Diplomado de Profundización CISCO CCNA1 & CCNA2

TRABAJO FINAL

Por:

Juan Carlos González Gutiérrez Código: 71756115

Roger Medrano Serpa Código: 92.446.117

Kelvin Abdala Lambraño, Código:

Elkin Rodríguez Pérez, Código: 1045683173

Jader Martínez, Código: 92548106

Grupo: 203092_5

Tutor

Gerardo Granados Acuña

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería

Programa de Ingeniería de Sistemas

Introducción

Manifiestamente estamos inmersos en una época de auge tecnológico, donde los avances en múltiples áreas son parte fundamental de la vida cotidiana, las telecomunicaciones y las nuevas técnicas de información y comunicación han adquirido gran relevancia en el desarrollo de la humanidad. Por lo tanto, la comprensión ínfima de cómo ocurren estos procesos de intercambio de información es de vital relevancia para nosotros como futuros ingenieros de sistemas, ya que cae directamente en el campo de las redes informáticas.

Teniendo en cuenta las anteriores apreciaciones, a continuación presentamos un informe de laboratorio de CCNA2, en el cual se presentan casos de configuración y resolución de problemas en el ámbito de la comunicación entre diversos dispositivos de red, utilizando el simulador Packet Tracer como parte sine qua non en la realización de esta actividad.

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar) que se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

El motivo más importante para configurar ACL es aportar seguridad a una red. En este capítulo, se explica cómo utilizar las ACL estándar y extendidas en un router
Cisco como parte de una solución de seguridad. Se incluyen consejos, consideraciones, recomendaciones y pautas generales sobre cómo utilizar las ACL.
La puesta de un servidor de protocolo de configuración dinámica de host (DHCP) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la

administración de direcciones IP sea más eficaz y asegura la coherencia en toda la[iii] organización, incluso en las sucursales.

DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6). En este capítulo, se explora la funcionalidad, la configuración y la resolución de problemas de DHCPv4 y de DHCPv6.

El diplomado de profundización cnn2 pretende desarrollar competencias de carácter analítico orientadas a la comprensión y formulación de hipótesis para la solución de situaciones propias del campo de las Telecomunicaciones. El desarrollo de competencias cognitivas lo llevan al establecimiento de metas, la comprensión e interpretación plasmados en ensayos, simulaciones, estudios de caso, análisis y síntesis. Aportando al estudiante herramientas teóricas que lo lleven a conceptualizar la ciencia, ingeniería y tecnología como base para la fundamentación de la Tecnología de Redes.

En este trabajo finalmente los datos y el desarrollo de los ejercicios anteriormente resueltos servirán eficientemente para profundizar nuestra base lógica en lo que concierne a la primera parte de los temas que abordan el Curso de Profundización de Cisco en su Modulo CCNA 2: Conceptos y Protocolos de Enrutamiento, más en particular de temas tales como Introducción al Enrutamiento y Envio de Paquetes y Enrutamiento Estático, además para aumentar nuestros conocimientos sobre el tema, que de una u otra manera, será aplicado en un determinado momento de nuestra vida laboral.


UNAD
Universidad Nacional
Abierta y a Distancia

Objetivos

Generales

Analizar, entender y comprender la configuración y funcionalidad de Switches, routers y otros dispositivos en redes pequeñas, mediante el desarrollo de prácticas simuladas de laboratorios que propendan por la adquisición de las competencias necesarias para la configuración y resolución de la conectividad entre dispositivos de redes.

