv6 route ospf
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
  ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
  D - EIGRP, EX - EIGRP external
O  2001:DB8:ACAD:A::/64 [110/65]
   via FE80::1, Serial0/0/0
O  2001:DB8:ACAD:B::/64 [110/65]
   via FE80::2, Serial0/0/1
O  2001:DB8:ACAD:12::/64 [110/128]
   via FE80::1, Serial0/0/0
   via FE80::2, Serial0/0/1

```

Step 2: establecer la interfaz pasiva como la interfaz predeterminada en el router.

- a. Emita el comando **passive-interface default** en el R2 para establecer todas las interfaces OSPFv3 como pasivas de manera predeterminada.

```

R2(config)# ipv6 router ospf 1
R2(config-rtr)# passive-interface default

```

```

R2(config)#ipv6 router ospf 1
R2(config-rtr)#passive-interface default
R2(config-rtr)#
01:24:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from FULL to D
OWN, Neighbor Down: Interface down or detached

01:24:28: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from FULL to D
OWN, Neighbor Down: Interface down or detached

R2(config-rtr)#

```

- b. Emita el comando **show ipv6 ospf neighbor** en el R1. Una vez que el temporizador de tiempo muerto caduca, el R2 ya no se muestra como un vecino OSPF.

R1# **show ipv6 ospf neighbor**

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:37	6	Serial0/0/1

R1#show ipv6 ospf neighbor

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:31	3	Serial0/0/1

R1#

- c. En el R2, emita el comando **show ipv6 ospf interface s0/0/0** para ver el estado OSPF de la interfaz S0/0/0.

R2# **show ipv6 ospf interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Link Local Address FE80::2, Interface ID 6

Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2

Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

No Hellos (Passive interface)

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 2, maximum is 3

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

```

R2#show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
Link Local Address FE80::2 , Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
R2#

```

- d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.

```

R1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:A::/64 [0/0]
  via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:A::1/128 [0/0]
  via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:C::/64 [110/65]
  via FE80::3, Serial0/0/1
C 2001:DB8:ACAD:12::/64 [0/0]
  via ::, Serial0/0/0
L 2001:DB8:ACAD:12::1/128 [0/0]
  via ::, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
  via ::, Serial0/0/1
L 2001:DB8:ACAD:13::1/128 [0/0]
  via ::, Serial0/0/1
O 2001:DB8:ACAD:23::/64 [110/128]
  via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
  via ::, Null0
R1#

R3#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
O 2001:DB8:ACAD:A::/64 [110/65]
  via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:C::/64 [0/0]
  via ::, GigabitEthernet0/0
L 2001:DB8:ACAD:C::3/128 [0/0]
  via ::, GigabitEthernet0/0
O 2001:DB8:ACAD:12::/64 [110/128]
  via FE80::1, Serial0/0/0
C 2001:DB8:ACAD:13::/64 [0/0]
  via ::, Serial0/0/0
L 2001:DB8:ACAD:13::3/128 [0/0]
  via ::, Serial0/0/0
C 2001:DB8:ACAD:23::/64 [0/0]
  via ::, Serial0/0/1
L 2001:DB8:ACAD:23::3/128 [0/0]
  via ::, Serial0/0/1
L FF00::/8 [0/0]
  via ::, Null0
R3#

```

- e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.

```
R2(config)# ipv6 router ospf 1
```

```
R2(config-rtr)# no passive-interface s0/0/1
```

```
*Apr 8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/1
R2(config-rtr)#
01:30:24: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-rtr)#
```

- f. Vuelva a emitir los comandos **show ipv6 route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 2001:DB8:ACAD:B::/64.

```
R1#show ipv6 route
```

```
IPv6 Routing Table - 10 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

```
U - Per-user Static route, M - MIPv6
```

```
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
```

```
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext
```

```
2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
D - EIGRP, EX - EIGRP external
```

```
C 2001:DB8:ACAD:A::/64 [0/0]
```

```
via ::, GigabitEthernet0/0
```

```
L 2001:DB8:ACAD:A::1/128 [0/0]
```

```
via ::, GigabitEthernet0/0
```

```
O 2001:DB8:ACAD:B::/64 [110/129]
```

```
via FE80::3, Serial0/0/1
```

```
O 2001:DB8:ACAD:C::/64 [110/65]
```

```
via FE80::3, Serial0/0/1
```

```
C 2001:DB8:ACAD:12::/64 [0/0]
```

```
via ::, Serial0/0/0
```

```
L 2001:DB8:ACAD:12::1/128 [0/0]
```

```
via ::, Serial0/0/0
```

```
C 2001:DB8:ACAD:13::/64 [0/0]
```

```
via ::, Serial0/0/1
```

```
L 2001:DB8:ACAD:13::1/128 [0/0]
```

```
via ::, Serial0/0/1
```

```
O 2001:DB8:ACAD:23::/64 [110/128]
```

```

via FE80::3, Serial0/0/1
L FF00::/8 [0/0]
via ::, Null0

```

```
R1#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	0	FULL/ -	00:00:39	3	Serial0/0/1

```
R3#show ipv6 route
```

IPv6 Routing Table - 10 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext

2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

```
O 2001:DB8:ACAD:A::/64 [110/65]
```

```
via FE80::1, Serial0/0/0
```

```
O 2001:DB8:ACAD:B::/64 [110/65]
```

```
via FE80::2, Serial0/0/1
```

```
C 2001:DB8:ACAD:C::/64 [0/0]
```

```
via ::, GigabitEthernet0/0
```

```
L 2001:DB8:ACAD:C::3/128 [0/0]
```

```
via ::, GigabitEthernet0/0
```

```
O 2001:DB8:ACAD:12::/64 [110/128]
```

```
via FE80::1, Serial0/0/0
```

```
via FE80::2, Serial0/0/1
```

```
C 2001:DB8:ACAD:13::/64 [0/0]
```

```
via ::, Serial0/0/0
```

```
L 2001:DB8:ACAD:13::3/128 [0/0]
```

```
via ::, Serial0/0/0
```

```
C 2001:DB8:ACAD:23::/64 [0/0]
```

```
via ::, Serial0/0/1
```

```
L 2001:DB8:ACAD:23::3/128 [0/0]
```

```
via ::, Serial0/0/1
```

```
L FF00::/8 [0/0]
```

```
via ::, Null0
```

```
R3#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	0	FULL/ -	00:00:32	4	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:39	4	Serial0/0/0

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64?

✓ O 2001:DB8:ACAD:B::/64 [110/129]

✓ via FE80::3, Serial0/0/1

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1?

✓ [110/129] 129

¿El R2 aparece como vecino OSPFv3 en el R1?

✓ NO

¿El R2 aparece como vecino OSPFv3 en el R3?

✓ SI

¿Qué indica esta información?

✓ Los paquetes enviados hacia la red 2001:DB8:ACAD:B::/64 que salen desde el router R1 son enviados primero hacia el router R3 ya que la interfaz S0/0/0 en el R2 fue configurada como pasiva.

g. En el R2, emita el comando **no passive-interface S0/0/0** para permitir que se anuncien las actualizaciones de routing OSPFv3 en esa interfaz.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#no passive-interface s0/0/0
R2(config-rtr)#
01:38:38: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING t
o FULL, Loading Done
```

```
R2(config-rtr)#
```

h. Verifique que el R1 y el R2 ahora sean vecinos OSPFv3.

```
R1#show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
2.2.2.2          0    FULL/ -         00:00:35   3             Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:30   3             Serial0/0/1
R1#
R1#
```

Reflexión

- Si la configuración OSPFv6 del R1 tiene la ID de proceso 1 y la configuración OSPFv3 del R2 tiene la ID de proceso 2, ¿se puede intercambiar información de routing entre ambos routers? ¿Por qué?
 - ✓ Estas ID no es necesario que coincida, si puede haber intercambio de información sin que estos sean los mismos.
- ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?
 - ✓ Por facilitar el proceso de configuración de IPV6.

Práctica de laboratorio: configuración de DHCPv4 básico en un router

Topología

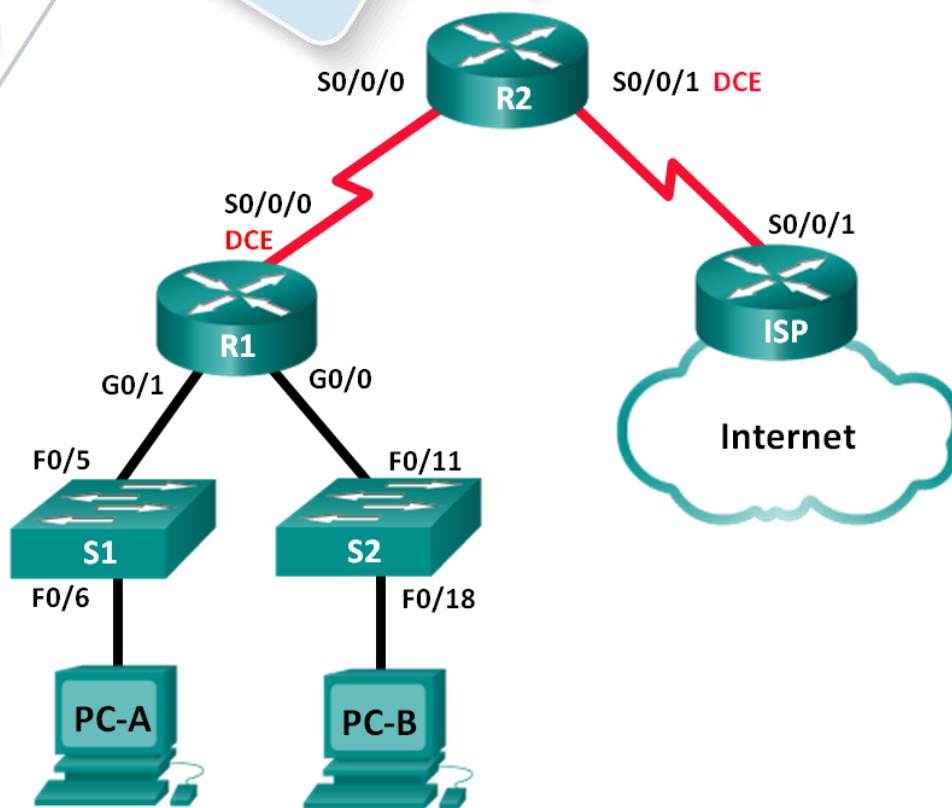


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP

PC-B	NIC	DHCP	DHCP	DHCP
------	-----	------	------	------

Objetivos

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

Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

Información básica/situación

El protocolo de configuración dinámica de host (DHCP) es un protocolo de red que permite a los administradores de red administrar y automatizar la asignación de direcciones IP. Sin DHCP, el administrador debe asignar y configurar manualmente las direcciones IP, los servidores DNS preferidos y los gateways predeterminados. A medida que aumenta el tamaño de la red, esto se convierte en un problema administrativo cuando los dispositivos se trasladan de una red interna a otra.

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv4 en dos subredes diferentes conectadas al router R1.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Part 9: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los routers y switches con los parámetros básicos, como las contraseñas y las direcciones IP. Además, configurará los parámetros de IP de las computadoras en la topología.

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

Step 2: inicializar y volver a cargar los routers y los switches.

Step 3: configurar los parámetros básicos para cada router.

R1

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip add 192.168.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int g0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int s0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#ip add 192.168.2.253 255.255.255.252
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#int s0/0/0
R2(config-if)#ip add 192.168.2.254 255.255.255.252
```

```
R2(config-if)#no sh
R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip add 209.165.200.226 255.255.255.224
R2(config-if)#no sh
```

- a. Desactive la búsqueda DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada de comandos.
- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.
- g. Configure la interfaz DCE serial en el R1 y el R2 con una frecuencia de reloj de 128000.

- h. Configure EIGRP for R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.255
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 192.168.2.252 0.0.0.3
R1(config-router)# no auto-summary
```

- i. Configure EIGRP y una ruta predeterminada al ISP en el R2.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- j. Configure una ruta estática resumida en el ISP para llegar a las redes en los routers R1 y R2.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

- k. Copie la configuración en ejecución en la configuración de inicio

Step 4: verificar la conectividad de red entre los routers.

Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso. Use los comandos **show ip route** y **show ip interface brief** para detectar posibles problemas.

Step 5: verificar que los equipos host estén configurados para DHCP.

Part 10: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP

— Para asignar automáticamente la información de dirección en la red, configure el R2 como servidor de DHCPv4 y el R1 como agente de retransmisión DHCP.

Step 1: configurar los parámetros del servidor de DHCPv4 en el router R2.

En el R2, configure un conjunto de direcciones DHCP para cada LAN del R1. Utilice el nombre de conjunto **R1G0** para G0/0 LAN y **R1G1** para G0/1 LAN. Asimismo, configure las direcciones que se excluirán de los conjuntos de direcciones. La práctica recomendada indica que primero se deben configurar las direcciones excluidas, a fin de garantizar que no se arrienden accidentalmente a otros dispositivos.

Excluya las primeras nueve direcciones en cada LAN del R1; empiece por .1. El resto de las direcciones deben estar disponibles en el conjunto de direcciones DHCP. Asegúrese de que cada conjunto de direcciones DHCP incluya un gateway predeterminado, el dominio **ccna-lab.com**, un servidor DNS (209.165.200.225) y un tiempo de arrendamiento de dos días.

En las líneas a continuación, escriba los comandos necesarios para configurar los servicios DHCP en el router R2, incluso las direcciones DHCP excluidas y los conjuntos de direcciones DHCP.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar DHCP en el R1 y el R2 sin consultar el apéndice.

Configuración de R2 (DHCP)

```
R2(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)#ip dhcp pool R1G0
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
R2(dhcp-config)#dns-server 209.165.200.225
R2(dhcp-config)#ex
R2(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)#ip dhcp pool R1G1
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 209.165.200.225
```

En la PC-A o la PC-B, abra un símbolo del sistema e introduzca el comando **ipconfig /all**. ¿Alguno de los equipos host recibió una dirección IP del servidor de DHCP? ¿Por qué?

Los equipos host no reciben las direcciones IP en R2 hasta que R1 no esté configurado.

Step 2: configurar el R1 como agente de retransmisión DHCP.

Configure las direcciones IP de ayuda en el R1 para que reenvíen todas las solicitudes de DHCP al servidor de DHCP en el R2.

En las líneas a continuación, escriba los comandos necesarios para configurar el R1 como agente de retransmisión DHCP para las LAN del R1.

```
R1>en
R1#conf t
R1(config)#int g0/0
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ip helper-address 192.168.2.254
R1(config-if)#exit
R1(config)#
```

Step 3: registrar la configuración IP para la PC-A y la PC-B.

En la PC-A y la PC-B, emita el comando **ipconfig /all** para verificar que las computadoras recibieron la información de la dirección IP del servidor de DHCP en el R2. Registre la dirección IP y la dirección MAC de cada computadora.

PC-A: 192.168.1.10 00E0.F9D7.10B6

PC-B: 192.168.0.10 0030.A332.C33E

Según el pool de DHCP que se configuró en el R2, ¿cuáles son las primeras direcciones IP disponibles que la PC-A y la PC-B pueden arrendar?

PC-B: 192.168.0.10 y PC-A: 192.168.1.10



Step 4: verificar los servicios DHCP y los arrendamientos de direcciones en el R2.

- a. En el R2, introduzca el comando **show ip dhcp binding** para ver los arrendamientos de direcciones DHCP.

Junto con las direcciones IP que se arrendaron, ¿qué otra información útil de identificación de cliente aparece en el resultado?

También las direcciones hardware cliente para saber que otras computadoras se unieron a la red.

- b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

Diez tipos de mensajes DHCP

- c. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.

En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current index)?

La próxima dirección de arrendamiento que se encuentre disponible.

- d. En el R2, introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.

- e. En el R2, introduzca el comando **show run interface** para las interfaces G0/0 y G0/1 para ver la configuración de retransmisión DHCP en la configuración en ejecución.

Reflexión

¿Cuál cree que es el beneficio de usar agentes de retransmisión DHCP en lugar de varios routers que funcionen como servidores de DHCP?

Tener un servidor de DHCP del router independiente para cada subred agregaría más complejidad y disminuir la administración centralizada de la red.




Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Apéndice A: comandos de configuración de DHCP

Router R1

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
```

```
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
```

Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología

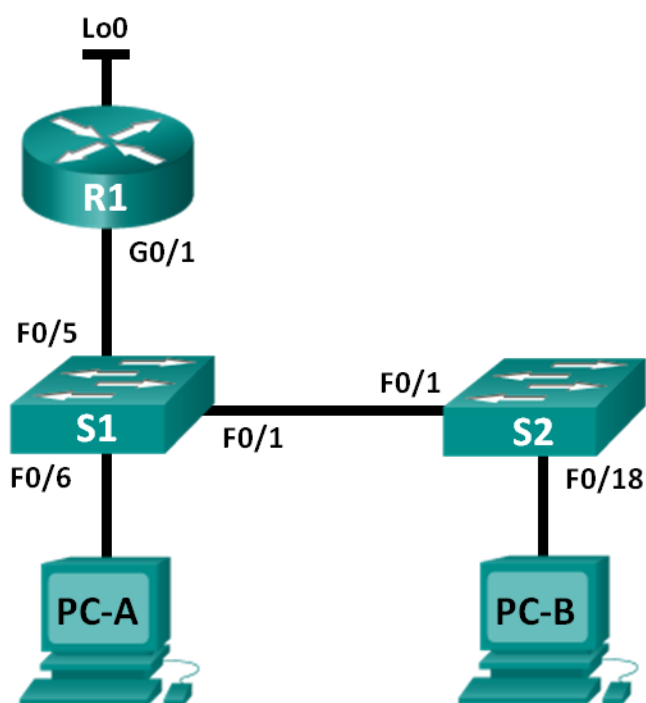


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.25	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Objetivos

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

Parte 2: cambiar la preferencia de SDM

- Establecer la preferencia de SDM en lanbase-routing en el S1.

Parte 3: configurar DHCPv4

- Configurar DHCPv4 para la VLAN 1.
- Verificar la conectividad y DHCPv4.

Parte 4: configurar DHCP para varias VLAN

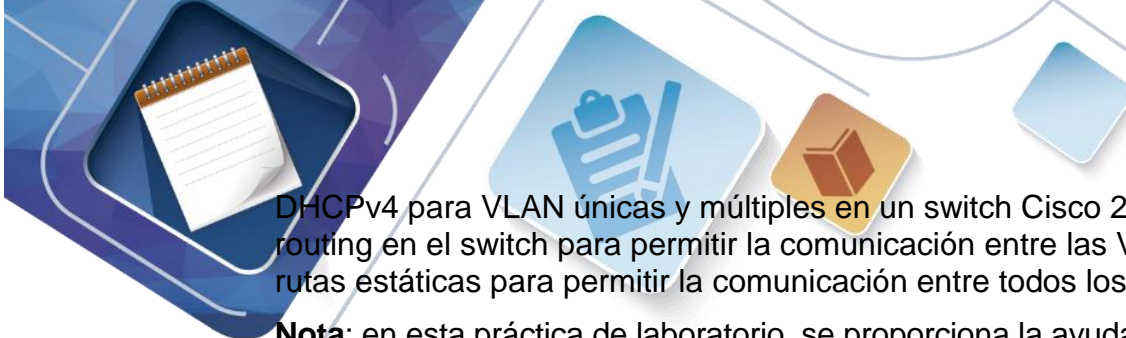
- Asignar puertos a la VLAN 2.
- Configurar DHCPv4 para la VLAN 2.
- Verificar la conectividad y DHCPv4.

Parte 5: habilitar el routing IP

- Habilite el routing IP en el switch.
- Crear rutas estáticas.

Información básica/situación

Un switch Cisco 2960 puede funcionar como un servidor de DHCPv4. El servidor de DHCPv4 de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones identificados que están asociados a VLAN específicas e interfaces virtuales de switch (SVI). El switch Cisco 2960 también puede funcionar como un dispositivo de capa 3 y hacer routing entre VLAN y una cantidad limitada de rutas estáticas. En esta práctica de laboratorio, configurará



DHCPv4 para VLAN únicas y múltiples en un switch Cisco 2960, habilitará el routing en el switch para permitir la comunicación entre las VLAN y agregará rutas estáticas para permitir la comunicación entre todos los hosts.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar DHCP. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

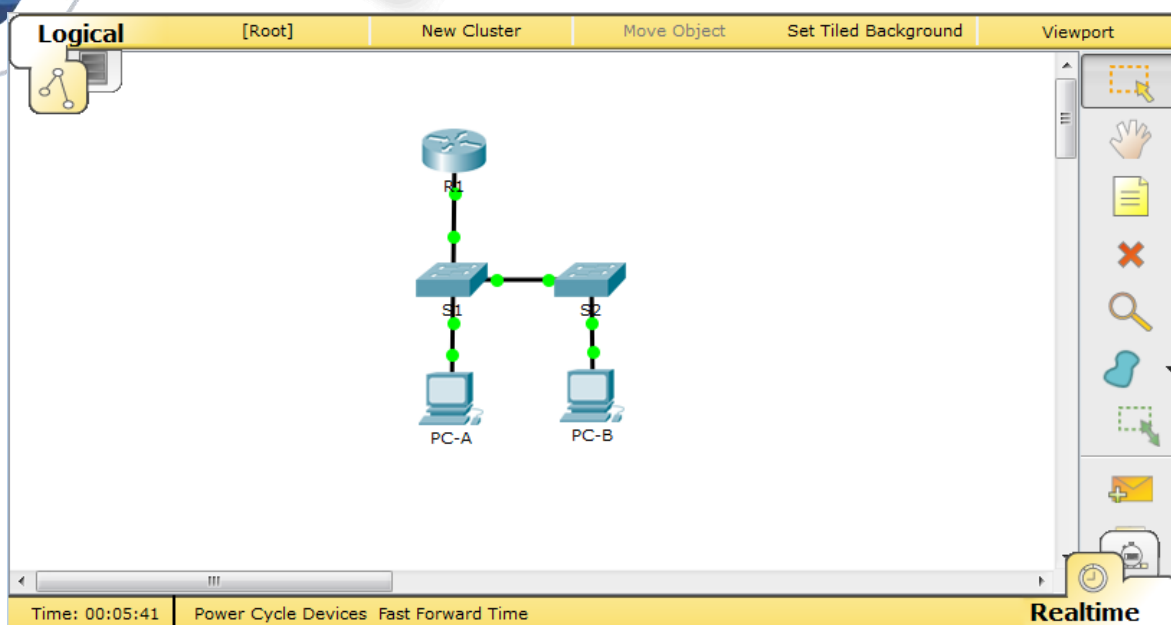
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 11: armar la red y configurar los parámetros básicos de los dispositivos



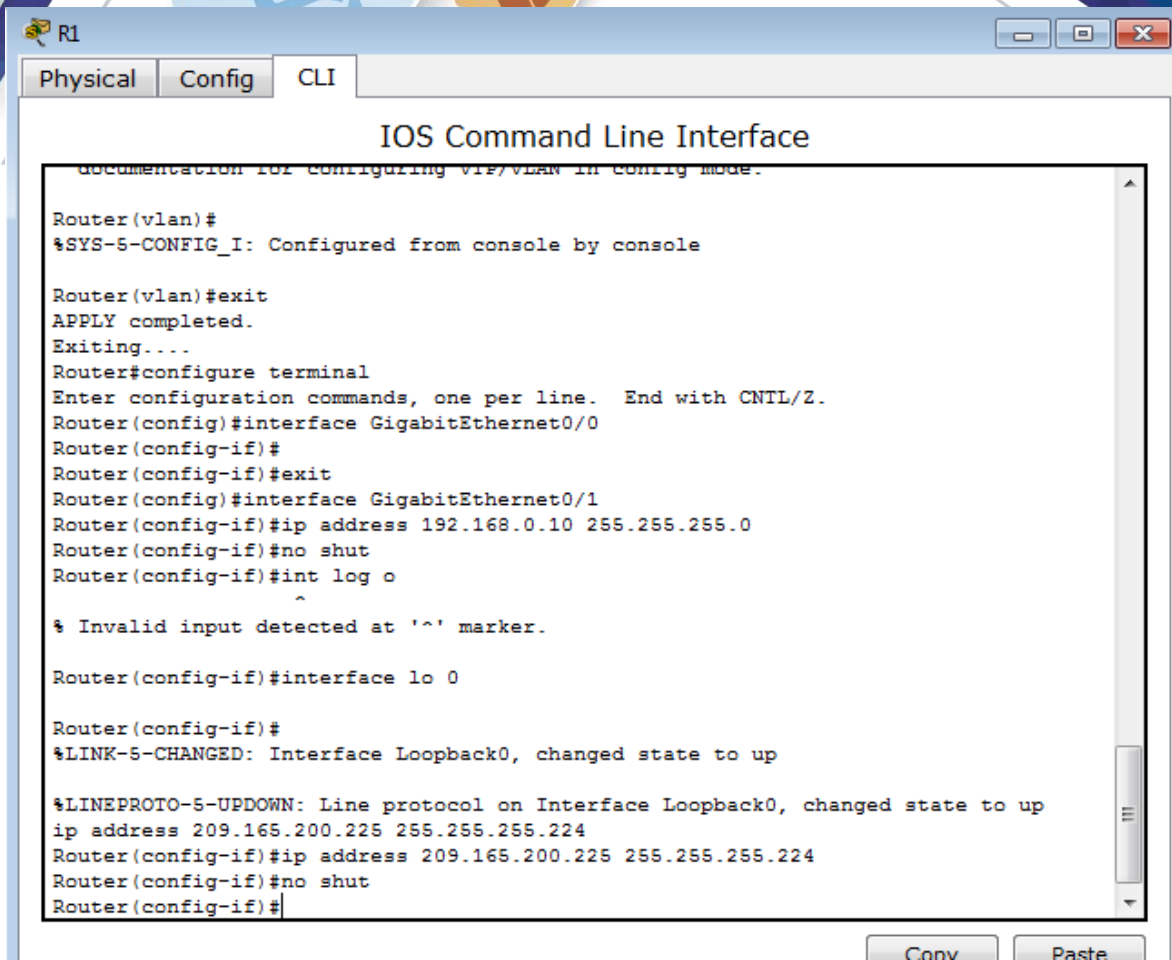
Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y switches.