Específicos

- Explicar el propósito y el funcionamiento de las ACL.
- Establecer la topología e inicializar los dispositivos, configurar los dispositivos y verificar la conectividad, configurar y verificar ACL estándar numeradas y con nombre, modificar una ACL estándar.
- Configurar los parámetros básicos de los dispositivos, configurar y aplicar la lista de control de acceso en el R1, verificar la lista de control de acceso mediante Telnet, configurar y aplicar la lista de control de acceso en el S1 (desafío).
- Establecer la topología e inicializar los dispositivos, configurar los dispositivos y verificar la conectividad, configurar y verificar las ACL de IPv6, editar las ACL de IPv6.
- Establecer la topología e inicializar los dispositivos, configurar los dispositivos y verificar la conectividad, configurar y verificar ACL extendidas numeradas y con nombre, modificar y verificar ACL extendidas.
- Armar la red y configurar los parámetros básicos de los dispositivos, resolver problemas de acceso interno, resolver problemas de acceso remoto.
- Implementar el filtrado de paquetes con ACL de IPv4 extendidas, según los requisitos de la red (incluir ACL con nombre y numeradas).
- Configurar DHCP para IPv4 en un switch LAN.

- Armar la red y configurar los parámetros básicos de los dispositivos, configurar un[vi] servidor de DHCPv4 y un agente de retransmisión DHCP Armar la red y configurar los parámetros básicos de los dispositivos, cambiar la preferencia de SDM, configurar DHCPv4, configurar DHCP para varias VLAN, habilitar el routing IP.
- Armar la red y configurar los parámetros básicos de los dispositivos, resolver problemas de DHCPv4.
- Armar la red y configurar los parámetros básicos de los dispositivos, configurar la red para SLAAC, configurar la red para DHCPv6 sin estado, configurar la red para DHCPv6 con estado.
- Armar la red y configurar los parámetros básicos de los dispositivos, resolver problemas de conectividad de IPv6, resolver problemas de DHCPv6 sin estado.
- Configure DHCP para IPv4 o IPv6 en un router Cisco 1941 Describa las características de NAT.
- Armar la red y verificar la conectividad, configurar y verificar la NAT estática, configurar y verificar la NAT dinámica.
- Armar la red y verificar la conectividad, configurar y verificar un conjunto de NAT con sobrecarga, configurar y verificar PAT.
- Armar la red y configurar los parámetros básicos de los dispositivos, resolver problemas de la NAT estática, resolver problemas de la NAT dinámica.
- Configure, verifique y analice la NAT estática, la NAT dinámica y la NAT con sobrecarga.