Paso 3: configurar los parámetros básicos en los dispositivos.

- a. Asigne los nombres de dispositivos como se muestra en la topología.
- b. Desactive la búsqueda del DNS.
- c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- d. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.
- e. Configure las direcciones IP en las interfaces VLAN 1 y VLAN 2 del S1, según la tabla de direccionamiento.
- f. Guarde la configuración en ejecución en el archivo de configuración de inicio.



```
documentation for configuring VIF/VLAN in config mode.

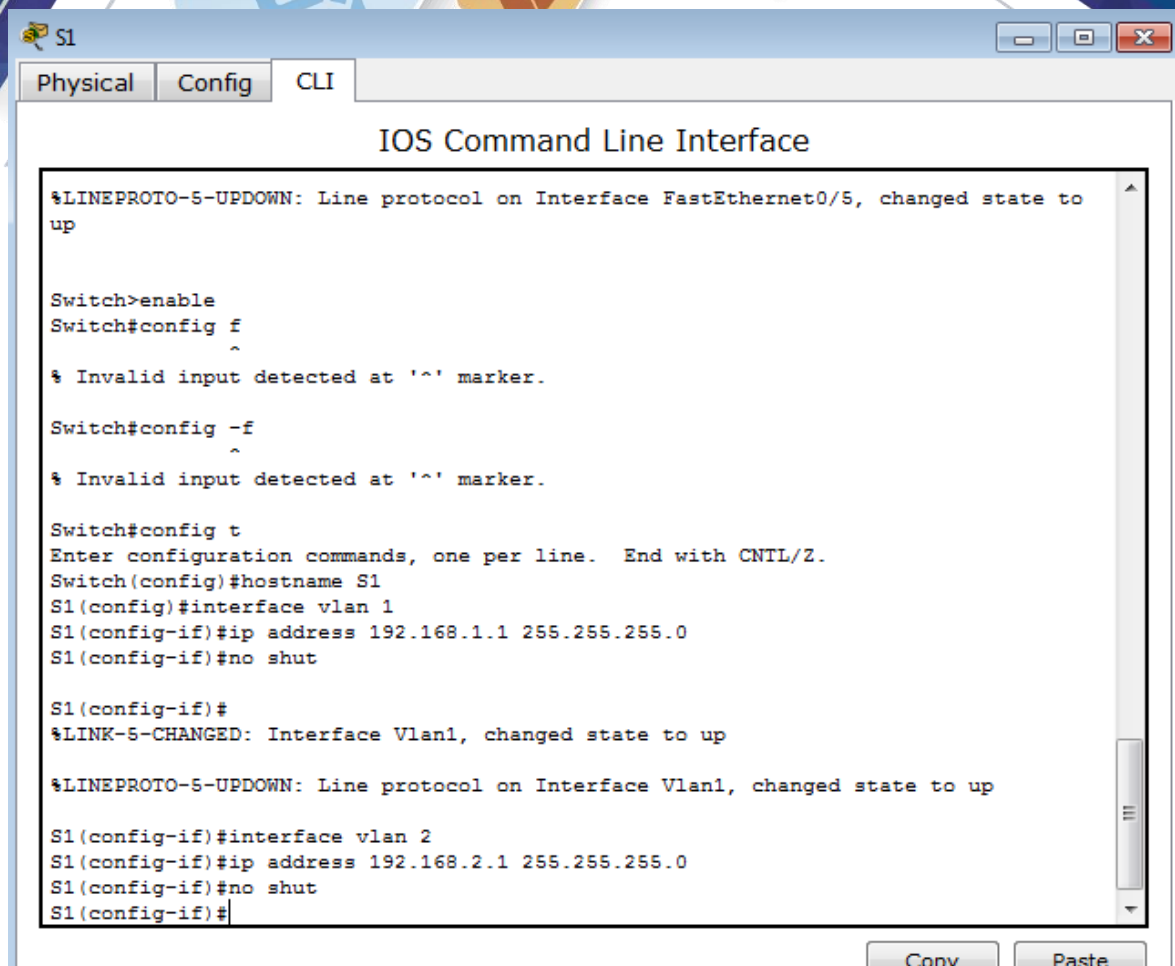
Router(vlan)#
%SYS-5-CONFIG_I: Configured from console by console

Router(vlan)#exit
APPLY completed.
Exiting....
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.0.10 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int log o
^
% Invalid input detected at '^' marker.

Router(config-if)#interface lo 0

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip address 209.165.200.225 255.255.255.224
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shut
Router(config-if)#
```



```

S1
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
up

Switch>enable
Switch#config f
^
% Invalid input detected at '^' marker.

Switch#config -f
^
% Invalid input detected at '^' marker.

Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#interface vlan 2
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#
  
```

Parte 12: cambiar la preferencia de SDM

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch Cisco 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. En esta práctica de laboratorio, la plantilla **lanbase-routing** está habilitada para permitir que el switch realice el routing entre VLAN y admita el routing estático.

Paso 1: mostrar la preferencia de SDM en el S1.

En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

S1# **show sdm prefer**

The current template is "default" template.

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	8K
number of IPv4 IGMP groups:	0.25K
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k

¿Cuál es la plantilla actual?

Default o en caso de cambiar la planilla será dual-ipv4-and-ipv6 default.

```
S1#show sdm prefer
^
% Invalid input detected at '^' marker.
S1#
```

Paso 2: cambiar la preferencia de SDM en el S1.

- a. Establezca la preferencia de SDM en **lanbase-routing**. (Si lanbase-routing es la plantilla actual, continúe con la parte 3). En el modo de configuración global, emita el comando **sdm prefer lanbase-routing**.

S1(config)# **sdm prefer lanbase-routing**

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga? **lanbase-routing**

```
S1#config
Configuring from terminal, memory, or network [terminal]? config
?Must be "terminal", "memory" or "network"
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#sdm prefer lanbase-routing
^
% Invalid input detected at '^' marker.
S1(config)#
```

- b. Se debe volver a cargar el switch para que la plantilla esté habilitada.

S1# **reload**

System configuration has been modified. Save? [yes/no]: **no**
 Proceed with reload? [confirm]

Nota: la nueva plantilla se utilizará después del reinicio, incluso si no se guardó la configuración en ejecución. Para guardar la configuración en

ejecución, responda **yes** (sí) para guardar la configuración modificada del sistema.

```

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#reload
Proceed with reload? [confirm]
  
```

Paso 3: verificar que la plantilla lanbase-routing esté cargada.

Emita el comando **show sdm prefer** para verificar si la plantilla lanbase-routing se cargó en el S1.

S1# show sdm prefer

The current template is "lanbase-routing" template.
 The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0.75K
number of directly-connected IPv4 hosts:	0.75K
number of indirect IPv4 routes:	16
number of IPv6 multicast groups:	0.375k
number of directly-connected IPv6 addresses:	0.75K
number of indirect IPv6 unicast routes:	16
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.375k
number of IPv6 security aces:	127

Parte 13: configurar DHCPv4

En la parte 3, configurará DHCPv4 para la VLAN 1, revisará las configuraciones IP en los equipos host para validar la funcionalidad de DHCP y verificará la conectividad de todos los dispositivos en la VLAN 1.

Paso 1: configurar DHCP para la VLAN 1.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

Ip dhcp excluded-address

```
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#
```

- Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.

Ip dhcp pool DHCP1

```
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#
```

- Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

Network

```
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#
```

- Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

Default-router

```
S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#
```

- Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

Dns-server

```
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#
```

- Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

```
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.
S1(dhcp-config)#
```

- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 2: verificar la conectividad y DHCP.

- a. En la PC-A y la PC-B, abra el símbolo del sistema y emita el comando **ipconfig**. Si la información de IP no está presente, o si está incompleta, emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: **192.168.1.11**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**

```

PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::206:2AFF:FEE2:2111
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::206:2AFF:FEE2:2111
IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

PC>exit
PC>

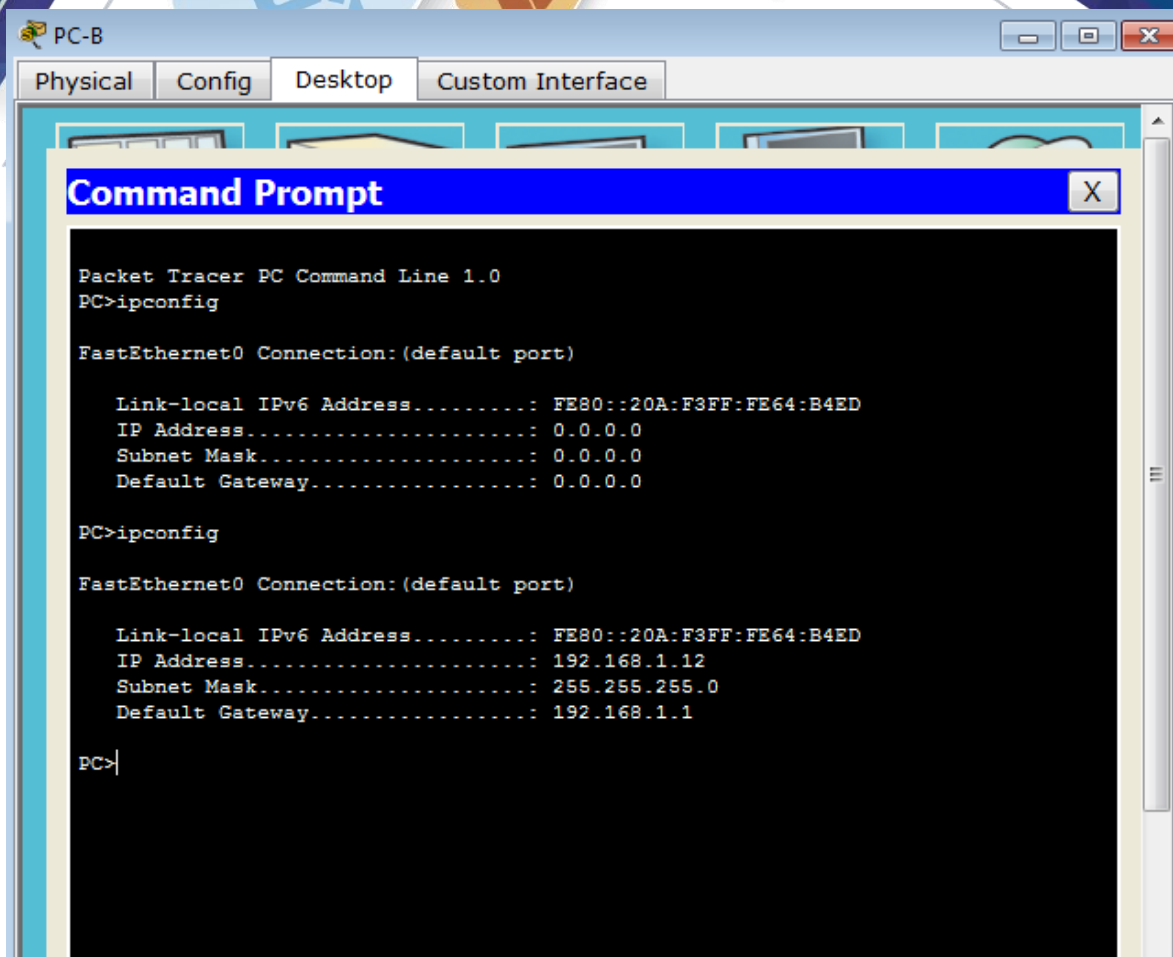
```

Para la PC-B, incluya lo siguiente:

Dirección IP: **192.168.1.12**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.1.1**



```
PC-B
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::20A:F3FF:FE64:B4ED
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

PC>ipconfig

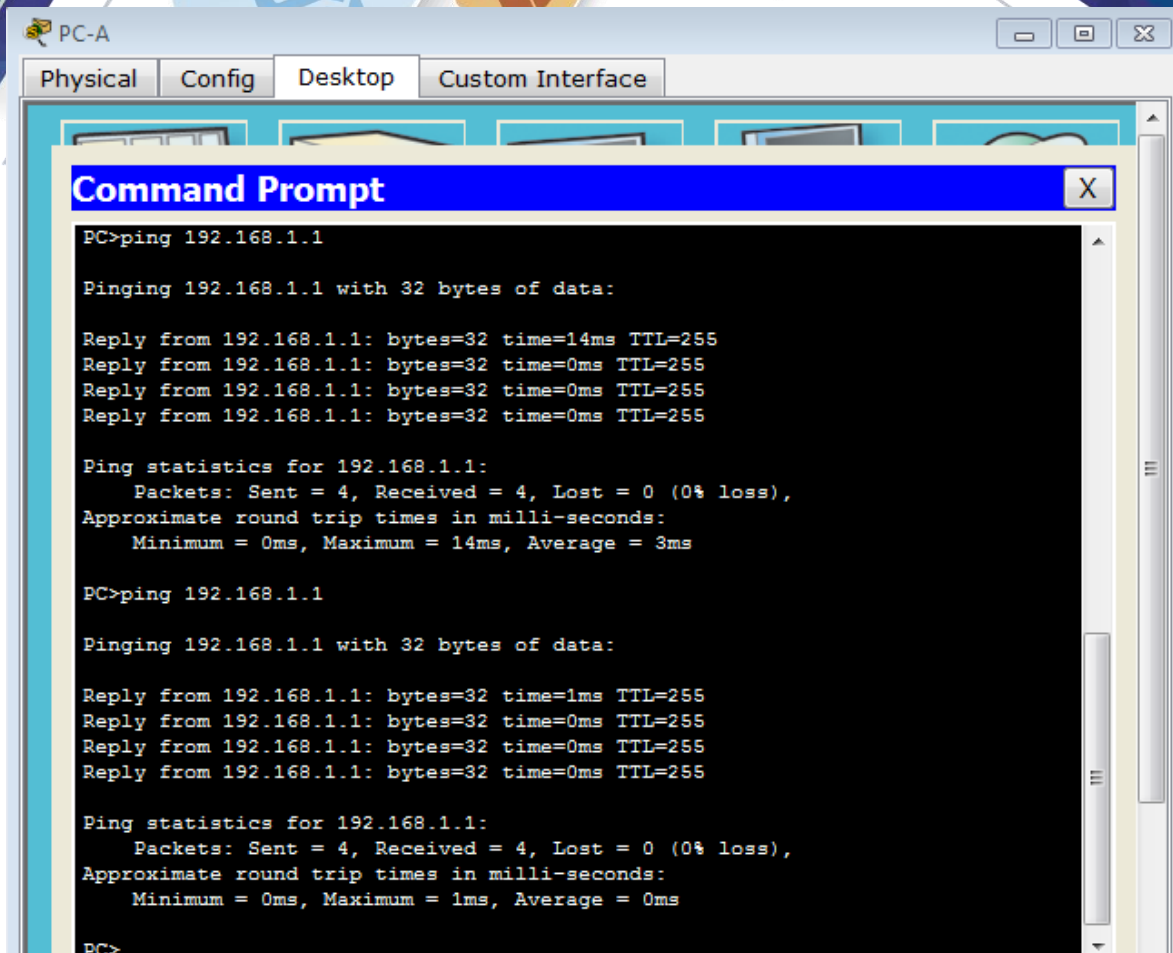
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::20A:F3FF:FE64:B4ED
IP Address.....: 192.168.1.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

PC>
```

b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 1? **Si**



The image shows a screenshot of a PC-A Command Prompt window. The window title is "PC-A" and it has tabs for "Physical", "Config", "Desktop", and "Custom Interface". The Command Prompt window has a blue title bar with "Command Prompt" and a close button. The text inside the window shows two successful ping operations to the IP address 192.168.1.1. The first ping shows a time of 14ms, and the second shows a time of 1ms. Both show 0% loss and 4 packets sent and received.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=14ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

PC>ping 192.168.1.1

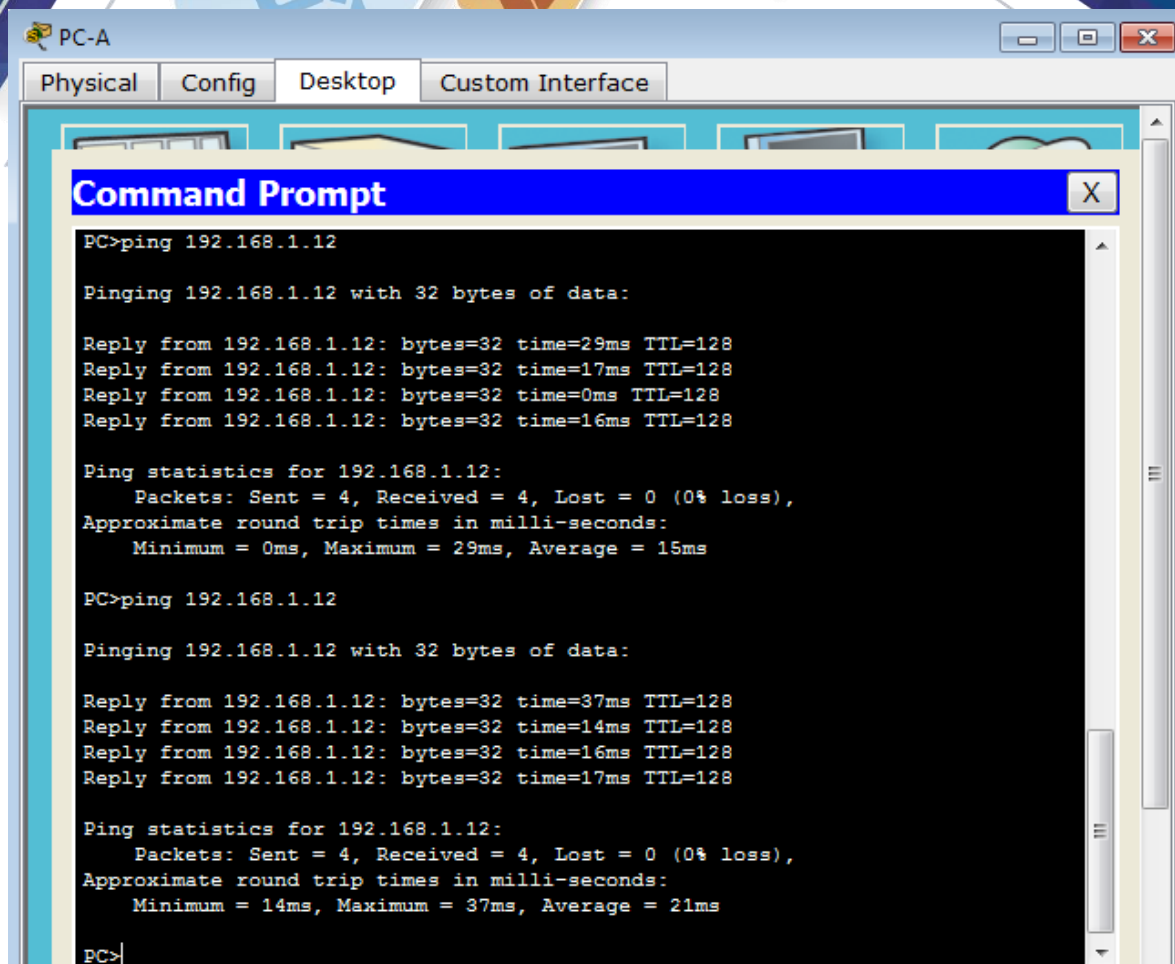
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

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



The screenshot shows a virtual PC environment titled 'PC-A' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. A 'Command Prompt' window is open, displaying the following text:

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=29ms TTL=128
Reply from 192.168.1.12: bytes=32 time=17ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 15ms

PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=37ms TTL=128
Reply from 192.168.1.12: bytes=32 time=14ms TTL=128
Reply from 192.168.1.12: bytes=32 time=16ms TTL=128
Reply from 192.168.1.12: bytes=32 time=17ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 37ms, Average = 21ms

PC>
```

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? **Si**

```

PC-A
Physical Config Desktop Custom Interface

Command Prompt

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=84ms TTL=255
Reply from 192.168.1.10: bytes=32 time=14ms TTL=255
Reply from 192.168.1.10: bytes=32 time=14ms TTL=255
Reply from 192.168.1.10: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 84ms, Average = 31ms

PC>
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=13ms TTL=255
Reply from 192.168.1.10: bytes=32 time=14ms TTL=255
Reply from 192.168.1.10: bytes=32 time=5ms TTL=255
Reply from 192.168.1.10: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 14ms, Average = 11ms

PC>
  
```

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

Parte 14: configurar DHCPv4 para varias VLAN

En la parte 4, asignará la PC-A un puerto que accede a la VLAN 2, configurará DHCPv4 para la VLAN 2, renovará la configuración IP de la PC-A para validar DHCPv4 y verificará la conectividad dentro de la VLAN.

Paso 1: asignar un puerto a la VLAN 2.

Coloque el puerto F0/6 en la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

Switchport mode

```

S1(config)#interface fa/06
^
% Invalid input detected at '^' marker.

S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access
% Incomplete command.
S1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

S1(config-if)#

```

Paso 2: configurar DHCPv4 para la VLAN 2.

- Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.
- Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.
- Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

```

S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#

```

- Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 3: verificar la conectividad y DHCPv4.

- En la PC-A, abra el símbolo del sistema y emita el comando **ipconfig /release**, seguido del comando **ipconfig /renew**.

Para la PC-A, incluya lo siguiente:

Dirección IP: _____

Máscara de subred: _____

Gateway predeterminado: _____

```

PC-A
Physical Config Desktop Custom Interface
Command Prompt
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=13ms TTL=255
Reply from 192.168.1.10: bytes=32 time=14ms TTL=255
Reply from 192.168.1.10: bytes=32 time=5ms TTL=255
Reply from 192.168.1.10: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 14ms, Average = 11ms

PC>ipconfig /release

IP Address. . . . . : 0.0.0.0
Subnet Mask. . . . . : 0.0.0.0
Default Gateway. . . . . : 0.0.0.0
DNS Server. . . . . : 0.0.0.0

PC>ipconfig /renew

IP Address. . . . . : 192.168.2.11
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . : 192.168.2.1
DNS Server. . . . . : 192.168.2.9

PC>

```

b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado de la VLAN 2 y a la PC-B.

¿Es posible hacer ping de la PC-A al gateway predeterminado? **Si**

¿Es posible hacer ping de la PC-A a la PC-B? **No**

¿Los pings eran correctos? ¿Por qué?

El ping de la PC-A al Gateway predeterminado es posible ya que están en la misma red, en cambio entre PC-A y PC-B no fue posible porque pertenecen a redes diferentes.

```

PC-A
Physical Config Desktop Custom Interface
IP Dial-up Terminal Command Web Browser
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=3ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
PC>ping 192.168.1.12
Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
  
```

c. Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?

```

S1(config)#show ip route
^
% Invalid input detected at '^' marker.

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show ip route
^
% Invalid input detected at '^' marker.