Contenido

Informe 1

10.1.2.4 Lab - Configuring Basic DHCPv4 on a Router

Práctica de laboratorio: configuración de dhcpv4 básico en un Router

Topología

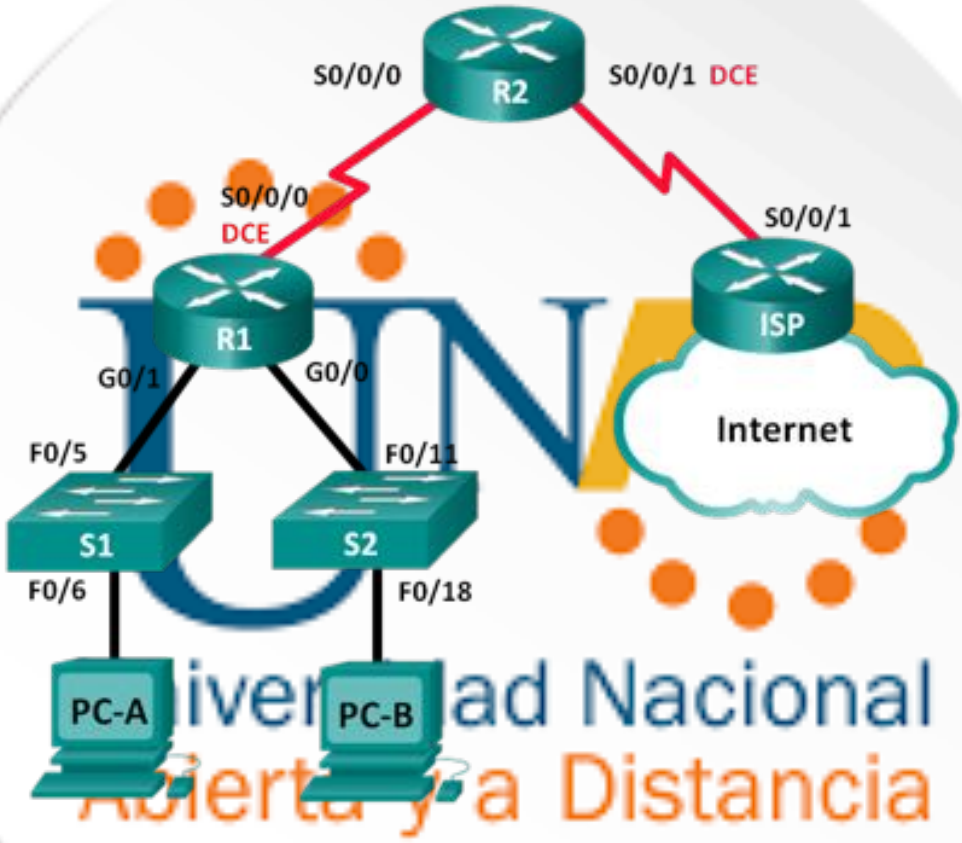


Tabla de direccionamiento

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

Parte1: 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.

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

Paso 2. inicializar y volver a cargar los routers y los switches.

Paso 3. configurar los parámetros básicos para cada router.

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 interrumpan 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

Paso 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.

Paso 5. verificar que los equipos host estén configurados para DHCP.

Parte 2: 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.

Paso 6. 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.

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)# 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

R2(dhcp-config)# dns-server 209.165.200.225

R2(dhcp-config)# lease 2

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 host no han recibido una dirección ip del servidor DHCP en R2 ya que R1 no ha sido configurado como un agente repetidor DHCP

Paso 7. 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(config)# interface g0/0

R1(config-if)# ip helper-address 192.168.2.254

R1(config-if)# exit R1(config)# interface g0/1

R1(config-if)# ip helper-address 192.168.2.254

Paso 8. 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 - MAC: 0001.C950.5C1D

PC-A - IP: 192.168.1.10

PC-B - MAC: 0050.0F93.3A09

PC-B - IP: 192.168.0.10

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-A: 192.168.0.10

PC-B: 192.168.1.10

Paso 9. 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?

   R2#show ip dhcp binding

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.10	0001.C950.5C1D	--	Automatic
192.168.0.10	0050.0F93.3A09	--	Automatic

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.

R2# show ip dhcp server statistics

Memory usage 42175

Address pools 2

Database agents 0

Automatic bindings 2

Manual bindings 0

Expired bindings 0

Malformed messages 0

Secure arp entries 0

Message Received

BOOTREQUEST 0

DHCPDISCOVER 2

DHCPREQUEST 2

DHCPDECLINE 0

DHCPRELEASE 0

DHCPINFORM 2

Message Sent

BOOTREPLY 0

DHCPOFFER 2

DHCPACK 4

DHCPNAK 0

¿Cuántos tipos de mensajes DHCP se indican en el resultado?

Se muestran 10 tipos de mensajes diferentes

c. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.

R2# show ip dhcp pool

Pool R1G1 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

Pending event : none

1 subnet is currently in the pool:

Current index IP address range Leased addresses

192.168.1.11 192.168.1.1 - 192.168.1.254 1

d.

Pool R1G0:

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

Pending event : none

1 subnet is currently in the pool :

Current index IP address range Leased addresses

192.168.0.11 192.168.0.1 - 192.168.0.254 1

En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current index)?

La próxima dirección disponible para arrendar

e. En el R2, introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.

R2# show run | section dhcp

ip dhcp excluded-address 192.168.0.1 192.168.0.9

ip dhcp excluded-address 192.168.1.1 192.168.1.9

ip dhcp pool R1G1

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 209.165.200.225

lease 2 ip dhcp pool R1G0

network 192.168.0.0 255.255.255.0

default-router 192.168.0.1

dns-server 209.165.200.225

lease 2

f. 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.

R2# show run interface g0/0

Building configuration...

Current configuration : 132 bytes

!

interface GigabitEthernet0/0

ip address 192.168.0.1 255.255.255.0

ip helper-address 192.168.2.254

duplex auto

speed auto

end

R2# show run interface g0/1

Building configuration...

Current configuration : 132 bytes

!

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

ip helper-address

92.168.2.254

duplex auto

speed auto

end

Reflexión

¿Cuál cree que es el beneficio de usar agentes de retransmisión DHCP en lugar de varios routers que funcionen como servidores de DHCP?

Utilizar un único servidor DHCP con agentes retransmisores ofrece muchos beneficios, como la centralización de la red (Ya que todas las direcciones se ofrecerán desde un único servidor), eficiencia y mejora en el rendimiento (solo un dispositivo se encarga de DHCP y los demás equipos liberan carga al no tener que volver a asignar ellos dhcp), facilidad en el mantenimiento (ya que hay que mantener solo un dispositivo y no uno por cada subred)

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

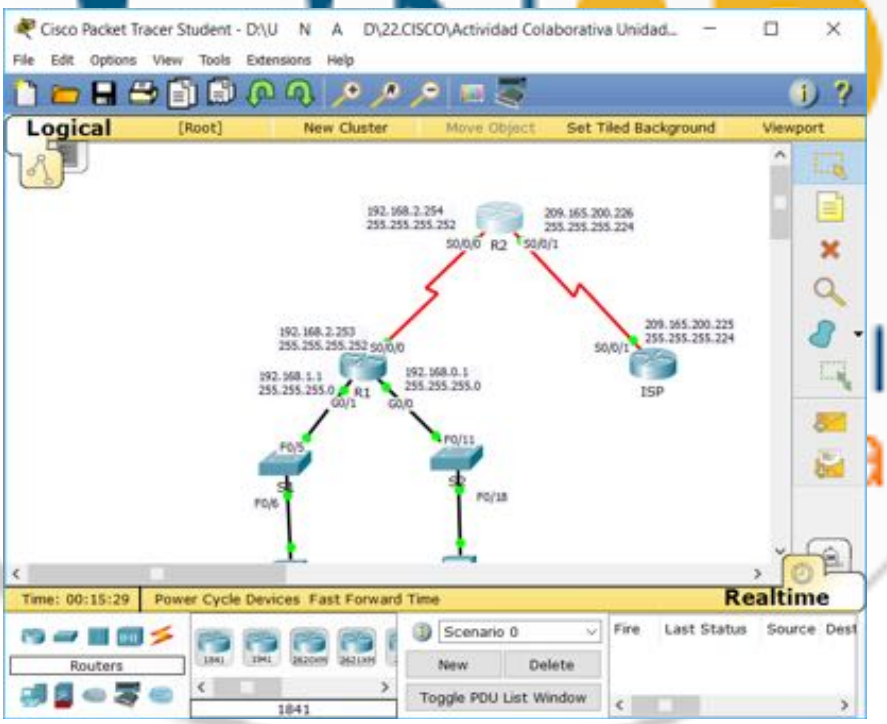
R1(config)# **interface g0/0**
R1(config-if)# **ip helper-address 192.168.2.254**
R1(config-if)# **exit**
R1(config-if)# **interface g0/1**
R1(config-if)# **ip helper-address 192.168.2.254**

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
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