S1#
  
```

Parte 15: habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN. Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

Paso 1: habilitar el routing IP en el S1.

- a. En el modo de configuración global, utilice el comando **ip routing** para habilitar el routing en el S1.

S1(config)# **ip routing**

- b. Verificar la conectividad entre las VLAN.

¿Es posible hacer ping de la PC-A a la PC-B? **Si**

¿Qué función realiza el switch?

Rotiando los paquetes entre vlans

- c. Vea la información de la tabla de routing para el S1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Dos redes directamente conectadas, 2 Vlan's

- d. Vea la información de la tabla de routing para el R1.

¿Qué información de la ruta está incluida en el resultado de este comando?

Muestra dos redes directamente conectada solo en la red 1 y no tiene entrada a la 192.168.2.0

- e. ¿Es posible hacer ping de la PC-A al R1? **No**

¿Es posible hacer ping de la PC-A a la interfaz Lo0? **No**

Considere la tabla de routing de los dos dispositivos, ¿qué se debe agregar para que haya comunicación entre todas las redes?

Para que corra la comunicación entre todas las redes, estas deben ser agregadas en la tabla.

Paso 2: asignar rutas estáticas.

Habilitar el routing IP permite que el switch enrute entre VLAN asignadas en el switch. Para que todas las VLAN se comuniquen con el router, es necesario agregar rutas estáticas a la tabla de routing del switch y del router.

- a. En el S1, cree una ruta estática predeterminada al R1. En el espacio proporcionado, escriba el comando que utilizó.

Ip route

- b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.



Ip route

- c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

Está representada como puerta de enlace de último recurso


- d. Vea la información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

Está representada en una de los enlaces Gigabit




- e. ¿Es posible hacer ping de la PC-A al R1? **Si**

¿Es posible hacer ping de la PC-A a la interfaz Lo0? **Si**





Reflexión

- 
- 
- 
1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Apéndice A: comandos de configuración

Configurar DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

Configurar DHCPv4 para varias VLAN

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
```

```
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

Habilitar routing IP

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

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

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)

- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcione correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Nota: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

S1# **show sdm prefer**

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

S1# **config t**

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**



```
S1(config)# end  
S1# reload
```

Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Nota: los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

Part 16: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

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

Step 2: inicializar y volver a cargar el router y el switch según sea necesario.

Step 3: Configurar R1

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Guardar la configuración en ejecución en la configuración de inicio.




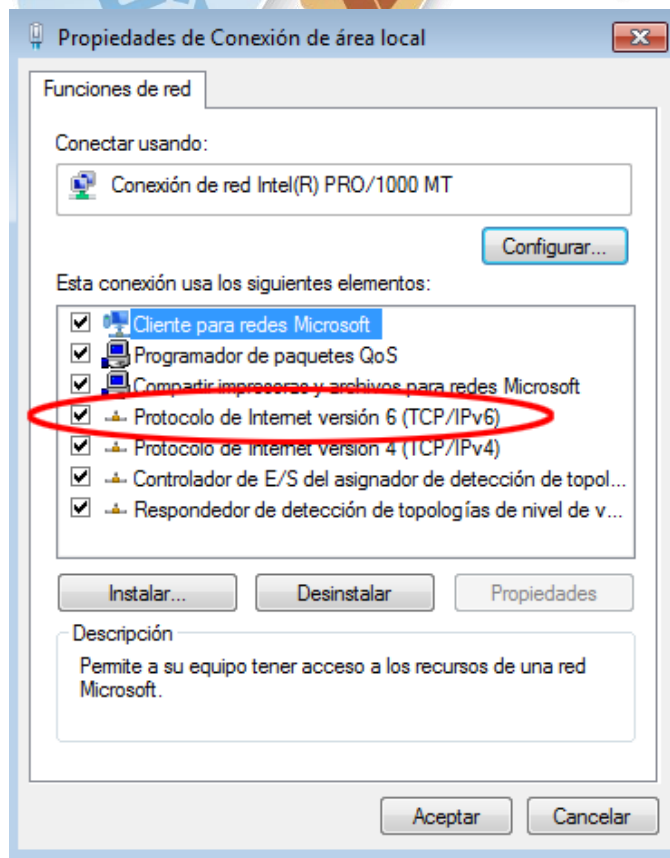
Step 4: configurar el S1.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

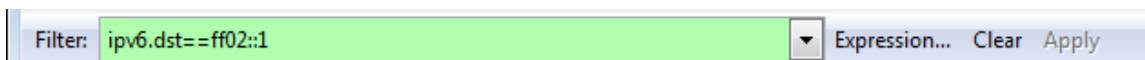
Part 17: configurar la red para SLAAC

Step 1: preparar la PC-A.

- a. Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.
- 



- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.



Step 2: Configurar R1

- a. Habilite el routing de unidifusión IPv6.
- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- d. Active la interfaz G0/1.

Step 3: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Step 4: configurar el S1.

Use el comando **ipv6 address autoconfig** en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

Step 5: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

S1# show ipv6 interface

Vlan1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40

No Virtual link-local address(es):

Stateless address autoconfig enabled

Global unicast address(es):

2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is
2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]

valid lifetime 2591988 preferred lifetime 604788

Joined group address(es):

FF02::1

FF02::1:FFE8:8A40

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachable are sent

Output features: Check hwidb

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND NS retransmit interval is 1000 milliseconds

Default router is FE80::1 on Vlan1

Step 6: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

- a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

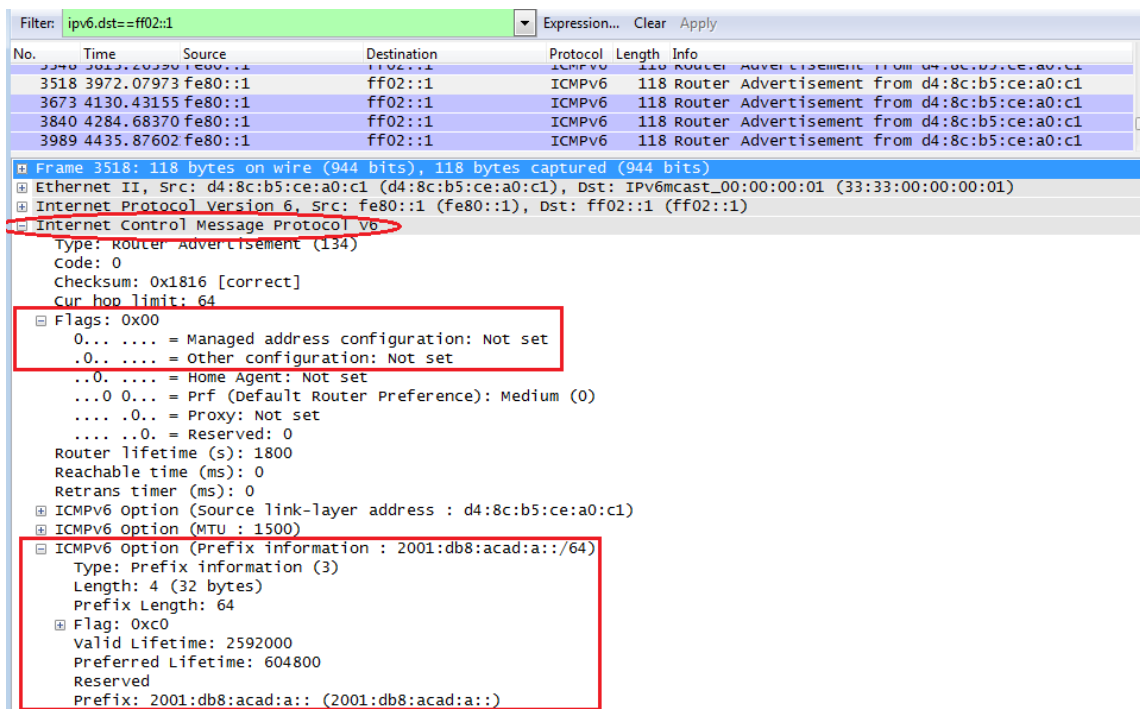
```

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . . . . : 
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Vínculo: dirección IPv6 local. . . . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>

Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1:1
Servidores DNS . . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

- b. En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.



Filter: `ipv6.dst==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
3518	3972.07973	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3673	4130.43155	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3840	4284.68370	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3989	4435.87602	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x1816 [correct]
 - Cur_hop_limit: 64
 - Flags: 0x00
 - 0... .. = Managed address configuration: Not set
 - .0... .. = Other configuration: Not set
 - ..0... .. = Home Agent: Not set
 - ...0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0.. = Reserved: 0
 - Router lifetime (s): 1800
 - Reachable time (ms): 0
 - Retrans timer (ms): 0
 - ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
 - ICMPv6 option (MTU : 1500)
 - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
 - Type: Prefix information (3)
 - Length: 4 (32 bytes)
 - Prefix Length: 64
 - Flag: 0xc0
 - Valid Lifetime: 2592000
 - Preferred Lifetime: 604800
 - Reserved
 - Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

Part 18: configurar la red para DHCPv6 sin estado

Step 1: configurar un servidor de DHCP IPv6 en el R1.

- Cree un pool de DHCP IPv6.
R1(config)# **ipv6 dhcp pool IPV6POOL-A**
- Asigne un nombre de dominio al pool.
R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**
- Asigne una dirección de servidor DNS.
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**
- Asigne el pool de DHCPv6 a la interfaz.
R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**
- Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.
R1(config-if)# **ipv6 nd other-config-flag**

R1(config-if)# end

Step 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

R1# **show ipv6 interface g0/1**

```
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.
```

Step 3: ver los cambios realizados en la red en la PC-A.

Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

```

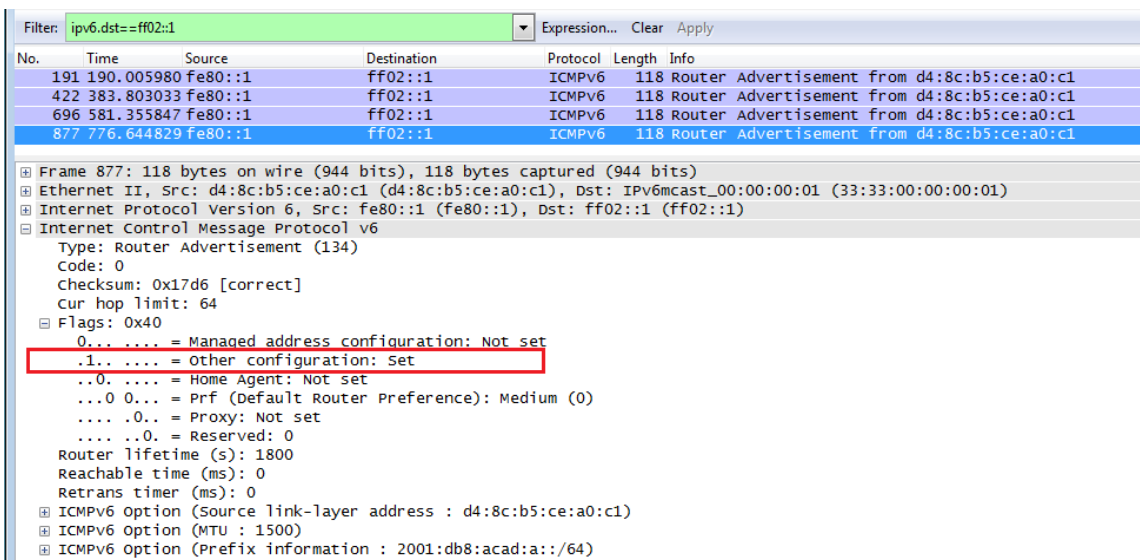
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Uínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>

Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::1%11
IAID DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-
E3-23-17
Servidores DNS . . . . . : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.localdomain:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : ccna-statelessDHCPv6.com
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí
  
```

Step 4: ver los mensajes RA en Wireshark.

Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.







```

Filter: ipv6.dst==ff02::1
No. Time Source Destination Protocol Length Info
191 190.005980 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
422 383.803033 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
696 581.355847 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1
877 776.644829 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x17d6 [correct]
Cur hop limit: 64
Flags: 0x40
0... .. = Managed address configuration: Not set
1... .. = Other configuration: Set
..0... .. = Home Agent: Not set
...0... = Prf (Default Router Preference): Medium (0)
....0.. = Proxy: Not set
.....0. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
ICMPv6 Option (MTU : 1500)
ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
  
```

Step 5: verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.



```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

Step 6: restablecer la configuración de red IPv6 de la PC-A.

- a. Desactive la interfaz F0/6 del S1.

Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

```
S1(config)# interface f0/6
```

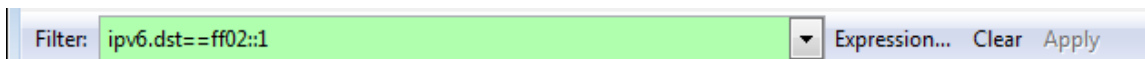
```
S1(config-if)# shutdown
```

- b. Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- c. Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
 - 1) Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.
 - 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

Part 19: configurar la red para DHCPv6 con estado

Step 1: preparar la PC-A.

- Inicie una captura del tráfico en la NIC con Wireshark.
- Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.



Step 2: cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
```

```
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

- Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

Nota: debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
```

```
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
```

```
R1(config-dhcpv6)# end
```

- Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
```

```
DHCPv6 pool: IPV6POOL-A
```

```
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)
```

```
DNS server: 2001:DB8:ACAD:A::ABCD
```

```
Domain name: ccna-StatefulDHCPv6.com
```

```
Active clients: 0
```

- Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

```
R1# debug ipv6 dhcp detail
```

```
IPv6 DHCP debugging is on (detailed)
```

Step 3: establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

```
R1(config)# interface g0/1
```

```
R1(config-if)# shutdown
```



```
R1(config-if)# ipv6 nd managed-config-flag  
R1(config-if)# no shutdown  
R1(config-if)# end
```

Step 4: habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

Step 5: verificar la configuración de DHCPv6 con estado en el R1.

- a. Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
Hosts use DHCP to obtain other configuration.
```

- b. En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.

- c. Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

- d. Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

R1# **show ipv6 dhcp binding**

Client: FE80::D428:7DE2:997C:B05A

DUID: 0001000117F6723D000C298D5444

Username : unassigned

IA NA: IA ID 0x0E00C29, T1 43200, T2 69120

Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE

preferred lifetime 86400, valid lifetime 172800

expires at Mar 07 2013 04:09 PM (171595 seconds)

```

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . : ccna-StatefulDHCPv6.com
  Descripción . . . . . : Conexión de red Intel(R) PRO/1000
  MT
  Dirección física. . . . . : 00-0C-29-E3-23-17
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
  Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
  16:07:59
  La concesión expira . . . . . : jueves, 05 de septiembre de 2013
  16:38:03
  Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
  Vínculo: dirección IPv6 local. . . . . : fe80::d428:7de2:997c:b05a%11<Preferido>
  Dirección IPv4. . . . . : 192.168.96.139<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%11
  IAID DHCPv6 . . . . . : 234884137
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
  Servidores DNS. . . . . : 2001:db8:acad:a::abcd
  NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

- e. Emita el comando **undebg all** en el R1 para detener la depuración de DHCPv6.

Nota: escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebg all** las detiene todas.

R1# **u all**

Se ha desactivado toda depuración posible

f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

*Mar 5 16:42:39.775: dst FF02::1:2

*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238

*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2

*Mar 5 16:42:39.775: elapsed-time 6300

*Mar 5 16:42:39.775: option CLIENTID(1), len 14

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1

*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents

*Mar 5 16:42:39.779: src FE80::1

*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)

*Mar 5 16:42:39.779: type REPLY(7), xid 1039238

*Mar 5 16:42:39.779: option SERVERID(2), len 10

*Mar 5 16:42:39.779: 00030001FC994775C3E0

*Mar 5 16:42:39.779: option CLIENTID(1), len 14

*Mar 5 16:42:39.779: 00010001

R1#17F6723D000C298D5444

*Mar 5 16:42:39.779: option IA-NA(3), len 40

*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120

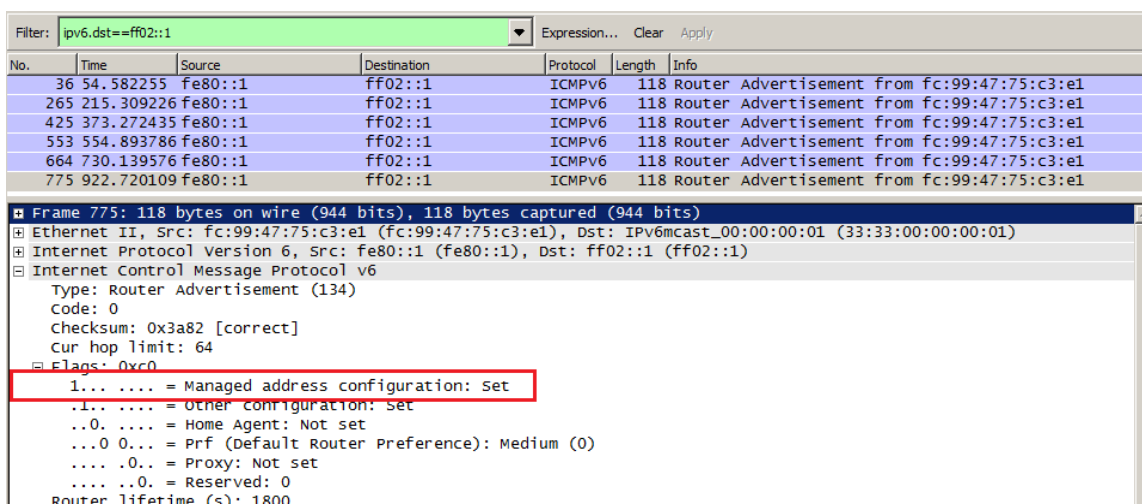
*Mar 5 16:42:39.779: option IAADDR(5), len 24

*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE

```
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```

Step 6: verificar DHCPv6 con estado en la PC-A.

- Detenga la captura de Wireshark en la PC-A.
- Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



Filter: `ipv6.dst==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
36	54.582255	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
265	215.309226	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
425	373.272435	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
553	554.893786	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
664	730.139576	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1
775	922.720109	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from fc:99:47:75:c3:e1

Frame 775: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x3a82 [correct]
 - Cur hop limit: 64
 - Flags: 0xc0
 - 1... .. = Managed address configuration: Set
 - .1... .. = Other configuration: Set
 - ..0. = Home Agent: Not set
 - ...0 0... = Prf (Default Router Preference): Medium (0)
 -0.. = Proxy: Not set
 -0. = Reserved: 0
 - Router lifetime (<) 1800

- Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.

Filter: dhcpv6 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c29
267	475.083284	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c29
425	656.281211	fe80::d428:7de2:997ff02::1:2		DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c29
429	656.282249	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c29
460	657.292018	fe80::d428:7de2:997ff02::1:2		DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c29
462	657.292638	fe80::1	fe80::d428:7de2:997ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298

Ethernet II, Src: fc:99:47:75:c3:e1 (Fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)
 Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)
 User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)
 DHCPv6

Message type: Reply (7)
 Transaction ID: 0xc86c32
 Server Identifier: 00030001fc994775c3e0
 Client Identifier: 0001000117f6723d000c298d5444
 Identity Association for Non-temporary Address
 Option: Identity Association for Non-temporary Address (3)
 Length: 40
 Value: 0e000c290000a8c000010e000005001820010db8acad000a...
 IAID: 0e000c29
 T1: 43200
 T2: 69120
 IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce
 DNS recursive name server
 Option: DNS recursive name server (23)
 Length: 16
 Value: 20010db8acad000a000000000000abcd
 DNS servers address: 2001:db8:acad:a:abcd
 Domain Search List
 Option: Domain Search List (24)
 Length: 25
 Value: 1363636e612d537461746566756c44484350763603636f6d...
 DNS Domain Search List
 Domain: ccna-statefulDHCPv6.com

Reflexión

1. ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?

DHCPv6 con estado utiliza más recursos de memoria. Las respuestas varían, pero DHCPv6 con estado requiere que el router almacene la información de estado dinámico de los clientes DHCPv6. Los clientes DHCPv6 sin estado no utilizan el servidor de DHCP para obtener información de dirección, de modo que no es necesario almacenarla.

2. ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

Cisco recomienda DHCPv6 sin estado para implementar redes IPv6 sin Cisco Network Registrar (CNR).

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Configuraciones de dispositivos: partes 1 y 2 combinadas para el R1 y el S1

Router R1 (después de las partes 1 y 2 de esta práctica de laboratorio)

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

no ip domain lookup

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

interface Embedded-Service-Engine0/0

no ip address

shutdown Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado © 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 16 de 21

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!

banner motd ^C

Unauthorized Access is Prohibited!

^C

!

line con 0

password 7 070C285F4D06

logging synchronous



login

line aux 0

!

line vty 0 4

password 7 13061E010803

login

transport input all

!

scheduler allocate 20000 1000

!

end Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado © 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 17 de 21

Switch S1 (después de las partes 1 y 2 de esta práctica de laboratorio)

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model



system mtu routing 1500

!

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

shutdown

!

interface FastEthernet0/2

shutdown

!

interface FastEthernet0/3

shutdown

!

interface FastEthernet0/4

shutdown

!

interface FastEthernet0/5

!

interface FastEthernet0/6



interface FastEthernet0/7

shutdown

!

interface FastEthernet0/8

shutdown

!

interface FastEthernet0/9

shutdown

!

interface FastEthernet0/10

shutdown

! Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 18 de 21

interface FastEthernet0/11

shutdown

!

interface FastEthernet0/12

shutdown

!

interface FastEthernet0/13

shutdown

!

interface FastEthernet0/14

shutdown





!
interface FastEthernet0/15

shutdown

!

interface FastEthernet0/16

shutdown

!

interface FastEthernet0/17

shutdown

!

interface FastEthernet0/18

shutdown

!

interface FastEthernet0/19

shutdown

!

interface FastEthernet0/20

shutdown

!

interface FastEthernet0/21

shutdown

!

interface FastEthernet0/22

shutdown

!



interface FastEthernet0/23

shutdown

!

interface FastEthernet0/24

shutdown

!

interface GigabitEthernet0/1

shutdown

!

interface GigabitEthernet0/2

shutdown

!

interface Vlan1 Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado © 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco. Página 19 de 21

no ip address

shutdown

!

ip http server

ip http secure-server

!


banner motd ^C

Unauthorized Access is Prohibited!

^C

!

line con 0



```
password 7 05080F1C2243
```

```
logging synchronous
```

```
login
```

```
line vty 0 4
```

```
password 7 02050D480809
```

```
login
```

```
line vty 5 15
```

```
password 7 02050D480809
```

```
login
```

```
!
```

```
end
```

```
Router R1 (Final)
```

```
service password-encryption
```

```
!
```

```
hostname R1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

```
!
```

```
no aaa new-model
```

```
memory-size iomem 15
```





no ip domain lookup

ip cef

ipv6 unicast-routing

ipv6 dhcp pool IPV6POOL-A

address prefix 2001:DB8:ACAD:A::/64

dns-server 2001:DB8:ACAD:A::ABCD

domain-name ccna-StatelfulDHCPv6.com

!

ipv6 cef

multilink bundle-name authenticated

!

interface GigabitEthernet0/0 Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado © 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.
Página 20 de 21

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:A::1/64



ipv6 nd managed-config-flag

ipv6 nd other-config-flag

ipv6 dhcp server IPV6POOL-A

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!


!

banner motd ^C

Unauthorized Access is Prohibited!

^C

!