Captura de Evidencia



Informe2

Laboratorio 10.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch

Práctica de laboratorio: configuración de DHCPv4 básico en un switch

Topología

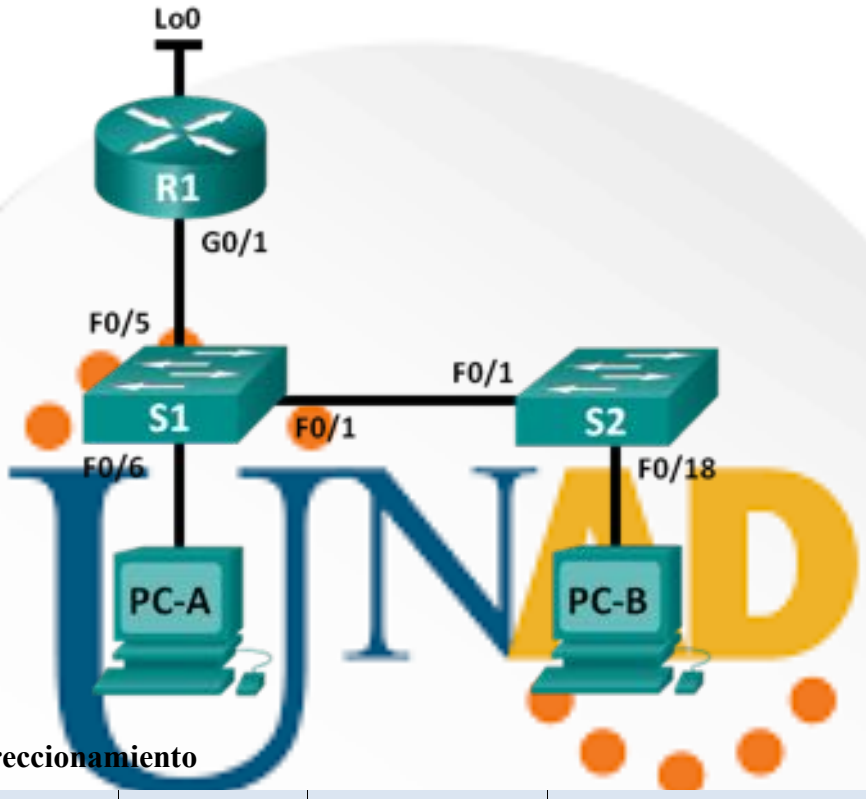


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	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 1. 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.

Parte 2. 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 “default dual-ipv4-and-ipv6” o “lanbase-routing”.

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

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.

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 3. 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.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.1.0/24. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ipdhcp excluded-address 192.168.1.1 192.168.1.10

b. Cree un pool de DHCP con el nombre **DHCP1**. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ipdhcp pool DHCP1

c. Asigne la red 192.168.1.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# network 192.168.1.0 255.255.255.0

d. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# default-router 192.168.1.1

e. Asigne el servidor DNS como 192.168.1.9. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# dns-server 192.168.1.9

f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# lease 3

g. 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**

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**

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? **SÍ**

¿Es posible hacer ping de la PC-A a la PC-B? **SÍ**

¿Es posible hacer ping de la PC-A a la interfaz G0/1 del R1? **SÍ**

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

Parte 4. *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.

S1(config)# interface f0/6

S1(config-if)# switchport access vlan 2

Paso 2. configurar DHCPv4 para la VLAN 2.

a. Excluya las primeras 10 direcciones host válidas de la red 192.168.2.0. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ipdhcp excluded-address 192.168.2.1 192.168.2.10

b. Cree un pool de DHCP con el nombre **DHCP2**. En el espacio proporcionado, escriba el comando que utilizó.

S1(config)# ipdhcp pool DHCP2

c. Asigne la red 192.168.2.0/24 para las direcciones disponibles. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# network 192.168.2.0 255.255.255.0

d. Asigne el gateway predeterminado como 192.168.2.1. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# default-router 192.168.2.1

e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# dns-server 192.168.2.9

f. Asigne un tiempo de arrendamiento de tres días. En el espacio proporcionado, escriba el comando que utilizó.

S1(dhcp-config)# lease 3

g. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 3. verificar la conectividad y DHCPv4.

a. 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: **192.168.2.11**

Máscara de subred: **255.255.255.0**

Gateway predeterminado: **192.168.2.1**

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? **SÍ**

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

¿Los pings eran correctos? ¿Por qué?

La razón por la cual no se puede hacer PING entre las dos PC es porque PC-B está en una red diferente; por lo tanto, el ping de la PC-A no es correcto.

c. Emita el comando **show ip route** en el S1.

¿Qué resultado arrojó este comando?

No se estableció un gateway predeterminado y no hay una tabla de routing presente en el switch.

Parte 5. 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? **SÍ**

¿Qué función realiza el switch?

El switch hace routing entre VLAN.

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?

El switch exhibe una tabla de routing que muestra las VLAN como las redes conectadas directamente 192.168.1.0/24 y 192.168.2.0/24.

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?

Se muestra las redes conectadas directamente a una de sus interfaces 192.168.1.0 y 209.165.200.224.

Observemos que no tenemos una ruta para 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?

Debemos tener rutas que permitan la unión de estas redes distantes.

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.

S1(config)# iproute 0.0.0.0 0.0.0.0 192.168.1.10

b. En el R1, cree una ruta estática a la VLAN 2. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1

c. Vea la información de la tabla de routing para el S1.

¿Cómo está representada la ruta estática predeterminada?

S* 0.0.0.0/0 [1/0] via 192.168.1.10

d. Vea la información de la tabla de routing para el R1.

¿Cómo está representada la ruta estática?

S 192.168.2.0/24 is directly connected, GigabitEthernet0/1

e. ¿Es posible hacer ping de la PC-A al R1? **SÍ**

¿Es posible hacer ping de la PC-A a la interfaz Lo0? **SÍ**

Reflexión

1. Al configurar DHCPv4, ¿por qué excluiría las direcciones estáticas antes de configurar el pool de DHCPv4?

   Si las direcciones estáticas se excluyeran después de la creación del pool de DHCPv4, existiría un lapso durante el cual las direcciones excluidas podrían pasarse dinámicamente a hosts, generando conflictos con las direcciones IP que ya están asignadas.

2. Si hay varios pools de DHCPv4 presentes, ¿cómo asigna el switch la información de IP a los hosts?

   Recordemos que cada uno de los puertos está asignado a determinado VLAN, esta es la forma de controlar el switch que dirección debe asignar y a que interfaz.

3. Además del switching, ¿qué funciones puede llevar a cabo el switch Cisco 2960?

   Este en un dispositivo real puede hacer la función de router, pero en el caso del simulador este ni puede hacer, por esto fue cambiado por otro tipo de switch que me permita realiza la práctica.