```
line con 0
```

```
password 7 070C285F4D06
```

```
logging synchronous
```

```
login
```

```
line aux 0
```

```
!
```

```
line vty 0 4
```

```
password 7 13061E010803
```

```
login
```

```
transport input all
```

```
! Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado  
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este  
documento es información pública de Cisco. Página 21 de 21
```

```
scheduler allocate 20000 1000
```

```
!
```

```
end
```

IdT y DHCP

Objetivo

Configure DHCP para IPv4 o IPv6 en un router Cisco 1941.

Situación

En este capítulo, se presenta el concepto del uso del proceso de DHCP en la red de una pequeña a mediana empresa; sin embargo, el protocolo DHCP también tiene otros usos.

Con la llegada de Internet de todo (IdT), podrá acceder a todos los dispositivos en su hogar que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

Con Packet Tracer, realice las siguientes tareas para esta actividad de creación de modelos:

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

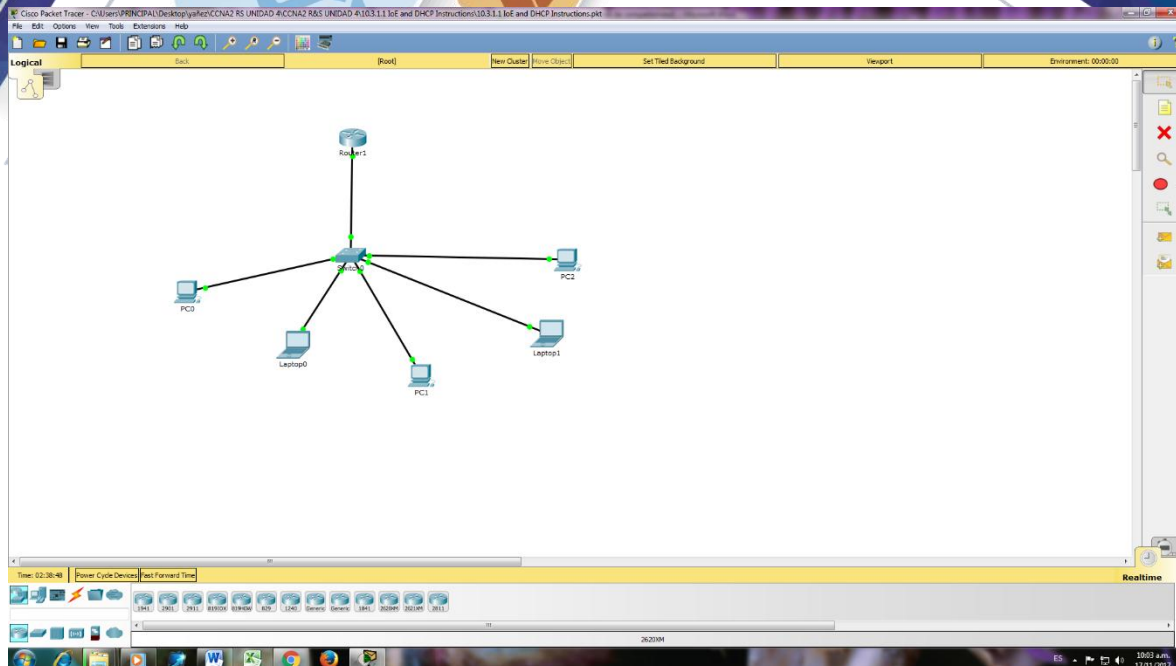
```

Router1
Physical Config CLI Attributes
IOS Command Line Interface

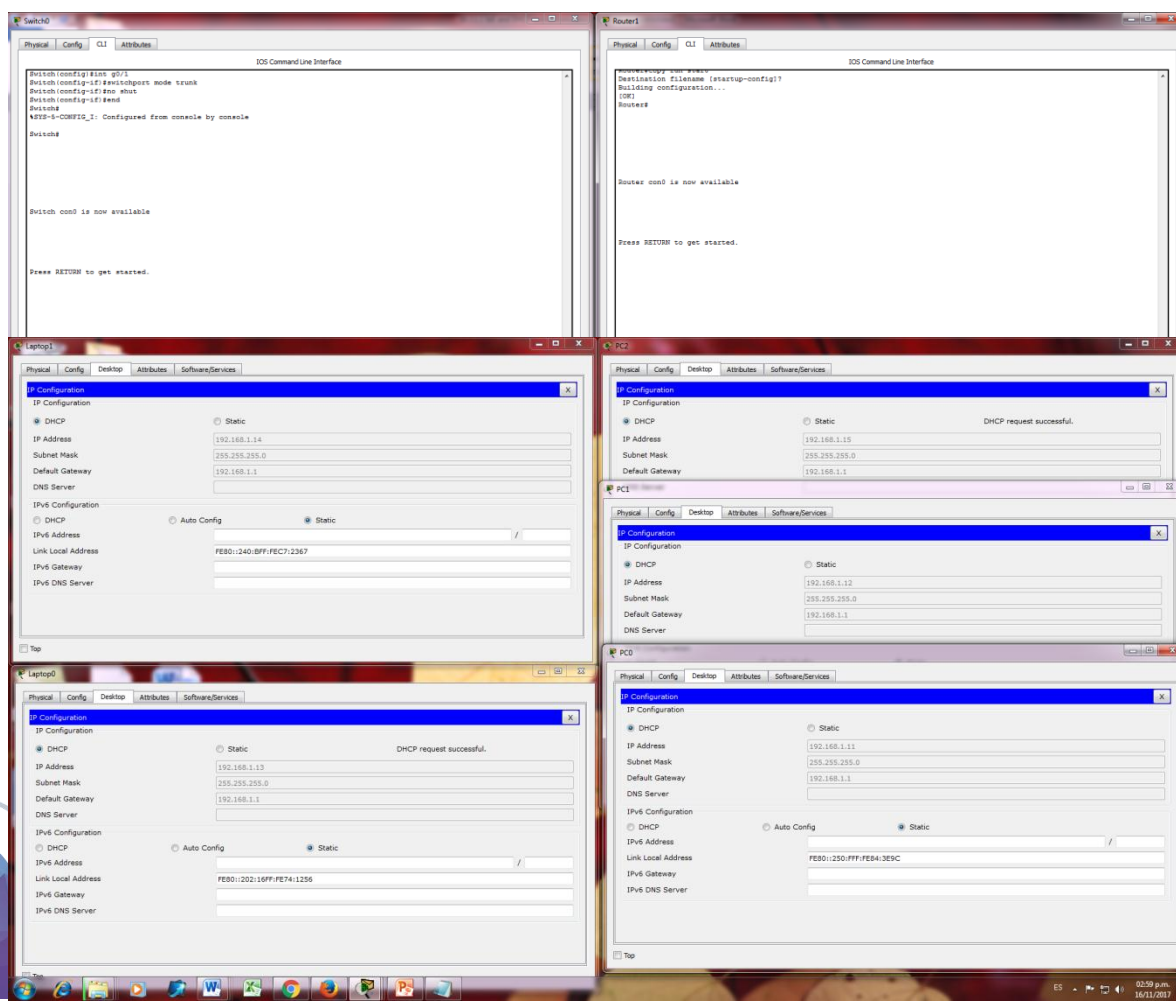
show running-config
Building configuration...

Current configuration : 786 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool MMDFR
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
!
ip cef
no ip vrf car
!
!
license udi plid CIS001941/E9 on YX1624507F
!
!
spanning-tree mode pvst
!
!
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
!
--More--
  
```

- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.



- Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.



Presente sus conclusiones a un compañero de clase o a la clase.

Recursos necesarios

Software de Packet Tracer

Reflexión

1. ¿Por qué un usuario desearía usar un router Cisco 1941 para configurar DHCP en su red doméstica? ¿No sería suficiente usar un ISR más pequeño como servidor de DHCP?

Los routers 1941 son más caros que los isr ofrecen más opciones para implementar planes de seguridad y son más sólidos en cuanto a capacidad de procesamiento y de ancho de banda. dhcp permite a los clientes de una red obtener una dirección ip y otra información del servidor dhcp. El protocolo automáticamente asigna direcciones ip, mascara de subred, puerta de enlace y otros parámetros ip. El cliente se conecta al servidor dhcp automáticamente para obtener una dirección ip dinámicamente cuando se conecta a la red. Para esto, el cliente envía un mensaje al servidor y este le contesta con los datos ip



solicitados. El servidor dhcp elige la dirección ip de un rango de direcciones configurado llamado pool.

La mayoría de las redes caseras o negocios pequeños usan un servicio integrado de ruteo (isr) que se conecta con el isp, en este caso el isr es ambos es un cliente y servidor dhcp, ya que el isr actúa como cliente para recibir la configuración del isp y funciona como servidor para los hosts locales de la red.

¿Cómo cree que las pequeñas y medianas empresas pueden usar la asignación de direcciones IP de DHCP en el mundo de las redes IPv6 e IdT? Mediante la técnica de la lluvia de ideas, piense y registre cinco respuestas posibles.

- Las pequeñas empresas podrían prender los sistemas de los clientes que se vayan de vacaciones según las asignaciones de direcciones IP del servidor de DHCP
- La empresa optimiza la configuración Mediante el uso de las asignaciones de direcciones IP de sus propios servidores de DHCP,
- Las pequeñas empresas de electricidad podrían revisar códigos de error en cualquier dispositivo con una dirección IP para evaluar si una terminal necesita reparación.
- Las pequeñas empresas automotrices podrían proporcionar cálculos de reparaciones según el direccionamiento IP de DHCP de los automóviles con direcciones automáticas vinculadas al servidor de DHCP de la empresa.
- El propietario de una casa podría encender la lavadora o la secadora desde cualquier lugar, según la ubicación de un servidor DNS y su propia dirección de servidor de DHCP. Se podrían controlar los televisores para apagarlos, encenderlos, seleccionar canales para grabar, grabar programas y más mediante un servidor DNS y un servidor de DHCP personal.

11.2.2.6. Práctica de laboratorio: configuración de NAT dinámica y estática



Topología

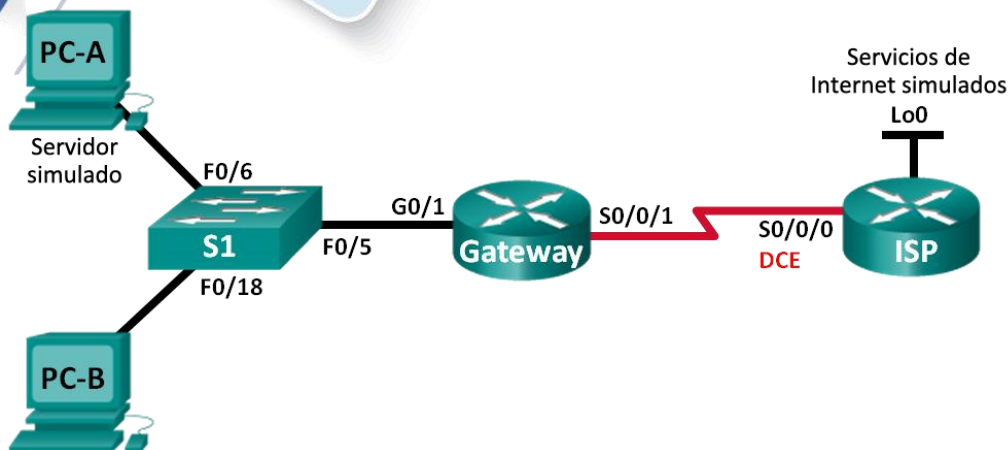


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	G0/0	192.31.7.1	255.255.255.0	N/A
Server ISP	NIC	192.31.7.2	255.255.255.0	192.31.7.1
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar la NAT estática

Parte 3: configurar y verificar la NAT dinámica

Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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



Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Part 20: armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

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

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

Step 2: configurar los equipos host.

Step 3: inicializar y volver a cargar los routers y los switches según sea necesario.

Step 4: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- c. Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.

- d. Configure el nombre del dispositivo como se muestra en la topología.
- e. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- f. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpen la entrada del comando.

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#username cisco pass
Gateway(config)#username cisco password cisco
Gateway(config)#line console 0
Gateway(config-line)#login local
Gateway(config-line)#logging syn
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit
Gateway(config)#no ip domain-lo
Gateway(config)#no ip domain-lookup
Gateway(config)#enable secret class
Gateway(config)#line vty 0 4
Gateway(config-line)#login local
Gateway(config-line)#logging synchronous
Gateway(config-line)#exit

```

Step 5: crear un servidor web simulado en el ISP.

- a. Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

- b. Habilite el servicio del servidor HTTP en el ISP.

```
ISP(config)# ip http server
```

- c. Configure el servicio HTTP para utilizar la base de datos local.

```
ISP(config)# ip http authentication local
```

(EL PROGRAMA NO PERMITE HACER ESTA CONFIGURACIÓN, EN SU REEMPLAZO COLOCAMOS UN SERVIDOR WEB “SERVER ISP”)

Step 6: configurar el routing estático.

- a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 7: Guardar la configuración en ejecución en la configuración de inicio.

Step 8: Verificar la conectividad de la red

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway.

Resuelva los problemas si los pings fallan.

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=54ms TTL=255
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=21ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 54ms, Average = 19ms
```

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=18ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 18ms, Average = 7ms
```

- b. Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

```
Gateway#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B
- BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

```
Gateway of last resort is 209.165.201.17 to network 0.0.0.0
```

```

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.16/30 is directly connected, Serial0/0/1
L    209.165.201.18/32 is directly connected, Serial0/0/1
S*  0.0.0.0/0 [1/0] via 209.165.201.17
```

```
ISP(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

192.31.7.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.31.7.0/24 is directly connected, GigabitEthernet0/0
L    192.31.7.1/32 is directly connected, GigabitEthernet0/0
209.165.200.0/27 is subnetted, 1 subnets
S    209.165.200.224/27 [1/0] via 209.165.201.18
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.16/30 is directly connected, Serial0/0/0
L    209.165.201.17/32 is directly connected, Serial0/0/0
```

Part 21: configurar y verificar la NAT estática.

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Step 1: configurar una asignación estática.

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios tengan acceso a la PC-A desde Internet. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20
209.165.200.225
```

Step 2: Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 3: probar la configuración.

- Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global   Inside local   Outside local   Outside global
--- 209.165.200.225  192.168.1.20   ---            ---
```

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local
-----
---  209.165.200.225    192.168.1.20      ---              ---
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = __209.165.200.225__

¿Quién asigna la dirección global interna?

__El router - el proveedor de internet__

¿Quién asigna la dirección local interna?

__Los administradores de red __

- b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=20ms TTL=254
Reply from 192.31.7.1: bytes=32 time=31ms TTL=254
Reply from 192.31.7.1: bytes=32 time=21ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 31ms, Average = 25ms

SERVER>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=38ms TTL=126
Reply from 192.31.7.2: bytes=32 time=16ms TTL=126
Reply from 192.31.7.2: bytes=32 time=39ms TTL=126
Reply from 192.31.7.2: bytes=32 time=36ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 39ms, Average = 32ms
```

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

```
icmp 209.165.200.225:1 192.168.1.20:1    192.31.7.1:1    192.31.7.1:1
--- 209.165.200.225    192.168.1.20    ---    ---
```

```
Gateway#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside
global
icmp 209.165.200.225:37192.168.1.20:37    192.31.7.2:37    192.31.7.2:37
icmp 209.165.200.225:38192.168.1.20:38    192.31.7.2:38    192.31.7.2:38
icmp 209.165.200.225:39192.168.1.20:39    192.31.7.2:39    192.31.7.2:39
icmp 209.165.200.225:40192.168.1.20:40    192.31.7.2:40    192.31.7.2:40
icmp 209.165.200.225:41192.168.1.20:41    192.31.7.1:41    192.31.7.1:41
icmp 209.165.200.225:42192.168.1.20:42    192.31.7.1:42    192.31.7.1:42
icmp 209.165.200.225:43192.168.1.20:43    192.31.7.1:43    192.31.7.1:43
icmp 209.165.200.225:44192.168.1.20:44    192.31.7.1:44    192.31.7.1:44
icmp 209.165.200.225:45192.168.1.20:45    192.31.7.2:45    192.31.7.2:45
icmp 209.165.200.225:46192.168.1.20:46    192.31.7.2:46    192.31.7.2:46
icmp 209.165.200.225:47192.168.1.20:47    192.31.7.2:47    192.31.7.2:47
icmp 209.165.200.225:48192.168.1.20:48    192.31.7.2:48    192.31.7.2:48
--- 209.165.200.225    192.168.1.20    ---    ---
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? __41__

Nota: puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

- c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.225:1 192.168.1.20:1    192.31.7.1:1    192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23
192.31.7.1:23
--- 209.165.200.225    192.168.1.20    ---    ---
```

```
Gateway#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside
global
--- 209.165.200.225    192.168.1.20    ---    ---
tcp 209.165.200.225:1025192.168.1.20:1025 192.31.7.2:80
192.31.7.2:80
```

Nota: es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? __Web__

¿Cuáles son los números de puerto que se usaron?

Global/local interno: __1025__

Global/local externo: __80__

- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```

Packet Tracer SERVER Command Line 1.0
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=3ms TTL=126
Reply from 209.165.200.225: bytes=32 time=16ms TTL=126
Reply from 209.165.200.225: bytes=32 time=13ms TTL=126
Reply from 209.165.200.225: bytes=32 time=12ms TTL=126

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 16ms, Average = 11ms
    
```

PC-A

Services
Desktop
Software/Services

HTTP

HTTP

On Off

HTTPS

On Off

File Name:

```

<html>
<h1>PCA</h1>
<center><font size='+2' color='blue'>Cisco Packet
Tracer</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new
opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
    
```



- e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# **show ip nat translations**

```
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.165.200.225:12 192.168.1.20:12  209.165.201.17:12
209.165.201.17:12
--- 209.165.200.225    192.168.1.20    ---            ---
```

```
Gateway#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
---  209.165.200.225    192.168.1.20    ---            ---
tcp  209.165.200.225:1025 192.168.1.20:1025  192.31.7.2:80    192.31.7.2:80
tcp  209.165.200.225:80  192.168.1.20:80  192.31.7.2:1025  192.31.7.2:1025
tcp  209.165.200.225:80  192.168.1.20:80  192.31.7.2:1026  192.31.7.2:1026
```

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la dirección global interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

- f. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ip nat statistics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 4 (1 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Part 22: configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Step 1: borrar las NAT.

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation *
```

```
Gateway# clear ip nat statistics
```

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
---  209.165.200.225     192.168.1.20     ---              ---
```

Step 2: definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 3: verificar que la configuración de interfaces NAT siga siendo válida.

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

```
Gateway#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 56 Misses: 51
Expired translations: 48
Dynamic mappings:
```

Step 4: definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

Step 5: definir la NAT desde la lista de origen interna hasta el conjunto externo.

Nota: recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas, y el nombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

Gateway(config)# ip nat inside source list 1 pool public_access

Step 6: probar la configuración.

- a. En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
PC>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=21ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=32ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 32ms, Average = 24ms
```

Gateway# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

```
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.242:33 192.168.1.21:33  192.31.7.1:33    192.31.7.1:33
icmp 209.165.200.242:34 192.168.1.21:34  192.31.7.1:34    192.31.7.1:34
icmp 209.165.200.242:35 192.168.1.21:35  192.31.7.1:35    192.31.7.1:35
icmp 209.165.200.242:36 192.168.1.21:36  192.31.7.1:36    192.31.7.1:36
---

```

¿Cuál es la traducción de la dirección host local interna de la PC-B?

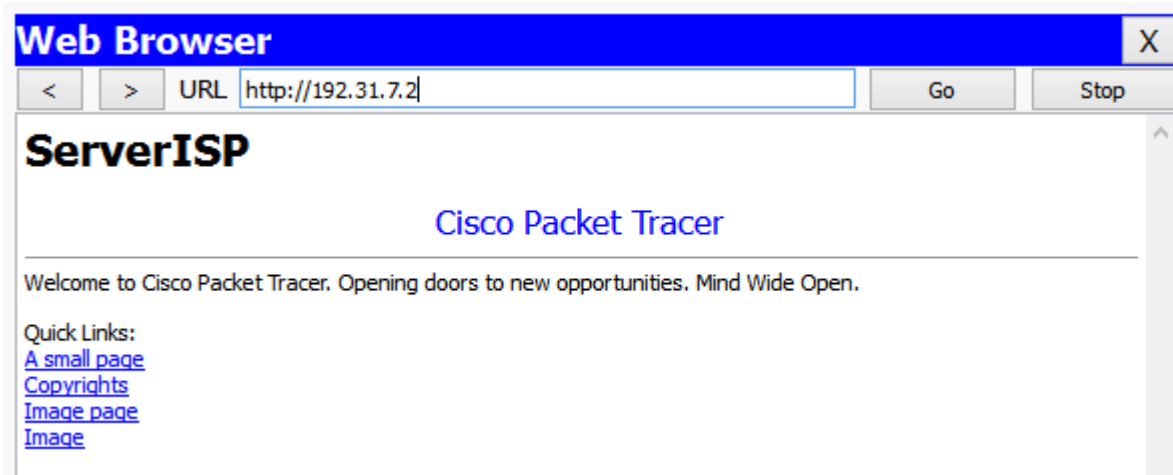
192.168.1.21 = 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? 33

- b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass**.

Para nuestro caso ingresamos por el web browser:



- c. Muestre la tabla de NAT.

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80

tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80
192.31.7.1:80

tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80
192.31.7.1:80

--- 209.165.200.242 192.168.1.22 --- ---

Gateway#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1025	192.168.1.21:1025	192.31.7.2:80	192.31.7.2:80

¿Qué protocolo se usó en esta traducción? _Http_

¿Qué números de puerto se usaron?

Interno: _1025_

Externo: _80_

¿Qué número de puerto bien conocido y qué servicio se usaron? _el http usó el 80_

- d. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

Gateway# **show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 2

pool public_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0

Appl doors: 0
Normal doors: 0
Queued Packets: 0

```
Gateway#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Step 7: eliminar la entrada de NAT estática.

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

- Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225
```

Static entry in use, do you want to delete child entries? [no]: **yes**

- Borre las NAT y las estadísticas.
- Haga ping al ISP (192.31.7.1) desde ambos hosts.
- Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
```

```
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
```

```
Peak translations: 15, occurred 00:00:43 ago
```

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 16 Misses: 0

CEF Translated packets: 285, CEF Punted packets: 0

Expired translations: 11

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 4

pool public_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

Gateway# **show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	
	192.31.7.1:512			
---	209.165.200.243	192.168.1.20	---	---
icmp	209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	
	192.31.7.1:512			
---	209.165.200.242	192.168.1.21	---	---

```

Gateway#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 71 Misses: 84
Expired translations: 56
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 1
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 1 (7%), misses 0
Gateway#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
tcp  209.165.200.242:1025  192.168.1.21:1025  192.31.7.2:80    192.31.7.2:80

```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

Debido a que las ipv4 se estaban acabando se implementó utilizar para un grupo de red privadas el uso de una sola red pública, de esta manera se realiza un ahorro de Ip porque varias pc pueden ingresar a internet con la misma Ip pública (Aumenta la flexibilidad de las conexiones con la red pública). Adicional a esto aumenta el nivel de seguridad, un usuario no aparece en internet con su Ip privada, sino con la Ip pública asignada.

2. ¿Cuáles son las limitaciones de NAT?

Entre su desventajas esta que algunas aplicaciones que utilizan el direccionamiento IP dejan de funcionar, porque esconde las direcciones IP de extremo a extremo, no todas las aplicaciones y protocolos son compatibles con NAT; también aumenta el retardo y necesita mayor potencia de computación.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

11.2.3.7 Lab - Configuring NAT Pool Overload and PAT

Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

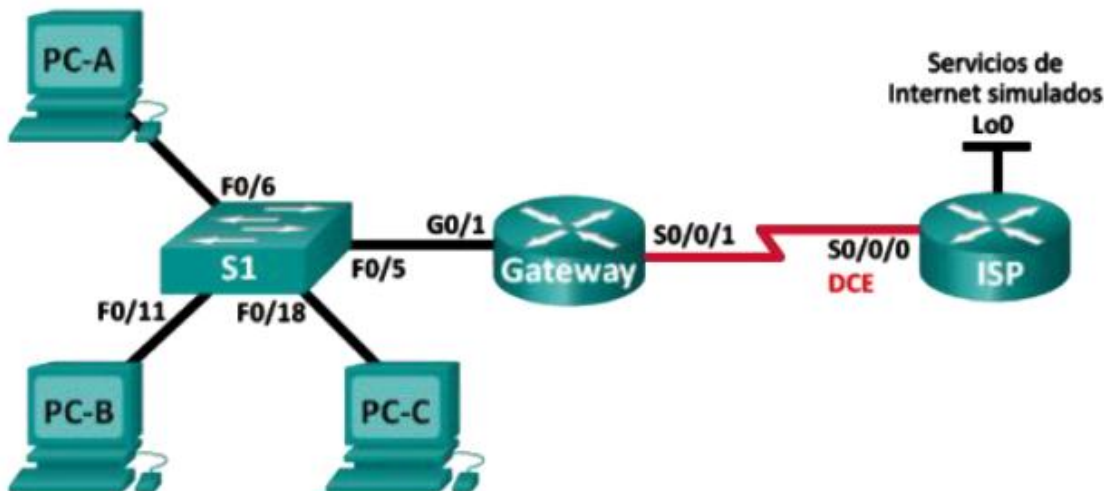


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objetivos

Parte 1: armar la red y verificar la conectividad

Parte 2: configurar y verificar un conjunto de NAT con sobrecarga

Parte 3: configurar y verificar PAT

Información básica/situación

En la primera parte de la práctica de laboratorio, el ISP asigna a su empresa el rango de direcciones IP públicas 209.165.200.224/29. Esto proporciona seis direcciones IP públicas a la empresa. Un conjunto de NAT dinámica con sobrecarga consta de un conjunto de direcciones IP en una relación de varias direcciones a varias direcciones. El router usa la primera dirección IP del conjunto y asigna las conexiones mediante el uso de la dirección IP más un número de puerto

único. Una vez que se alcanzó la cantidad máxima de traducciones para una única dirección IP en el router (específico de la plataforma y el hardware), utiliza la siguiente dirección IP del conjunto. En la parte 2, el ISP asignó una única dirección IP, 209.165.201.18, a su empresa para usarla en la conexión a Internet del router Gateway de la empresa al ISP. Usará la traducción de la dirección del puerto (PAT) para convertir varias direcciones internas en la única dirección pública utilizable. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

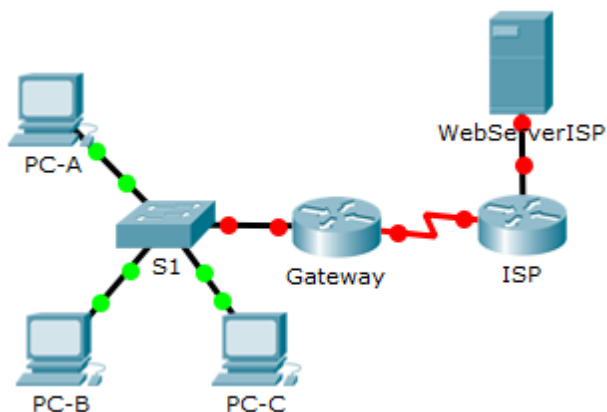
Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

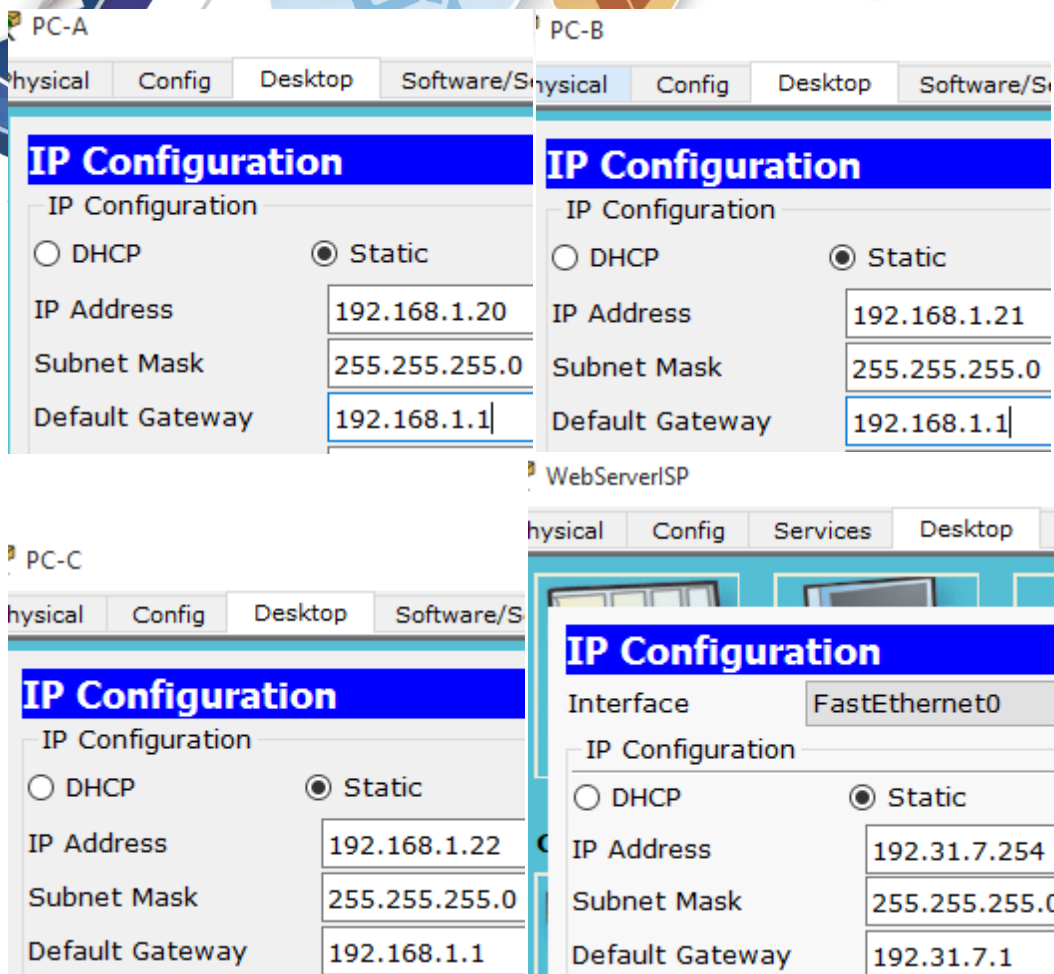
Parte 1: armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Paso 8. realizar el cableado de red tal como se muestra en la topología.



Paso 9. Configurar los equipos host.



Paso 10. inicializar y volver a cargar los routers y los switches.

Paso 11. configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

Gateway

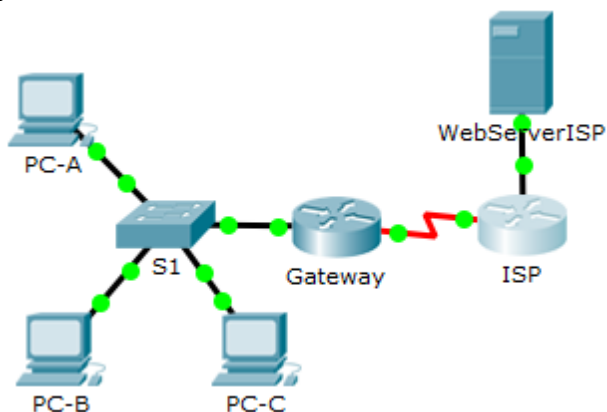
```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#int g0/1
Gateway(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway(config-if)#no shut
Gateway(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
Gateway(config-if)#int s0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#no shut
Gateway(config-if)#shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to administratively
down
Gateway(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down ISP
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
ISP(config-if)#int g0/0
ISP(config-if)#ip address 192.31.7.1 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
ISP(config-if)#exit
```

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
ISP(config-if)#int g0/0
ISP(config-if)#ip address 192.31.7.1 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
ISP(config-if)#