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

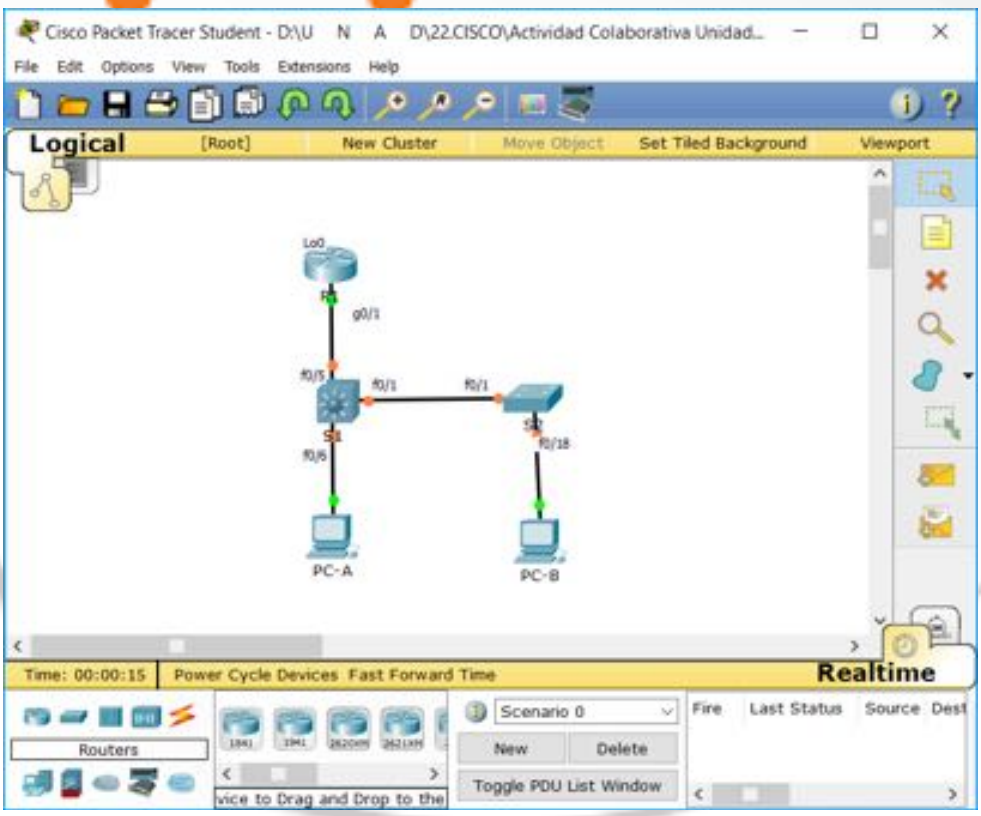
S1(config)# **interface f0/6**
S1(config-if)# **switchport access vlan 2**

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**

Captura de Evidencia



Informe 3

10.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6

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.

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 de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

Paso 10. realizar el cableado de red tal como se muestra en la topología.

Paso 11. inicializar y volver a cargar el router y el switch según sea necesario.

Paso 12. 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.

Paso 13. 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.

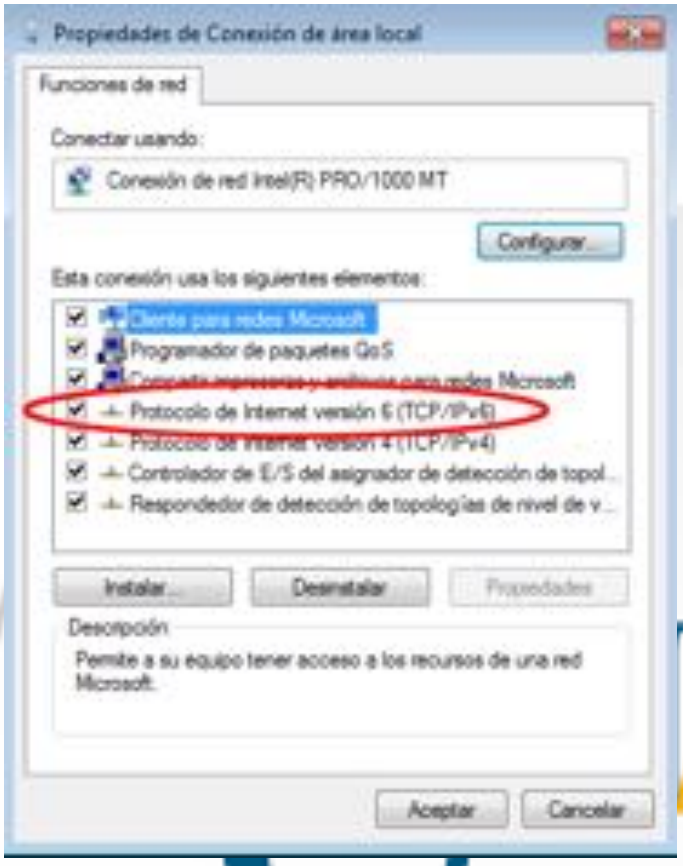
h. Desactive administrativamente todas las interfaces inactivas.

i. Guarde la configuración en ejecución en la configuración de inicio.