```



Paso 12. configurar el routing estático.

a. Cree una ruta estática desde el router ISP hasta el router Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

b. Cree una ruta predeterminada del router Gateway al router ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Paso 13. Verificar la conectividad de la red

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

PC-A

```
PC>ping 192.168.1.1
```

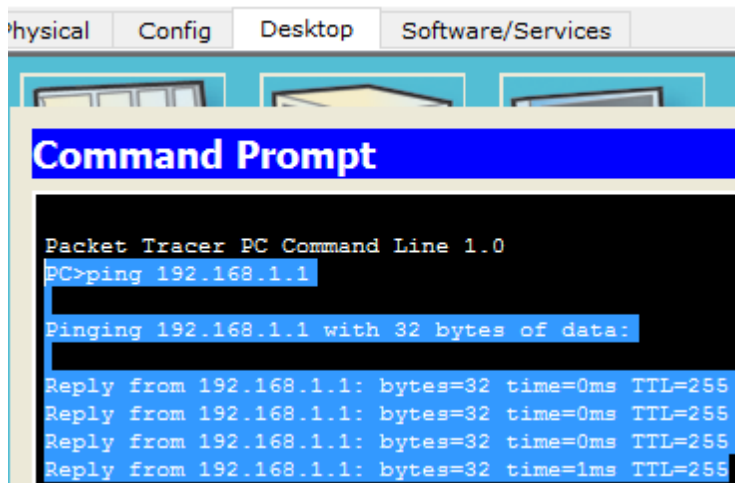
```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255  
PC-B  
PC-C
```

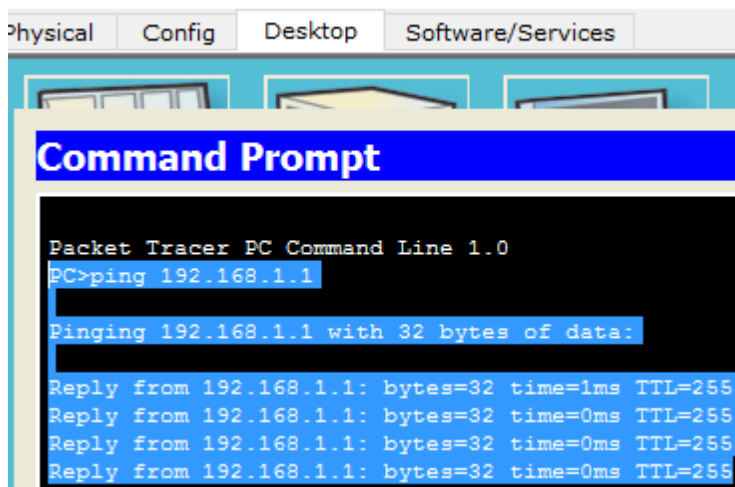
b. Verifique

PC-A

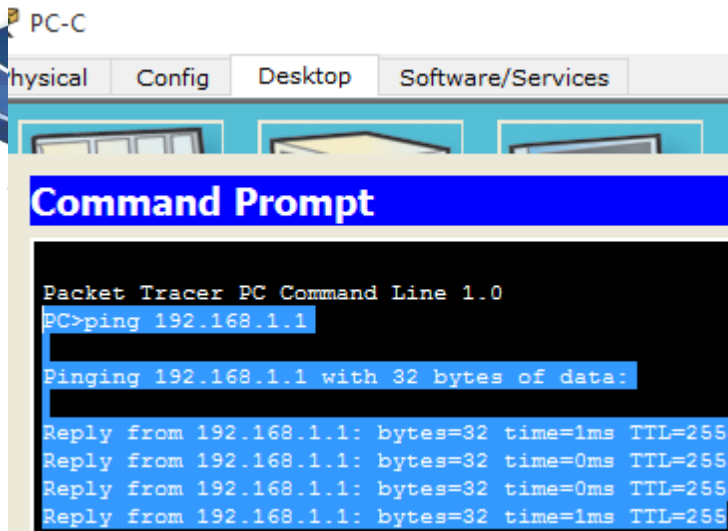


```
Physical Config Desktop Software/Services  
Command Prompt  
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.1  
Pinging 192.168.1.1 with 32 bytes of data:  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

PC-B



```
Physical Config Desktop Software/Services  
Command Prompt  
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.1  
Pinging 192.168.1.1 with 32 bytes of data:  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
```



The image shows a screenshot of a Packet Tracer PC Command Line interface. The window title is "PC-C" and it has tabs for "Physical", "Config", "Desktop", and "Software/Services". The "Desktop" tab is active, showing a "Command Prompt" window. The command prompt displays the following text:

```
Packet Tracer PC Command Line 1.0  
PC>ping 192.168.1.1  
Pinging 192.168.1.1 with 32 bytes of data:  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Parte2: configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

Paso 14. definir una lista de control de acceso que coincida con las direcciones IP privadas de LAN.

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Paso 15. definir el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
```

Paso 16. definir la NAT desde la lista de origen interna hasta el conjunto externo.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Paso 17. Especifique las interfaces.

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Paso 18. verificar la configuración del conjunto de NAT con sobrecarga.

a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.

PC-A

```
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-B

```
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-C

```
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
```

```

Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses 0
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

```

c. Muestre las NAT en el router Gateway.

```

Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1 192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1 192.31.7.1:2

```

```

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1024 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1024
icmp 209.165.200.225:1025 192.168.1.21:2 192.31.7.1:2 192.31.7.1:1025
icmp 209.165.200.225:1026 192.168.1.21:3 192.31.7.1:3 192.31.7.1:1026
icmp 209.165.200.225:1027 192.168.1.21:4 192.31.7.1:4 192.31.7.1:1027
icmp 209.165.200.225:1028 192.168.1.22:1 192.31.7.1:1 192.31.7.1:1028
icmp 209.165.200.225:1029 192.168.1.22:2 192.31.7.1:2 192.31.7.1:1029
icmp 209.165.200.225:1030 192.168.1.22:3 192.31.7.1:3 192.31.7.1:1030
icmp 209.165.200.225:1031 192.168.1.22:4 192.31.7.1:4 192.31.7.1:1031
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.20:2 192.31.7.1:2 192.31.7.1:2
icmp 209.165.200.225:3 192.168.1.20:3 192.31.7.1:3 192.31.7.1:3
icmp 209.165.200.225:4 192.168.1.20:4 192.31.7.1:4 192.31.7.1:4

```

Nota: es posible que no vea las tres traducciones, según el tiempo que haya transcurrido desde que hizo los pings en cada computadora. Las traducciones de ICMP tienen un valor de tiempo de espera corto.

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior?

3 _____

¿Cuántas direcciones IP globales internas se indican? 1 _____

¿Cuántos números de puerto se usan en conjunto con las direcciones globales internas?

12 _____

¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

El ping no funciona porque el router solo conoce la ubicación de las direcciones internas globales en su tabla de enrutamiento, pero las direcciones internas locales no están notificadas. _____

Parte 3: configurar y verificar PAT

En la parte 3, configurará PAT mediante el uso de una interfaz, en lugar de un conjunto de direcciones, a fin de definir la dirección externa. No todos los comandos de la parte 2 se volverán a usar en la parte 3.

Paso 19. borrar las NAT y las estadísticas en el router Gateway.

```
Gateway#clear ip nat translation *
Gateway#clear ip nat statistics
^
% Invalid input detected at '^' marker
PACKET TRACERT NO SOPORTA EL ULTIMO COMANDO
```

Paso 20. verificar la configuración para NAT.

- Verifique que se hayan borrado las estadísticas.
 - Verifique que las interfaces externa e interna estén configuradas para NAT.
 - Verifique que la ACL aún esté configurada para NAT.
- ¿Qué comando usó para confirmar los resultados de los pasos a al c?

```
show ip nat statistics
-----
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 12 Misses: 12
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6 , allocated 0 (0%), misses 0
```

Paso 21. eliminar el conjunto de direcciones IP públicas utilizables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask
255.255.255.248
%Pool public_access in use, cannot destroy
Gateway(config)#
```

Paso 22. eliminar la traducción NAT de la lista de origen interna al conjunto externo.

```
Gateway(config)# no ip nat inside source list 1 pool public_access
overload
Gateway(config)#no ip nat inside source list 1 pool public_access overload
Gateway(config)#
```

Paso 23. asociar la lista de origen a la interfaz externa.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1
overload
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
Gateway(config)#
```

Paso 24. probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

PC-A

```
PC>ping 192.31.7.1
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=13ms TTL=254
```

PC-B

```
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=15ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

PC-C

```
Pinging 192.31.7.1 with 32 bytes of data:
Reply from 192.31.7.1: bytes=32 time=13ms TTL=25
Reply from 192.31.7.1: bytes=32 time=2ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
```

b. Muestre las estadísticas de NAT en el router Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
```

```

Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

```

```

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Gateway#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 24 Misses: 24
Expired translations: 24
Dynamic mappings:

```

```

Gateway#show ip nat translations
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 36 Misses: 36
Expired translations: 24
Dynamic mappings:

```

c. Muestre las traducciones NAT en el Gateway.

```

Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.201.18:3 192.168.1.20:1 192.31.7.1:1 192.31.7.1:3
icmp 209.165.201.18:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.201.18:4 192.168.1.22:1 192.31.7.1:1 192.31.7.1:4

```

```

Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.201.18:1024 192.168.1.21:9 192.31.7.1:9 192.31.7.1:1024
icmp 209.165.201.18:1025 192.168.1.21:10 192.31.7.1:10 192.31.7.1:1025
icmp 209.165.201.18:1026 192.168.1.21:11 192.31.7.1:11 192.31.7.1:1026
icmp 209.165.201.18:1027 192.168.1.21:12 192.31.7.1:12 192.31.7.1:1027

```

```
icmp 209.165.201.18:1028192.168.1.22:9 192.31.7.1:9 192.31.7.1:1028
icmp 209.165.201.18:1029192.168.1.22:10 192.31.7.1:10 192.31.7.1:1029
icmp 209.165.201.18:1030192.168.1.22:11 192.31.7.1:11 192.31.7.1:1030
icmp 209.165.201.18:1031192.168.1.22:12 192.31.7.1:12 192.31.7.1:1031
icmp 209.165.201.18:10 192.168.1.20:10 192.31.7.1:10 192.31.7.1:10
icmp 209.165.201.18:11 192.168.1.20:11 192.31.7.1:11 192.31.7.1:11
icmp 209.165.201.18:12 192.168.1.20:12 192.31.7.1:12 192.31.7.1:12
icmp 209.165.201.18:9 192.168.1.20:9 192.31.7.1:9 192.31.7.1:9
```

```
Gateway#show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.201.18:1024192.168.1.21:9 192.31.7.1:9 192.31.7.1:1024
icmp 209.165.201.18:1025192.168.1.21:10 192.31.7.1:10 192.31.7.1:1025
icmp 209.165.201.18:1026192.168.1.21:11 192.31.7.1:11 192.31.7.1:1026
icmp 209.165.201.18:1027192.168.1.21:12 192.31.7.1:12 192.31.7.1:1027
icmp 209.165.201.18:1028192.168.1.22:9 192.31.7.1:9 192.31.7.1:1028
icmp 209.165.201.18:1029192.168.1.22:10 192.31.7.1:10 192.31.7.1:1029
icmp 209.165.201.18:1030192.168.1.22:11 192.31.7.1:11 192.31.7.1:1030
icmp 209.165.201.18:1031192.168.1.22:12 192.31.7.1:12 192.31.7.1:1031
icmp 209.165.201.18:10 192.168.1.20:10 192.31.7.1:10 192.31.7.1:10
icmp 209.165.201.18:11 192.168.1.20:11 192.31.7.1:11 192.31.7.1:11
icmp 209.165.201.18:12 192.168.1.20:12 192.31.7.1:12 192.31.7.1:12
icmp 209.165.201.18:9 192.168.1.20:9 192.31.7.1:9 192.31.7.1:9
```

Reflexión

¿Qué ventajas tiene la PAT?

El PAT minimiza el uso del número de direcciones públicas necesarias para acceder a internet, PAT al igual que NAT, sirve para esconder las direcciones privadas de la red externa.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

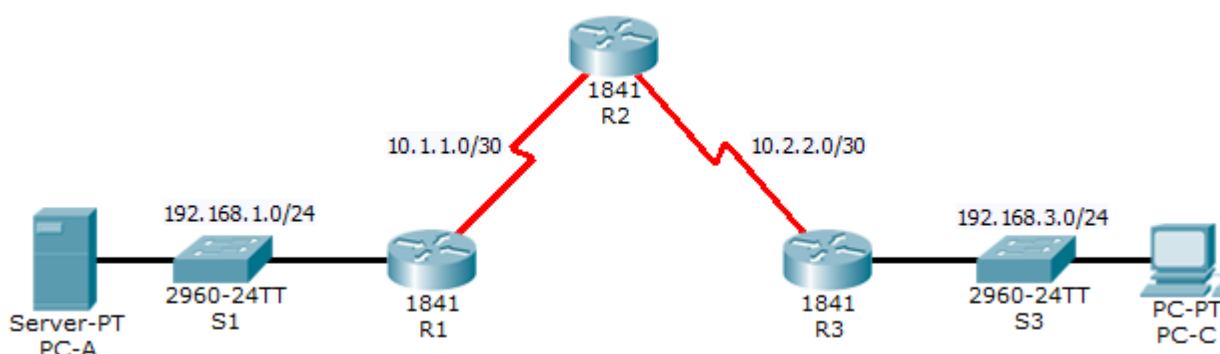
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks

Packet Tracer - Configure IP ACLs to Mitigate Attacks (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topología



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality.

Background / Scenario

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

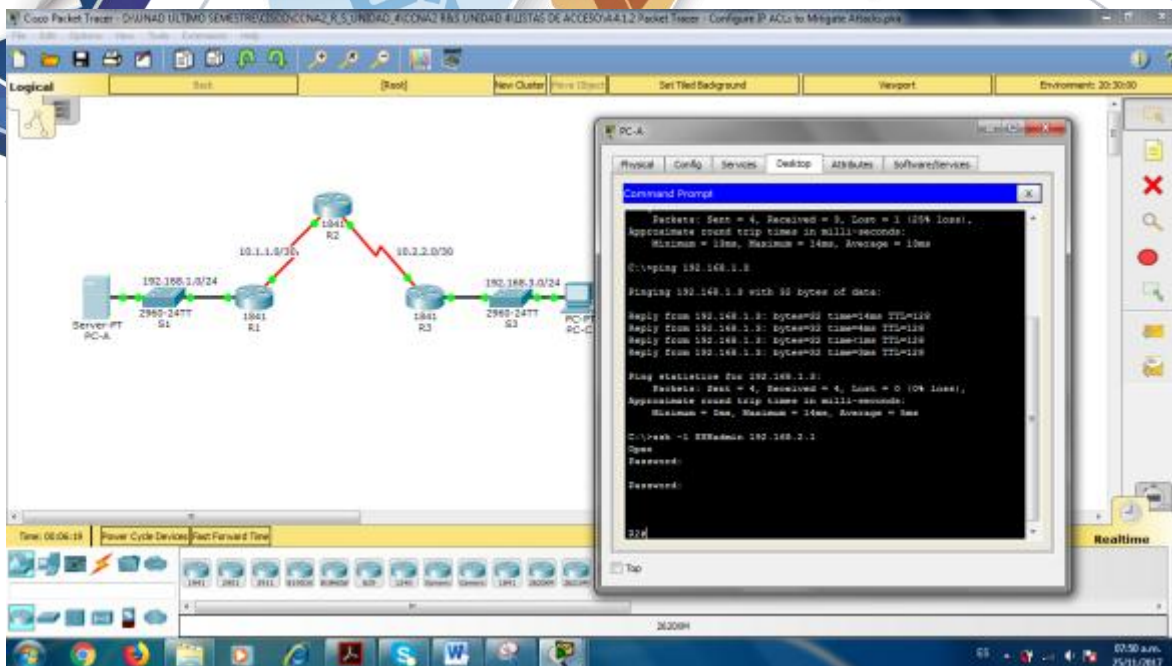
Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

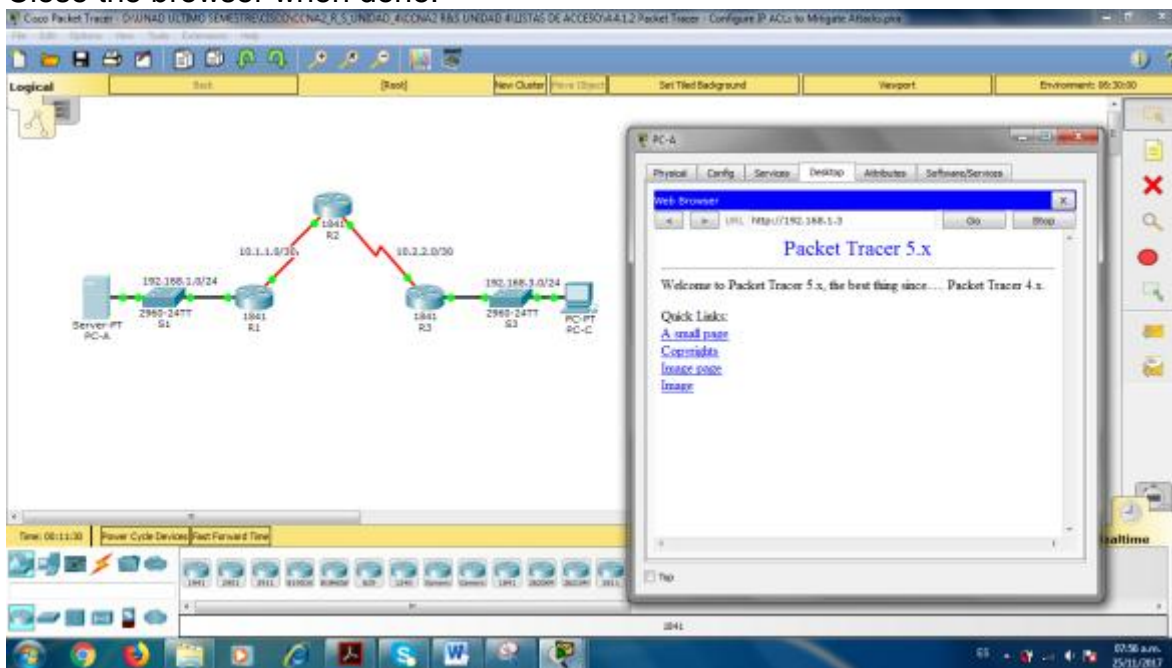
- o Enable password: **ciscoenpa55**
- o Password for console: **ciscoconpa55**
- o Username for VTY lines: **SSHadmin**
- o Password for VTY lines: **ciscosshpa55**
- o IP addressing
- o Static routing

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.



c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser when done.

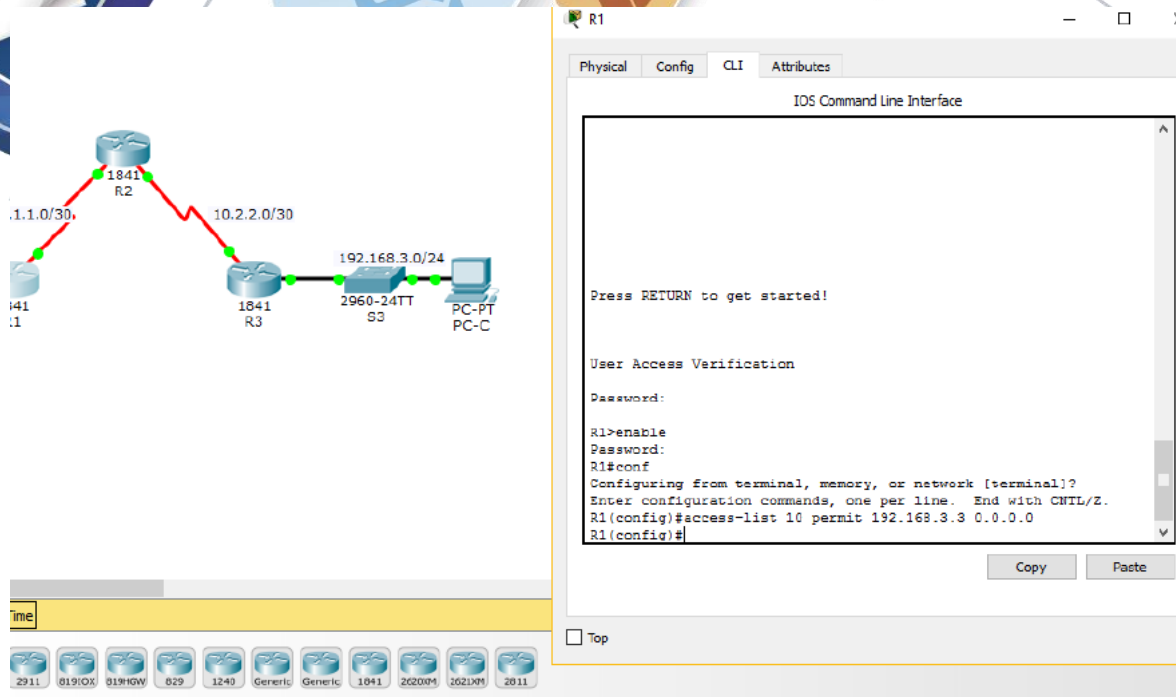


Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

Use the **access-list** command to create a numbered IP ACL on R1, R2, and R3.

R1(config)# **access-list 10 permit 192.168.3.3 0.0.0.0**



The network diagram shows three routers: R1 (1841) on the left, R2 (1841) in the center, and R3 (1841) on the right. R1 and R2 are connected via a link with IP addresses 1.1.0/30 and 10.2.2.0/30. R2 and R3 are connected via a link with IP addresses 10.2.2.0/30 and 192.168.3.0/24. R3 is connected to a switch (S3, 2960-24TT) and two PCs (PC-PT and PC-C).

The R1 CLI window shows the following output:

```

R1
-----
Physical  Config  CLI  Attributes
IOS Command Line Interface

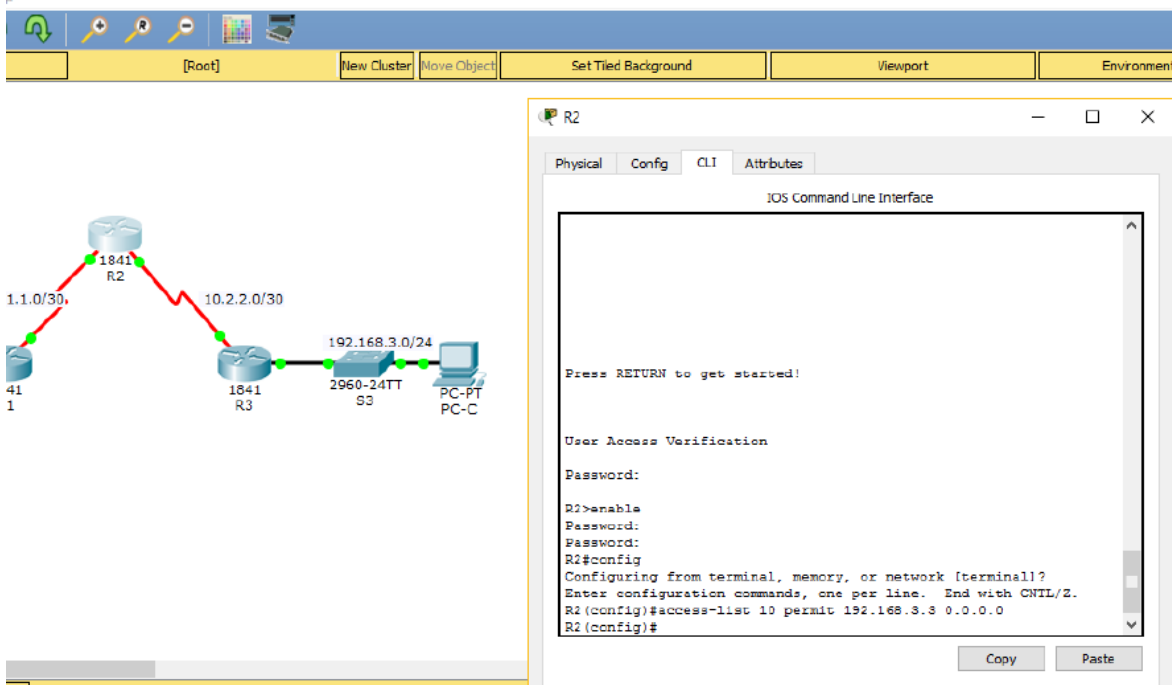
Press RETURN to get started!

User Access Verification

Password:

R1>enable
Password:
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#
    
```

R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0



The network diagram is identical to the previous one, showing the topology of routers R1, R2, R3, switch S3, and PCs.

The R2 CLI window shows the following output:

```

R2
-----
Physical  Config  CLI  Attributes
IOS Command Line Interface

Press RETURN to get started!

User Access Verification

Password:

R2>enable
Password:
R2#ccnfig
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(ccnfig)#
    
```

R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0

The network diagram shows three routers: R1 (1841) with IP 10.1.1.0/30, R2 (1841) with IP 10.1.1.0/30, and R3 (1841) with IP 10.2.2.0/30. R2 is connected to R1 and R3. R3 is connected to a switch S3 (2960-24TT) with IP 192.168.3.0/24, which is connected to two PCs (PC-PT and PC-C).

```

R3
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

User Access Verification

Password:
Password:

R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#
    
```

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

R1(config-line)# access-class 10 in

The network diagram shows three routers: R1 (1841) with IP 10.1.1.0/30, R2 (1841) with IP 10.1.1.0/30, and R3 (1841) with IP 10.2.2.0/30. R2 is connected to R1 and R3. R3 is connected to a switch S3 (2960-24TT) with IP 192.168.3.0/24, which is connected to two PCs (PC-PT and PC-C).

```

R1
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

User Access Verification

Password:

R1>enable
Password:
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty 5 10
R1(config-line)#access-class 10 in
R1(config-line)#
    
```

R2(config-line)# access-class 10 in

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started!

User Access Verification
Password:
R2>enable
Password:
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.2.2 0.0.0.0
R2(config)#access-list 10 permit 192.168.2.2 0.0.0.0
R2(config)#exit
R2#
*SYS-6-CONFIG_I: Configured from console by console
R2#conf line
^
% Invalid input detected at '^' marker.
R2#
R2#config-line
Translating "config-line"...domain server (0.0.0.0)
% Unknown command or computer name, or unable to find computer address
R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 5 10
R2(config-line)#access-class 10 in
R2(config-line)#
Copy Paste

```

R3(config-line)# access-class 10 in

```

R3
Physical Config CLI Attributes
IOS Command Line Interface

Cisco I841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTK094711E
M80 processor: part number 3, mask 40
1 FastEthernet/IEEE 802.3 interface(s)
2 low-speed serial (async) console interfaces(s)
192K bytes of NVRAM.
60480K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, I841 Software (I841-ANVIPSERVLCISK3-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc)
Technical support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 10-Jul-07 04:52 by pt_team

Press RETURN to get started!

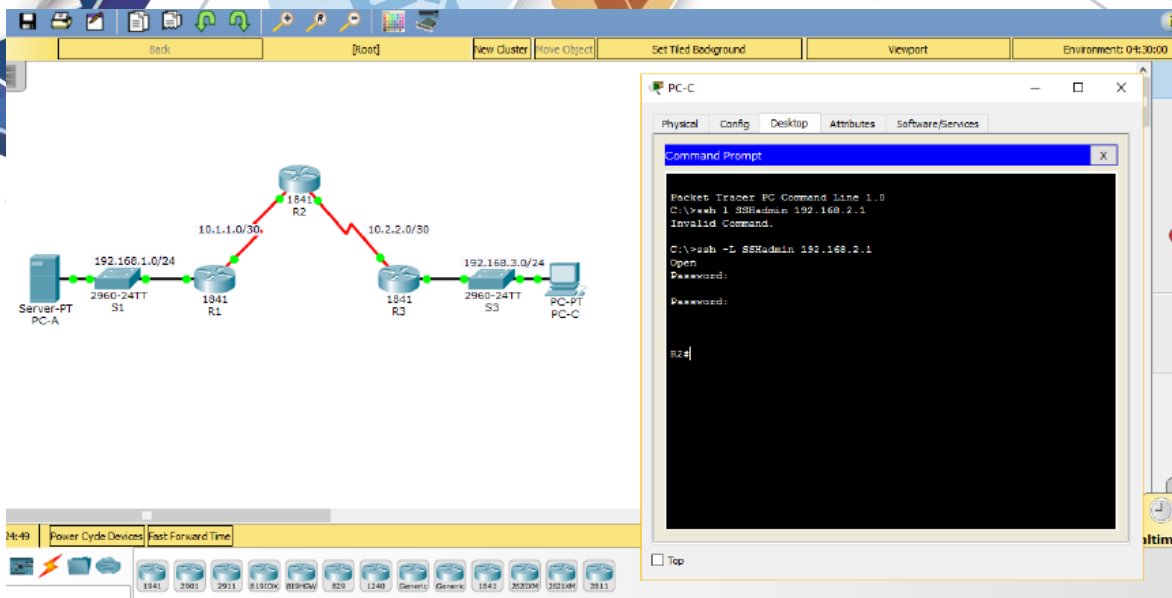
%LINK-3-CHANGED: Interface Serial0/0/1, changed state to up
%LINKPROTO-1-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINKPROTO-3-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification
Password:
R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.2.2 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#
Copy Paste

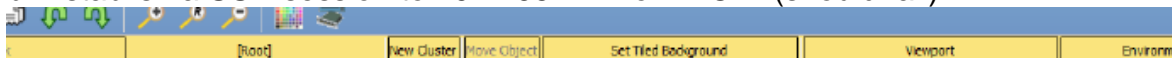
```

Step 3: Verify exclusive access from management station PC-C.

- a. Establish a SSH session to 192.168.2.1 from PC-C (should be successful).
PC> ssh -l SSHAdmin 192.168.2.1



b. Establish a SSH session to 192.168.2.1 from **PC-A** (should fail).

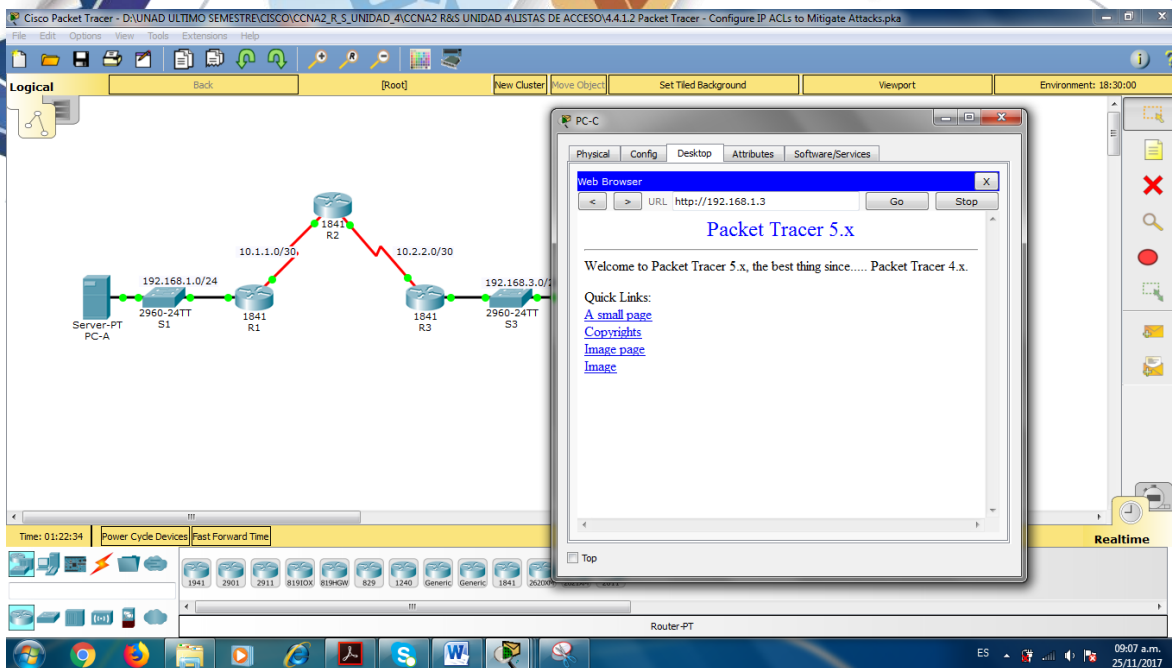


Part 3: Create a Numbered IP ACL 120 on R1

Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A**, deny any outside host access to HTTPS services on **PC-A**, and permit **PC-C** to access **R1** via SSH.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.



Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

```
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain
```

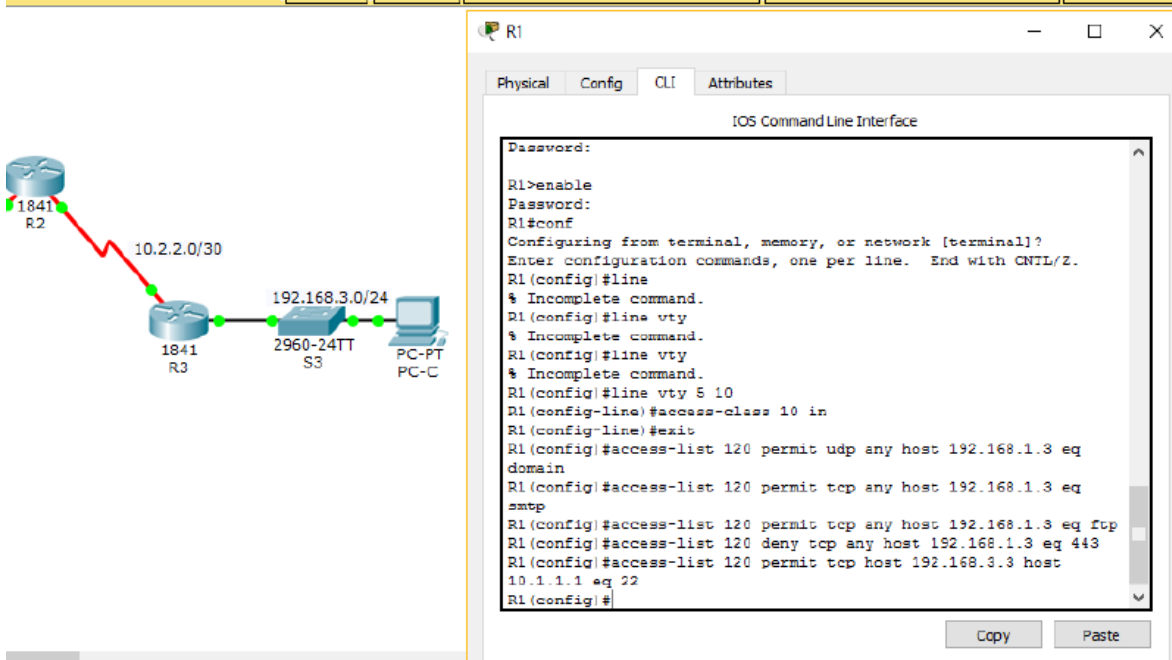
```
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp
```

```
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp
```

```
R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443
```

```
R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
```

[Root] [New Cluster] [Move Object] [Set Tied Background] [Viewport] [Environment]



Step 3: Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip access-group 120 in**

```

R1
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

Press RETURN to get started!

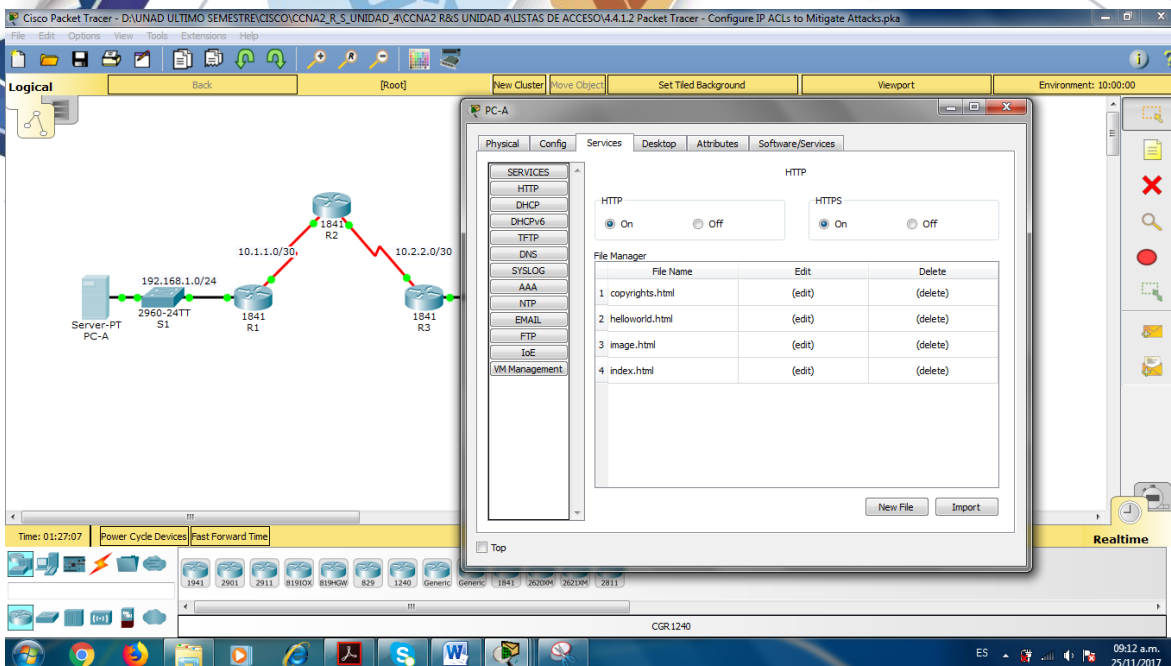
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

User Access Verification

Password:

R1>enable
Password:
R1#conf
Configuring from terminal, memory, or network (terminal)?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty 5 10
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 403
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-g
R1(config-if)#ip access-group 120 in
R1(config-if)#
  
```

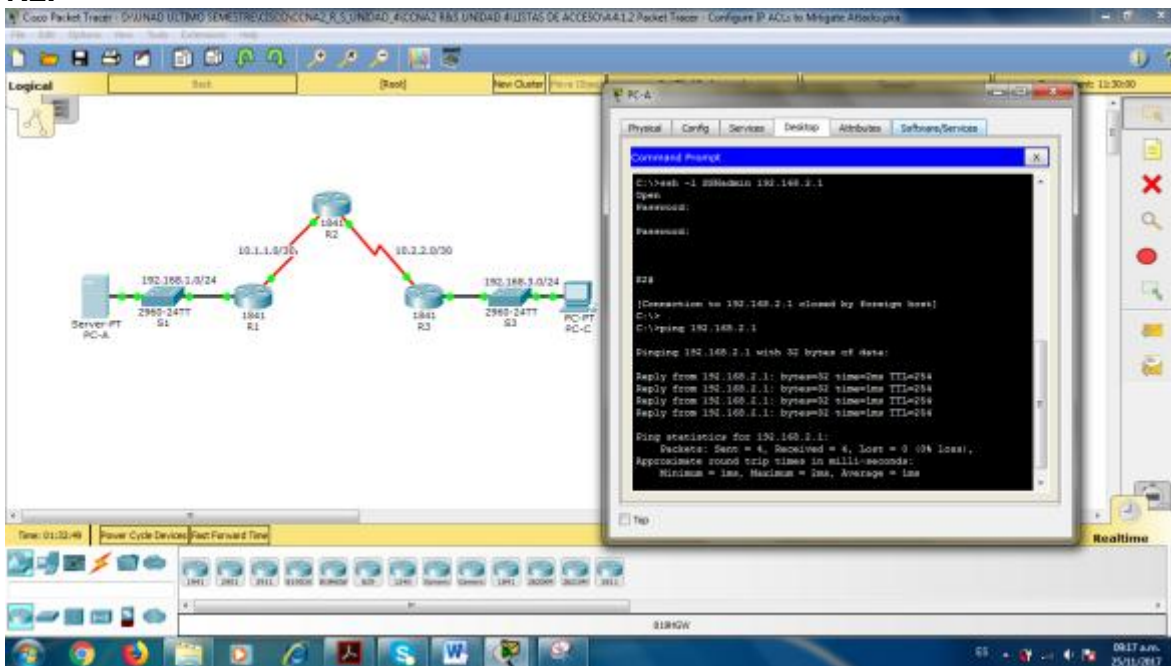
Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify An Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.



Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

R1(config)# **access-list 120 permit icmp any any echo-reply**

```
R1(config)# access-list 120 permit icmp any any unreachable
R1(config)# access-list 120 deny icmp any any
R1(config)# access-list 120 permit ip any any
```

Environment: 19:00

R1

IOS Command Line Interface

```
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty
% Incomplete command.
R1(config)#line vty 5 10
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq
domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq
smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host
10.1.1.1 eq 22
R1(config)#interface s0/0/0
R1(config-if)#ip access-g
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

Copy Paste

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

Cisco Packet Tracer - D:\UNAD ULTIMO SEMESTRE\GISCO\CCNA2_R3\UNIDAD 4\LISTAS DE ACCESO\4.4.1.2 Packet Tracer - Configure IP ACLs to Mitigate Attacks.pka

Logical [Root] New Cluster Move Object

PC-A

Command Prompt

```
C:\>ssh -l SSHAdmin 192.168.2.1
Open
Password:
Password:

R2#
[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Realtime

09:23 a.m. 25/11/2017

Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on R3.

R3

```

Physical  Config  CLI  Attributes
IOS Command Line Interface

63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(16)T1, RELEASE SOFTWARE (&c2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to up

User Access Verification

Password:
Password:

R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#

```

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

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

```

R3
Physical Config CLI Attributes
IOS Command Line Interface

$B488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(16)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification

Password:
Password:

R3>enable
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#

```

Step 2: Apply the ACL to interface F0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1.

R3(config)# **interface fa0/1**

R3(config-if)# **ip access-group 110 in**

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User Access Verification

Password:
Password:

R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network (terminal)?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.8.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#

```

Part 6: Create a Numbered IP ACL 100 on R3

On R3, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the **access-list** command to create a numbered IP ACL.

```

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any

```

```

R3
Physical  Config  CLI  Attributes
IOS

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to up

User Access Verification

Password:
Password:

R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network (terminal)?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 16.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#

```

Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

R3(config)# **interface s0/0/1**

R3(config-if)# **ip access-group 100 in**

```

R3
Physical Config CLI Attributes
IOS Command Lin

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

User: Access Verification
Password:
Password:

R3>enable
Password:
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 5 10
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.16.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 16.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interf
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#

```

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the **PC-C** command prompt, ping the **PC-A** server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

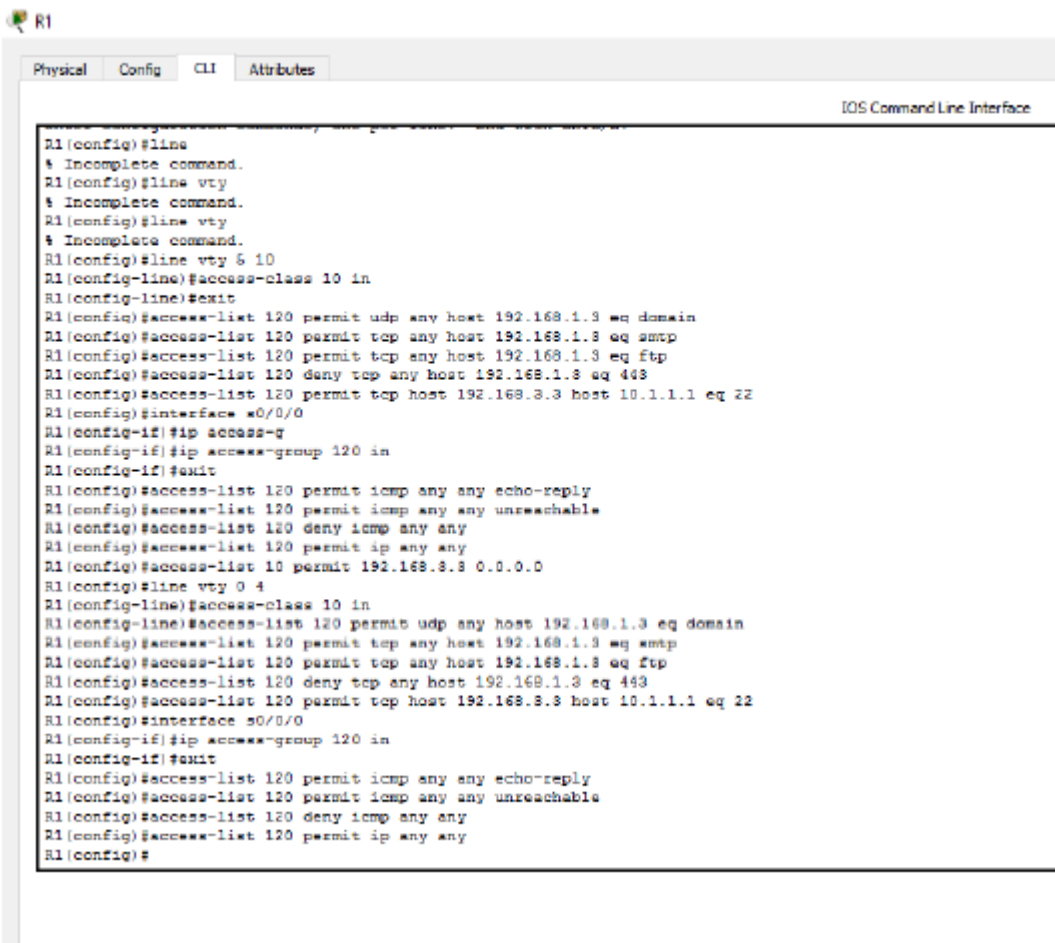
!!!Script for R1

```

access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 120 permit udp any host 192.168.1.3 eq domain
access-list 120 permit tcp any host 192.168.1.3 eq smtp
access-list 120 permit tcp any host 192.168.1.3 eq ftp
access-list 120 deny tcp any host 192.168.1.3 eq 443
access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

```

```
interface s0/0/0
ip access-group 120 in
access-list 120 permit icmp any any echo-reply
access-list 120 permit icmp any any unreachable
access-list 120 deny icmp any any
access-list 120 permit ip any any
```



```
R1
R1 (config)#line
R1 (config)#line vty
R1 (config)#line vty
R1 (config)#line vty 5 10
R1 (config-line)#access-class 10 in
R1 (config-line)#exit
R1 (config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1 (config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1 (config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1 (config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1 (config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1 (config)#interface s0/0/0
R1 (config-if)#ip access-g
R1 (config-if)#ip access-group 120 in
R1 (config-if)#exit
R1 (config)#access-list 120 permit icmp any any echo-reply
R1 (config)#access-list 120 permit icmp any any unreachable
R1 (config)#access-list 120 deny icmp any any
R1 (config)#access-list 120 permit ip any any
R1 (config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1 (config)#line vty 0 4
R1 (config-line)#access-class 10 in
R1 (config-line)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1 (config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1 (config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1 (config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1 (config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1 (config)#interface s0/0/0
R1 (config-if)#ip access-group 120 in
R1 (config-if)#exit
R1 (config)#access-list 120 permit icmp any any echo-reply
R1 (config)#access-list 120 permit icmp any any unreachable
R1 (config)#access-list 120 deny icmp any any
R1 (config)#access-list 120 permit ip any any
R1 (config)#
```

!!!Script for R2

```
access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
```

```

Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
R2>enable
Password:
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#conf line
^
% Invalid input detected at '^' marker.

R2#
R2#config-line
Translating "config-line"...domain server (0.0.0.0)
% Unknown command or computer name, or unable to find computer address

R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 5 10
R2(config-line)#access-class 10 in
R2(config-line)#exit
R2(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#

```

!!!Script for R3

```

access-list 10 permit 192.168.3.3 0.0.0.0
line vty 0 4
access-class 10 in
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit ip any any
interface s0/0/1
ip access-group 100 in
access-list 110 permit ip 192.168.3.0 0.0.0.255 any
interface fa0/1
ip access-group 110 in

```

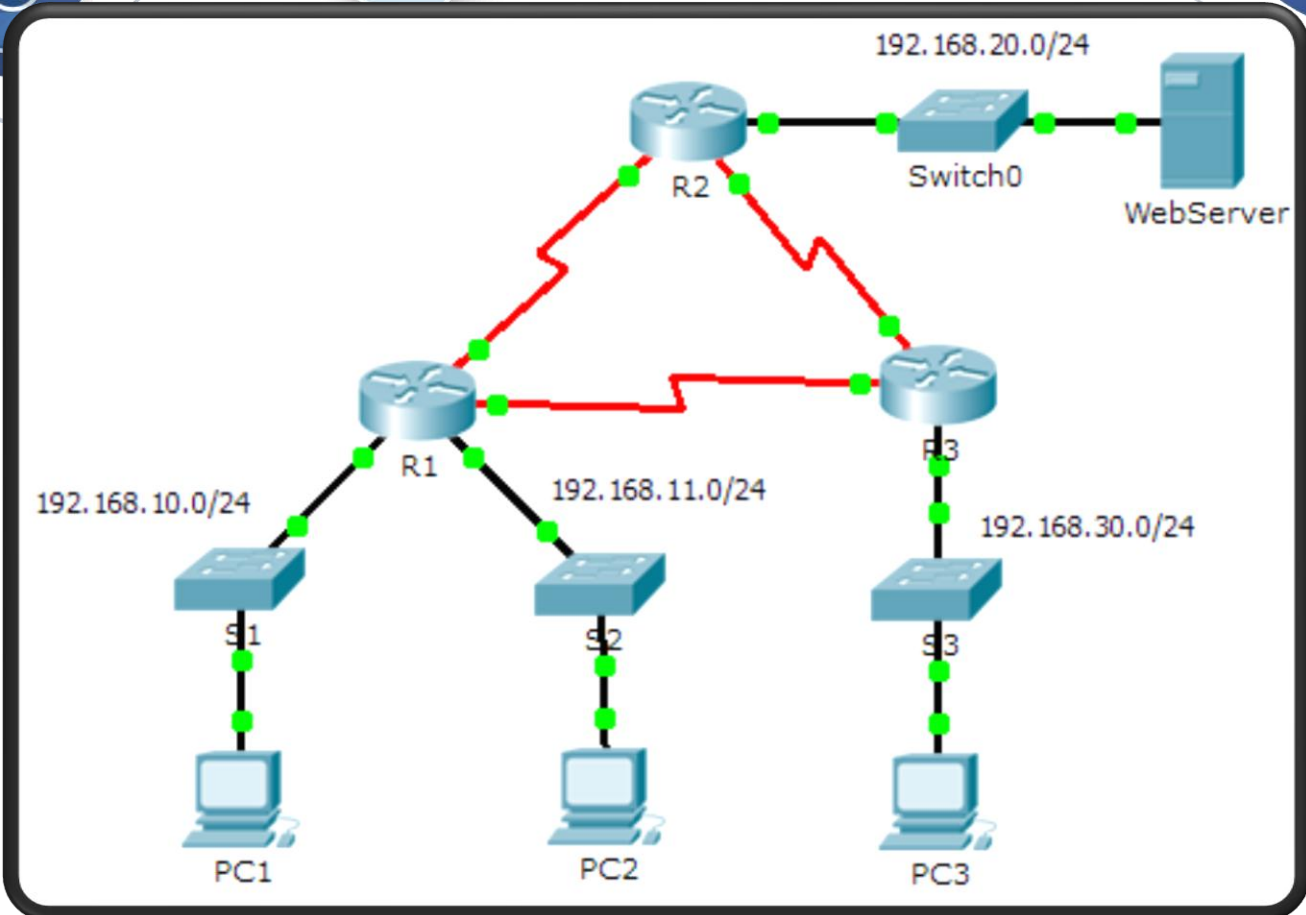
```

R3
Physical Config CLI Attributes
IOS Command Line
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 16.256.256.256 any
R3(config)#access-list 100 permit ip any any
R3(config)#intertf
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#exit
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#access-list 120 permit udp any host 192.168.1.3 eq domain
R3(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R3(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R3(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R3(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R3(config)#interface s0/0/0
R3(config-if)#ip access-group 120 in
R3(config-if)#exit
R3(config)#access-list 120 permit icmp any any echo-reply
R3(config)#access-list 120 permit icmp any any unreachable
R3(config)#access-list 120 deny icmp any any
R3(config)#access-list 120 permit ip any any
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.16.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 16.256.256.256 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface fa0/1
R3(config-if)# ip access-group 110 in
R3(config-if)#
  
```

Packet

Tracer - Configuring Standard ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A

	S0/0/1	10.3.3.1	255.255.255.2 52	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.2 52	N/A
	S0/0/1	10.2.2.1	255.255.255.2 52	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.2 52	N/A
	S0/0/1	10.2.2.2	255.255.255.2 52	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.25 4	255.255.255.0	192.168.20.1

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Información básica/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la

ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1:

planificar una implementación de ACL

Paso 1:

investigar la configuración actual de red.

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

Debería poder hacer ping correctamente a todos los dispositivos.

Paso 2:

evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el

R2

están implementadas las siguientes políticas de red:

-

La red 192.168.11.0/24 no tiene permiso para acceder al servidor web en la red 192.168.20.0/24.

-

Se permite el resto de los tipos de acceso. Para restringir el acceso de la red 192.168.11.0/24 al servidor web en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el R2

- . La lista de acceso se debe colocar en la interfaz de salida hacia el servidor web

- . Se debe crear una segunda regla en el R2 para permitir el resto del tráfico.

b. En el

R3

están implementadas las siguientes políticas de red:

-

La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.

-

Se permite el resto de los tipos de acceso. Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el R3

- . La ACL se debe colocar en la interfaz de salida hacia la PC3

- .

- . Se debe crear una segunda regla en el

R3
para permitir el resto del tráfico.

Parte 2:
configurar, aplicar y verificar una ACL estándar

Paso 1:

configurar y aplicar una ACL estándar numerada en el R2.

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

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

b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con una regla.

Para permitir el resto del tráfico, configure la siguiente instrucción:

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

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

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

Paso 2:

configurar y aplicar una ACL estándar numerada en el R3.

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

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

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

```
R3(config)#
access-
```



list 1 permit any

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

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

Paso 3:

verificar la configuración y la funcionalidad de la ACL.

a. En el R2 y el R3, introduzca el comando show access-list para verificar las configuraciones de la ACL.

Introduzca el comando show run o show ip interface gigabitethernet 0/0 para verificar la colocación de las ACL.

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

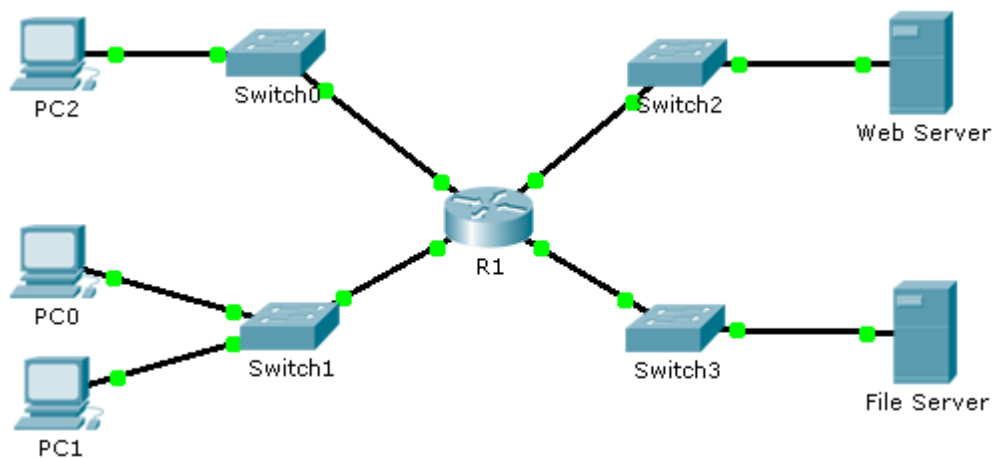
- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
- Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
- Un ping de 192.168.11.10 a 192.168.20.254 falla.
- Un ping de 192.168.10.10 a 192.168.30.10 falla.
- Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.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

9.2.1.11 Packet Tracer - Configuring Named Standard ACLs

Packet Tracer - Configuring Named Standard ACLs (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

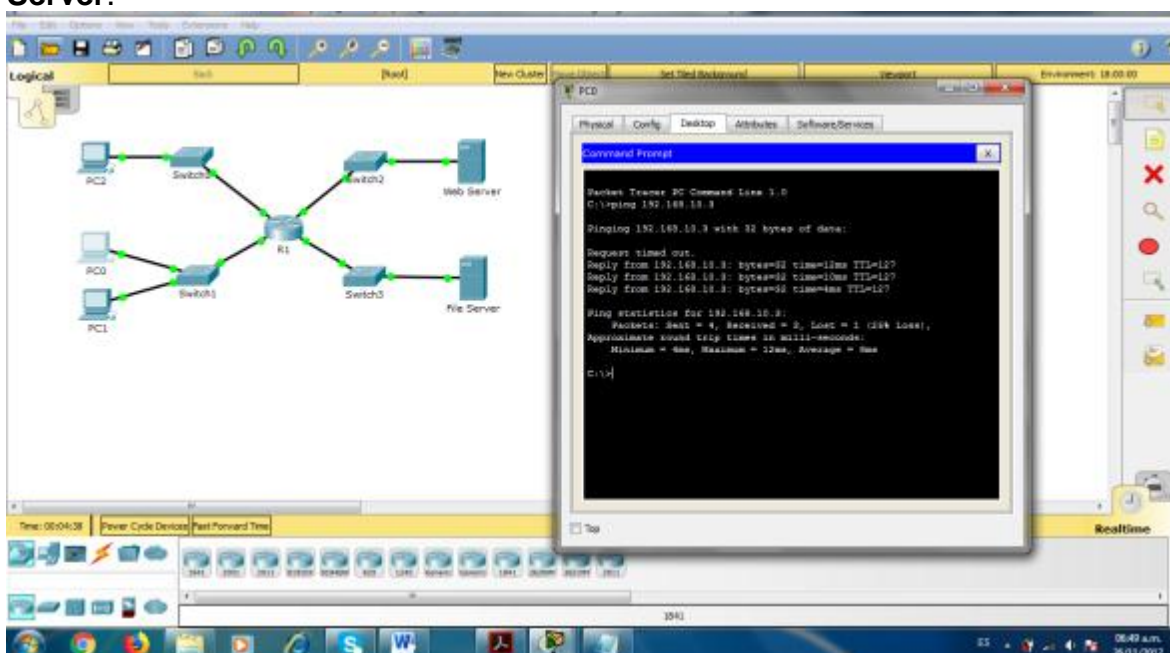
Background / Scenario

The senior network administrator has tasked you to create a standard named ACL to prevent access to a file server. All clients from one network and one specific workstation from a different network should be denied access.

Part 1: Configure and Apply a Named Standard ACL

Step 1: Verify connectivity before the ACL is configured and applied.

All three workstations should be able to ping both the **Web Server** and **File Server**.



The screenshot shows a Packet Tracer environment with a network diagram and a terminal window for PC1. The network diagram includes PC1, PC2, PC3, Switch1, Switch2, Switch3, R1, a Web Server, and a File Server. The terminal window displays the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 17ms, Average = 15ms

C:\>
```

The screenshot shows a Packet Tracer environment with a network diagram and a terminal window for PC2. The network diagram is identical to the one above. The terminal window displays the following output:

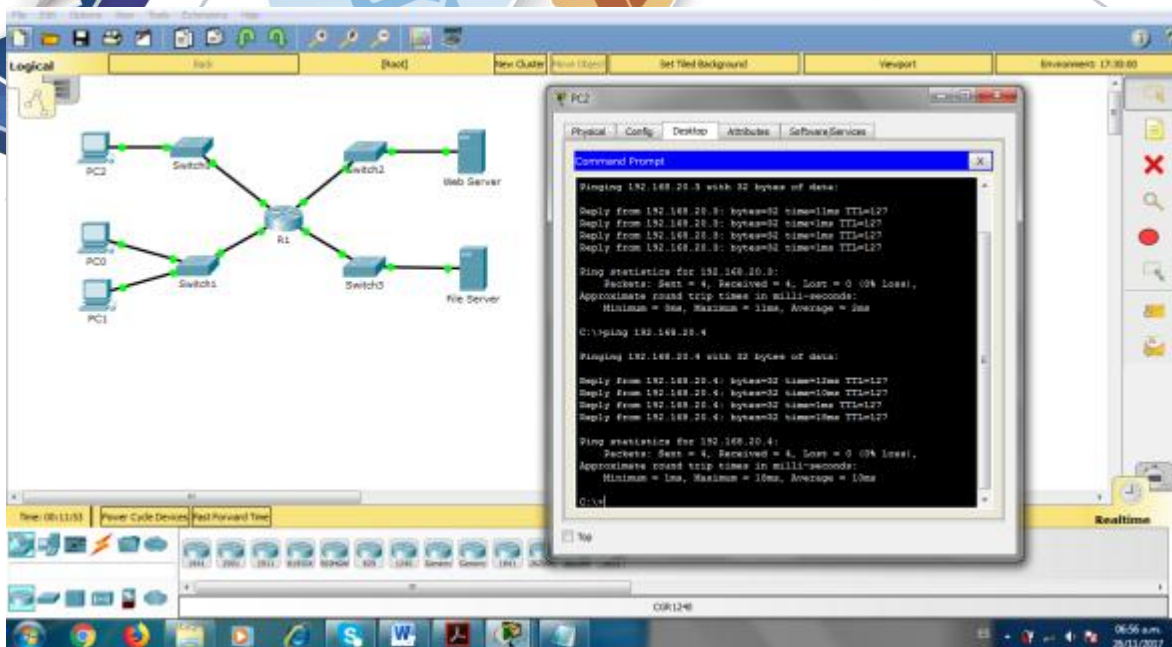
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127
Reply from 192.168.20.3: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 2ms

C:\>
```



Step 2: Configure a named standard ACL.

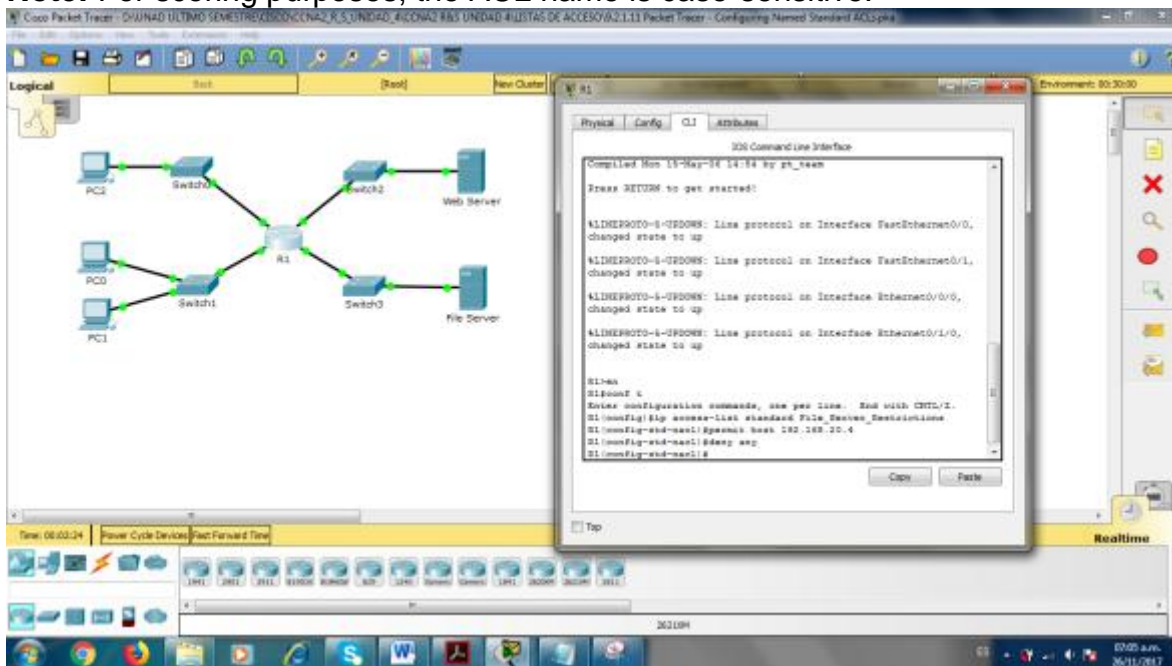
Configure the following named ACL on R1.

```
R1(config)# ip access-list standard File_Server_Restrictions
```

```
R1(config-std-nacl)# permit host 192.168.20.4
```

```
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive.



Step 3: Apply the named ACL.

a. Apply the ACL outbound on the interface Fast Ethernet 0/1.


```

R1#
R1#show ip inter f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.200.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is File Server Restrictions
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  --More--
  
```

Step 2: Verify that the ACL is working properly.

All three workstations should be able to ping the **Web Server**, but only **PC1** should be able to ping the **File Server**.

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time=6ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>
  
```

```

PC2
Physical Config Desktop Attributes Software/Services
Command Prompt

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=5ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
  
```

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:35:54

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

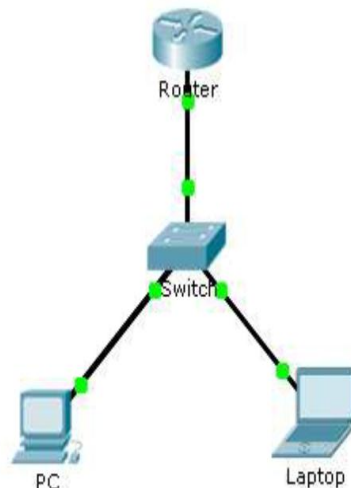
Assessment Items	Status	Points
[-] Network		
[-] R1		
[-] ACL		0
[-] File_Server_Restri...	Correct	80
[-] Ports		0
[-] FastEthernet0/1		0
[-] Access-group ...	Correct	20

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100

Score : 100/100
Item Count : 2/2

Packet Tracer - Configuring an ACL on VTY Lines

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Laptop	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objectives

Part 1: Configure and Apply an ACL to VTY Lines

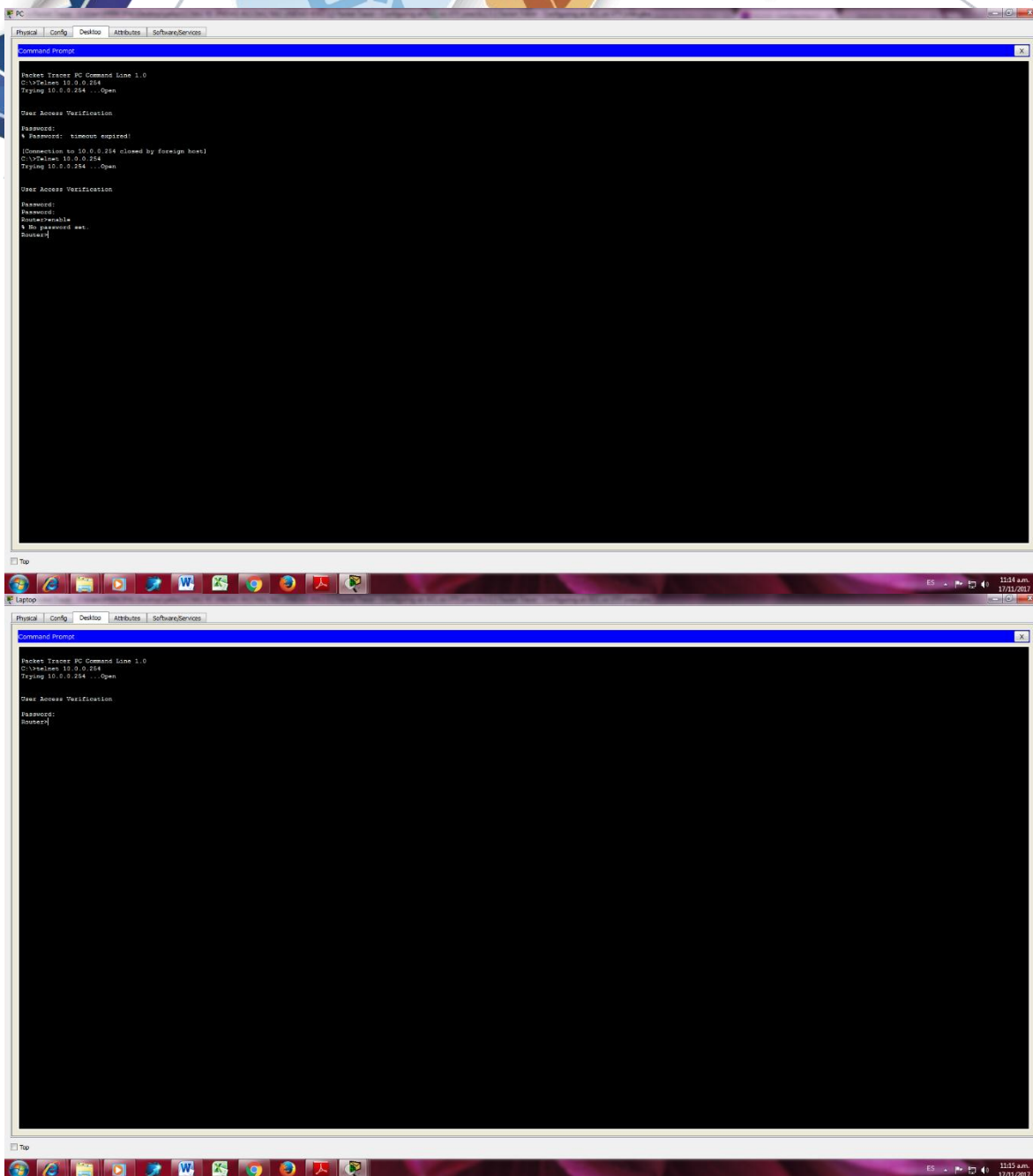
Part 2: Verify the ACL Implementation

Background

Como administrador de red, debe tener acceso remoto a su enrutador. Este acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permite PC acceso a las líneas Telnet, pero niega todas las otras direcciones IP de origen.

Parte 1: configurar y aplicar una ACL a líneas VTY

Paso 1: Verifique el acceso de Telnet antes de que se configure la ACL. Ambas computadoras deberían poder Telnet al Enrutador. La contraseña es Cisco



Step 2: Configure a standard ACL numbered.

Configure the following numbered ACL on Router.

Router (config) # access-list 99 allow host 10.0.0.1

```

Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#access-list 99 deny any
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#end
Router#
MPLS-CORFIS_1: Configured from console by console

Router#show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
 20 deny any
Router#
  
```

Como no queremos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita del acceso lista satisface nuestros requisitos.

```

Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#access-list 99 deny any
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#end
Router#
MPLS-CORFIS_1: Configured from console by console

Router#show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
 20 deny any
Router#
  
```

Paso 3: Coloque una ACL estándar nombrada en el enrutador.

Se debe permitir el acceso a las interfaces del enrutador, mientras que el acceso a Telnet debe estar restringido. Por lo tanto, debemos ubicar la ACL en las líneas Telnet 0 a 4. Desde el indicador de configuración de Router, ingrese al modo de

configuración de línea para las líneas 0 - 4 y use el comando access-class para aplicar la ACL a todas las líneas VTY:

Router (config) # line vty 0 15
Router (config-line) # access-class 99 en

The screenshot displays a Cisco Packet Tracer environment. The top window shows the configuration of a router (R1) in the CLI. The configuration includes enabling the router, setting the hostname to 'R1', and configuring an access list (ACL) named '99' to permit traffic from 10.0.0.1 and deny all other traffic. This ACL is then applied to VTY lines 0 through 15. The bottom window shows the 'Activity Results' for this task, indicating a score of 100/100 and a completion time of 01:51:36. The results table is as follows:

Assessment Item	Status	Points	Component(s)	Feedback
Router		70		
ACL		0	ACL	
ACL 99	Correct	70	IPv4 Standard...	
VTY Lines		0		
VTY Line 0		0	Physical	
Access Conf...	Correct	5	IPv4 Standard...	
VTY Line 1		0	Physical	
Access Conf...	Correct	5	IPv4 Standard...	
VTY Line 2		0	Physical	
Access Conf...	Correct	5	IPv4 Standard...	
VTY Line 3		0	Physical	
Access Conf...	Correct	5	IPv4 Standard...	
VTY Line 4		0	Physical	
Access Conf...	Correct	5	IPv4 Standard...	

Parte 2: Verificar la implementación de ACL

```

Router>
Router>enable
Router#configure terminal
Router(config)#access-list 99 deny any
Router(config)#exit
Router>
Router>show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
 20 deny any
Router#
Router con0 is now available.

Press RETURN to get started.

Router#enable
Router#configure terminal
Router(config)#access-list 99 deny any
Router(config)#exit
Router>
Router>show access-lists
Router#access
Translating "access"...domain server (10.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#access
Translating "access"...domain server (10.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#config t
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config)#line#access-class 99 in
Router(config)#line#
  
```

Paso 1: Verifique la configuración de ACL y la aplicación a las líneas VTY.

```

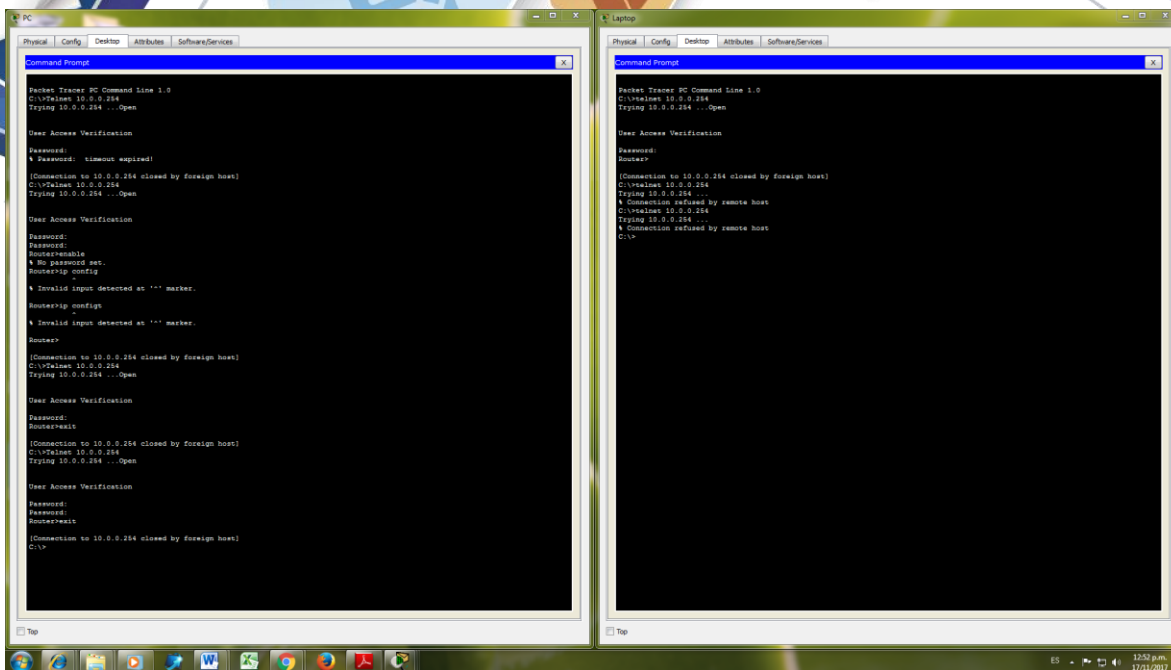
Router>
Router>enable
Router#configure terminal
Router(config)#access-list 99 deny any
Router(config)#exit
Router>
Router>show access-lists
Standard IP access list 99
 10 permit host 10.0.0.1
 20 deny any
Router#
Router con0 is now available.

Press RETURN to get started.

Router#enable
Router#configure terminal
Router(config)#access-list 99 deny any
Router(config)#exit
Router>
Router>show access-lists
Router#access
Translating "access"...domain server (10.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#access
Translating "access"...domain server (10.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router#config t
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config)#line#access-class 99 in
Router(config)#line#
  
```

Use las listas de acceso del programa para verificar la configuración de ACL. Use el comando show run para verificar que la ACL se aplica a las líneas VTY.

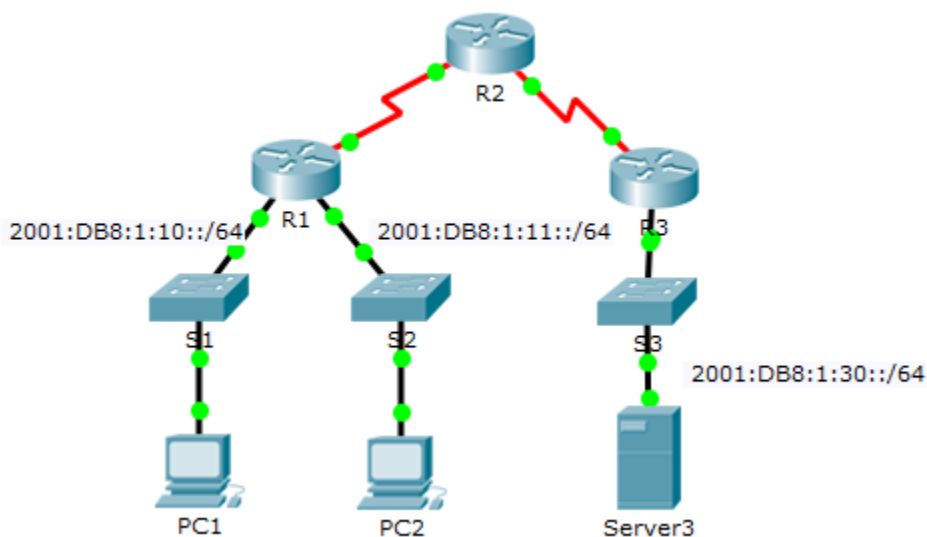
Paso 2: Verifique que la ACL esté funcionando correctamente.



Ambas computadoras deberían poder hacer ping al Enrutador, pero solo las PC deberían poder usar Telnet.

9.5.2.6 Packet Tracer - Configuring IPv6 ACLs

Topology



Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Part 1: Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing their web page causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

Step 1: Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK_HTTP** on **R1** with the following statements.

- Block HTTP and HTTPS traffic from reaching **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

- Allow all other IPv6 traffic to pass.

```
R1(config)#
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any
R1(config-ipv6-acl)#
```

Step 2: Apply the ACL to the correct interface.

Apply the ACL on the interface closest the source of the traffic to be blocked.

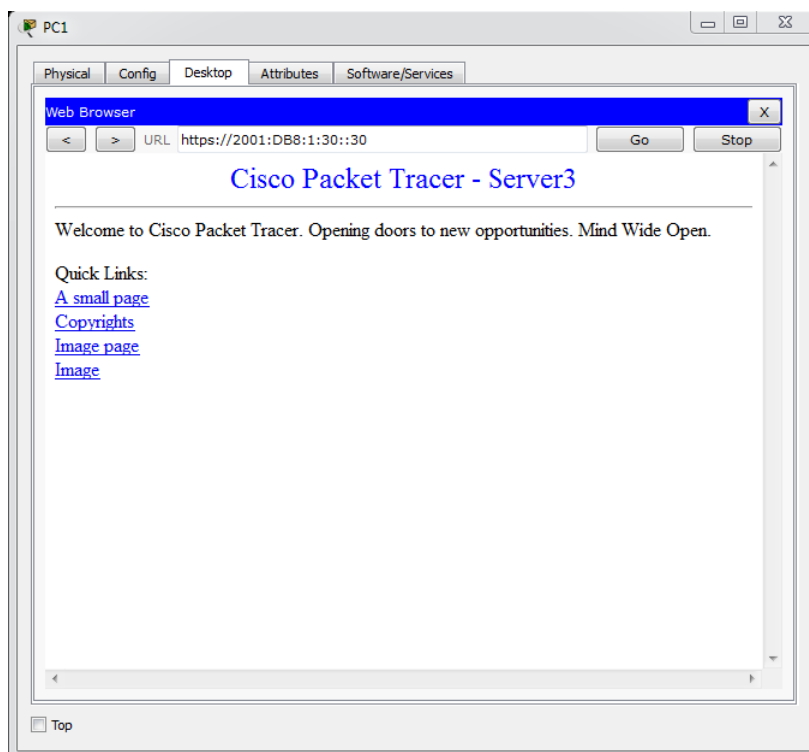
```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

```
R1(config)#interface g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#
```

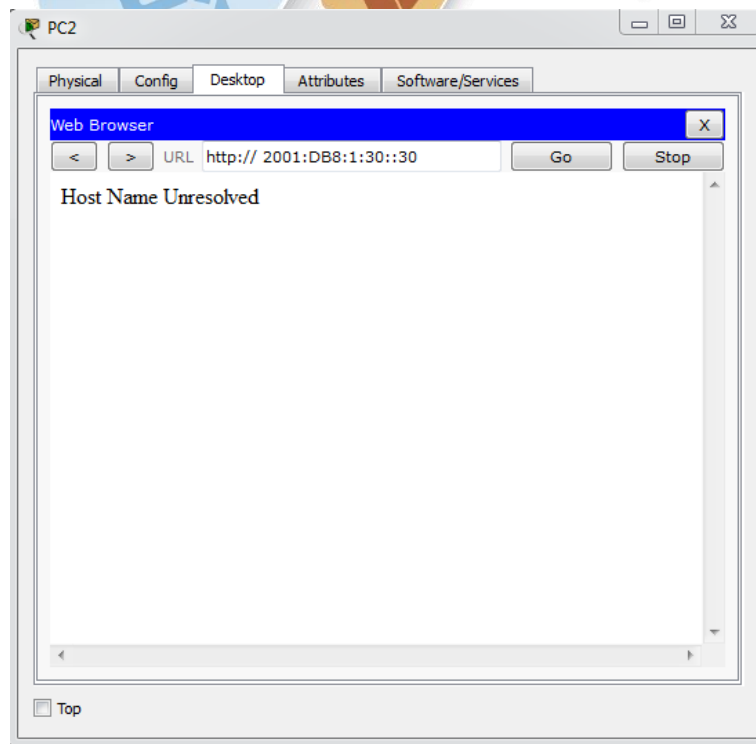
Step 3: Verify the ACL implementation.

Verify the ACL is operating as intended by conducting the following tests:

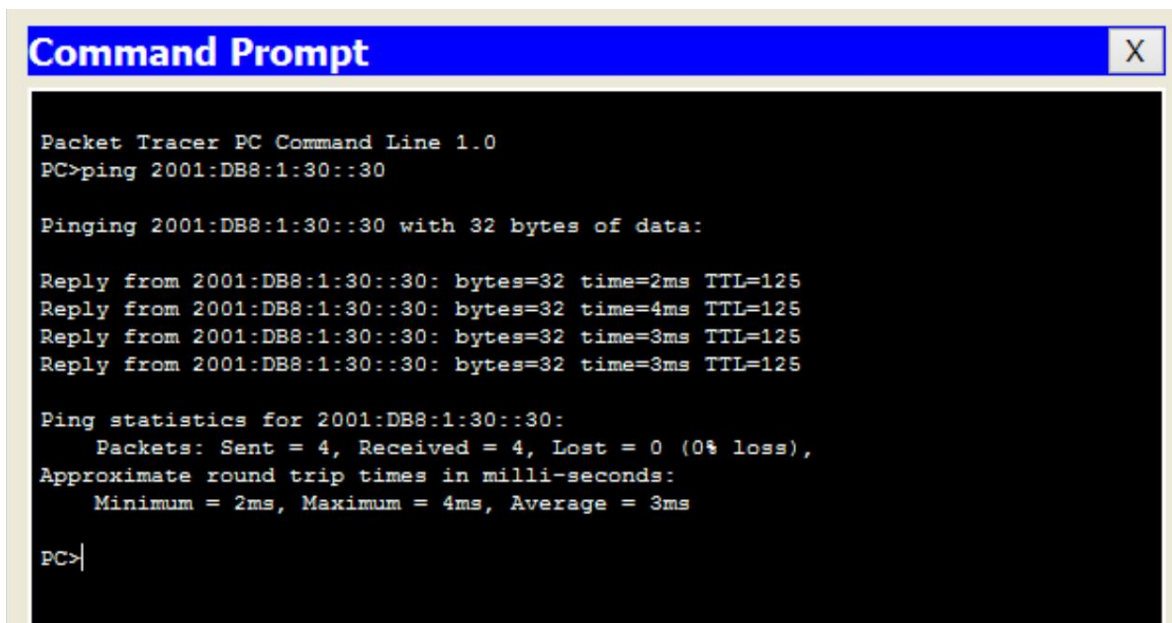
- Open the **web browser** of **PC1** to `http:// 2001:DB8:1:30::30` or `https://2001:DB8:1:30::30`. The website should appear.



- Open the **web browser** of **PC2** to `http:// 2001:DB8:1:30::30` or `https://2001:DB8:1:30::30`. The website should be blocked



- Ping from **PC2** to 2001:DB8:1:30::30. The ping should be successful.



Part 2: Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named **BLOCK_ICMP** on **R3** with the following statements:

- Block all ICMP traffic from any hosts to any destination.
- Allow all other IPv6 traffic to pass.

```
R3(config)#
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#exit
R3(config)#
```

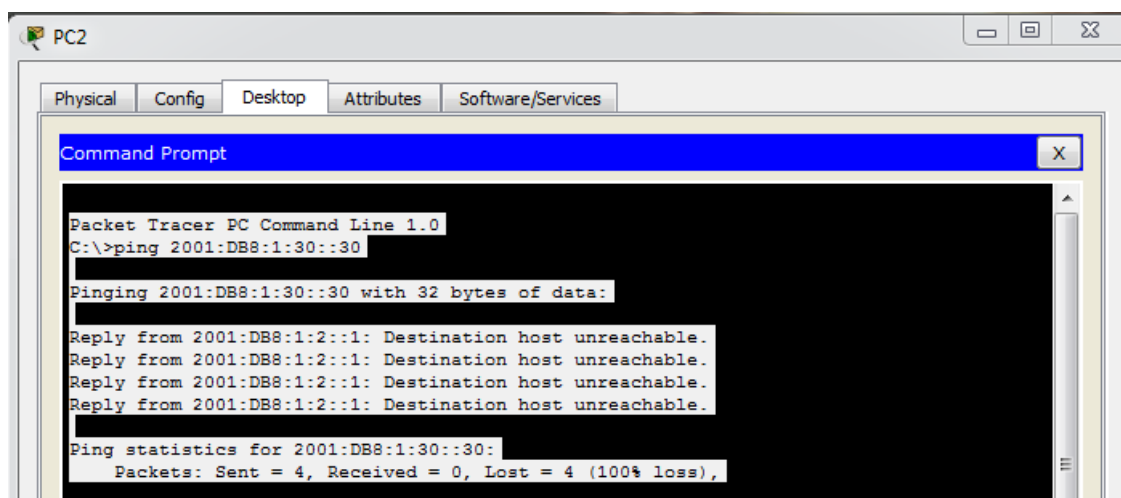
Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked regardless of its source or changes that occur to the network topology, apply the ACL closest to the destination.

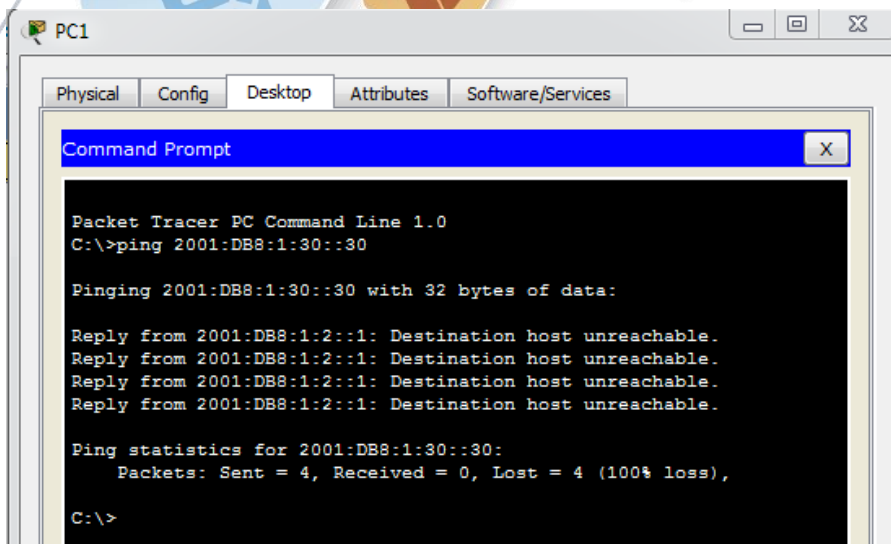
```
R3(config)#interface g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Step 3: Verify that the proper access list functions.

- Ping from **PC2** to 2001:DB8:1:30::30. The ping should fail.

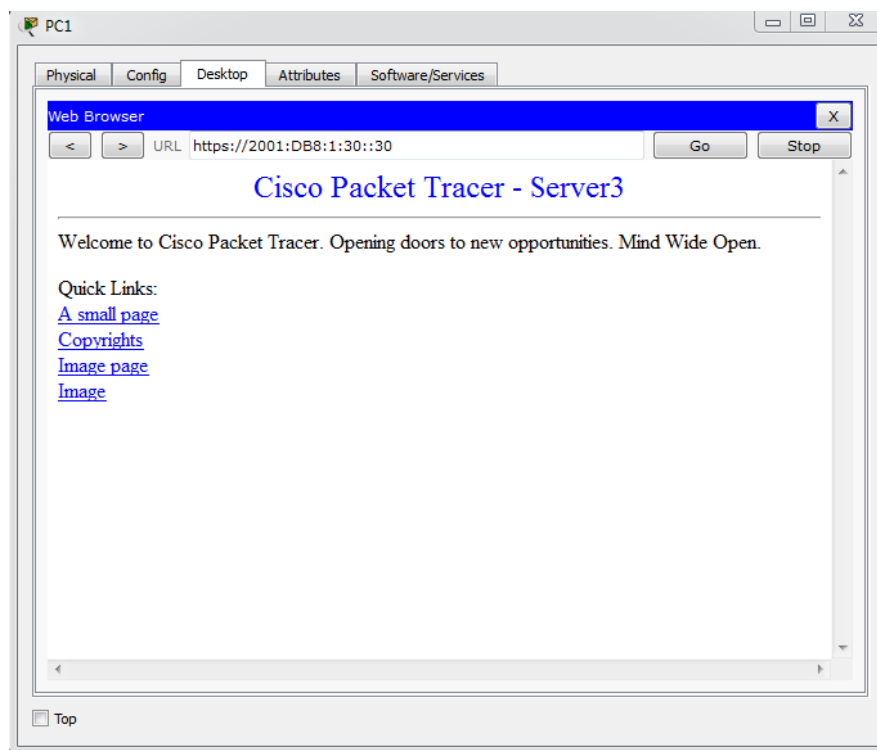


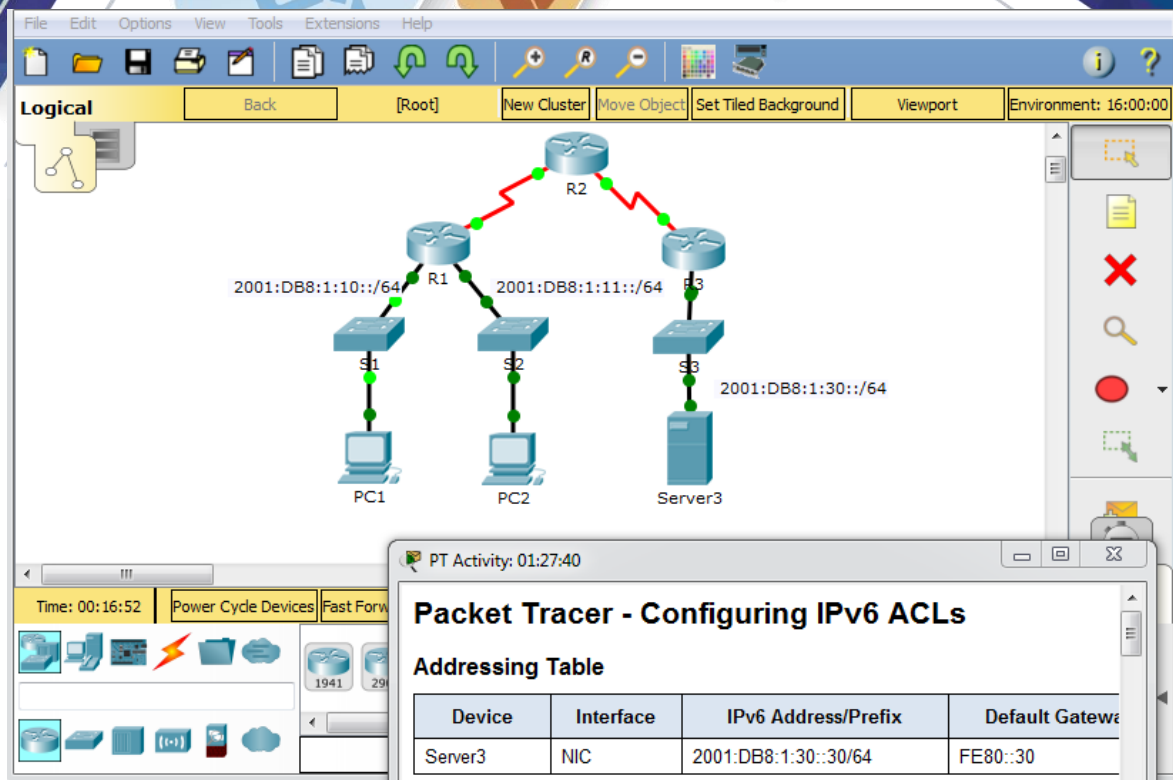
- Ping from **PC1** to 2001:DB8:1:30::30. The ping should fail.



C.

Open the **web browser** of **PC1** to [http:// 2001:DB8:1:30::30](http://2001:DB8:1:30::30) or <https://2001:DB8:1:30::30>. The website should display.





PT Activity: 01:27:40

Packet Tracer - Configuring IPv6 ACLs

Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectives

- Part 1: Configure, Apply, and Verify an IPv6 ACL
- Part 2: Configure, Apply, and Verify a Second IPv6 ACL

Time Elapsed: 01:27:40 Completion: 100/100

Top




CONCLUSIONES

Mediante la realización de los ejercicios prácticos propuestos en la unidad 4 el grupo complementa las instrucciones recibidas en dicha unidad, concerniente al enrutamiento dinámico en Routers, se amplía los conocimientos en cuanto al uso de algunos protocolos de enrutamiento como: EIGRP, IS-IS, OSPF, entre otros, de igual modo se comprende la importancia de listas de control de acceso (ACL) para darle mayor seguridad a nuestras redes.

En consecuencia se destaca que el componente práctico mediante el software de Packet-Tracer, en los cursos dictados por la UNAD facilita la interacción educativa a su vez ayuda al estudiante en eficacia del proceso de aprendizaje sobre las redes de comunicaciones.

En conclusión todo el proceso practico y teórico se completan y se hacen una realidad para nosotros mediante la simulación de cada ejercicio propuesto en el curso.





REFERENCIAS

CISCO. (s.f.). *CAPITULO 10. DETECCION, ADMINISTRACION Y MANTENIMIENTO DE DISPOSITIVOS*. Recuperado el 6 de MAYO de 2017, de <https://www.netacad.com/es/>

CISCO. (s.f.). *CAPÍTULO 7. LISTAS DE CONTROL DE ACCESO*. Recuperado el 6 de MAYO de 2017, de <https://www.netacad.com/es/>

CISCO. (s.f.). *CAPITULO 8. DHCP*. Recuperado el 6 de MAYO de 2017, de <https://www.netacad.com/es/>

CISCO. (s.f.). *CAPITULO 9. NAT PARA IPV4*. Recuperado el 6 de MAYO de 2017, de <https://www.netacad.com/es/>