Parte 2. configurar la red para SLAAC

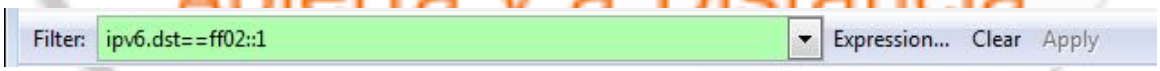
Paso 1. preparar la PC-A.

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.



Paso 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.

Paso 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 unreachables 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.
```

Paso 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
```

Paso 5. verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

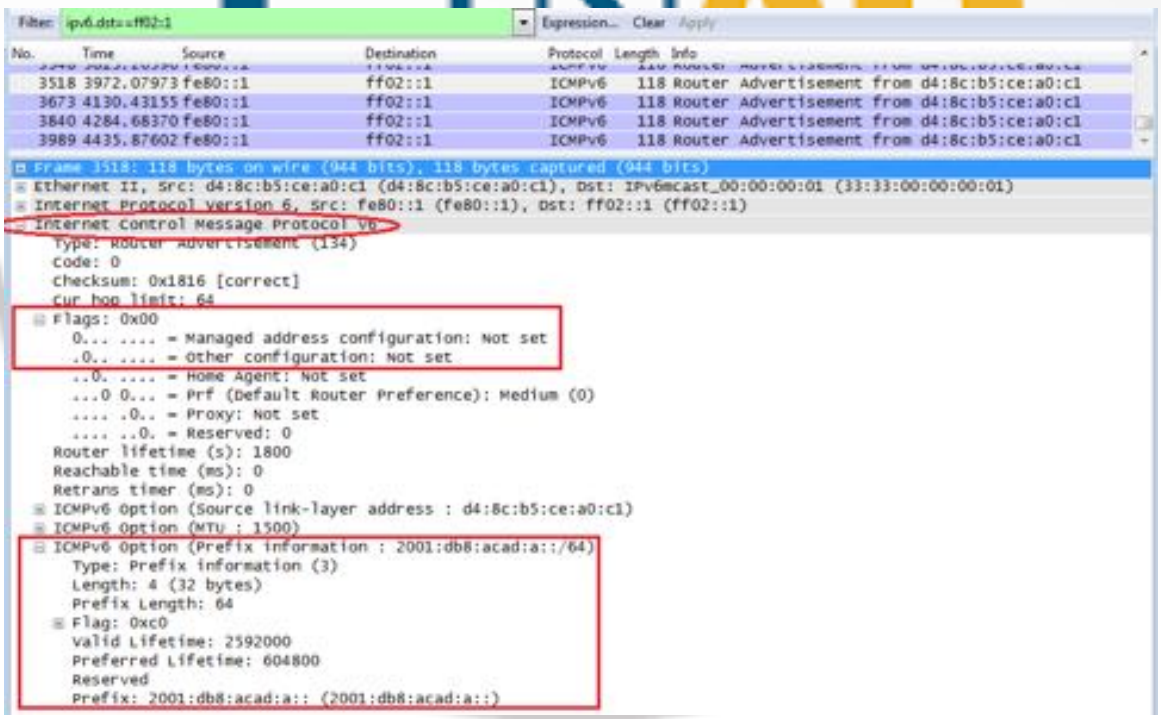
Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

```
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 unreachables 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
```

Paso 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.

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.



Parte 3. *configurar la red para DHCPv6 sin estado*

Paso 1. configurar un servidor de DHCP IPv6 en el R1.

a. Cree un pool de DHCP IPv6.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**

b. Asigne un nombre de dominio al pool.

R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**

c. Asigne una dirección de servidor DNS.

R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**
R1(config-dhcpv6)# **exit**

d. Asigne el pool de DHCPv6 a la interfaz.

R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

e. Establezca la detección de redes (ND) DHCPv6 **other-config-flag**.

R1(config-if)# **ipv6 nd other-config-flag**
R1(config-if)# **end**

Paso 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

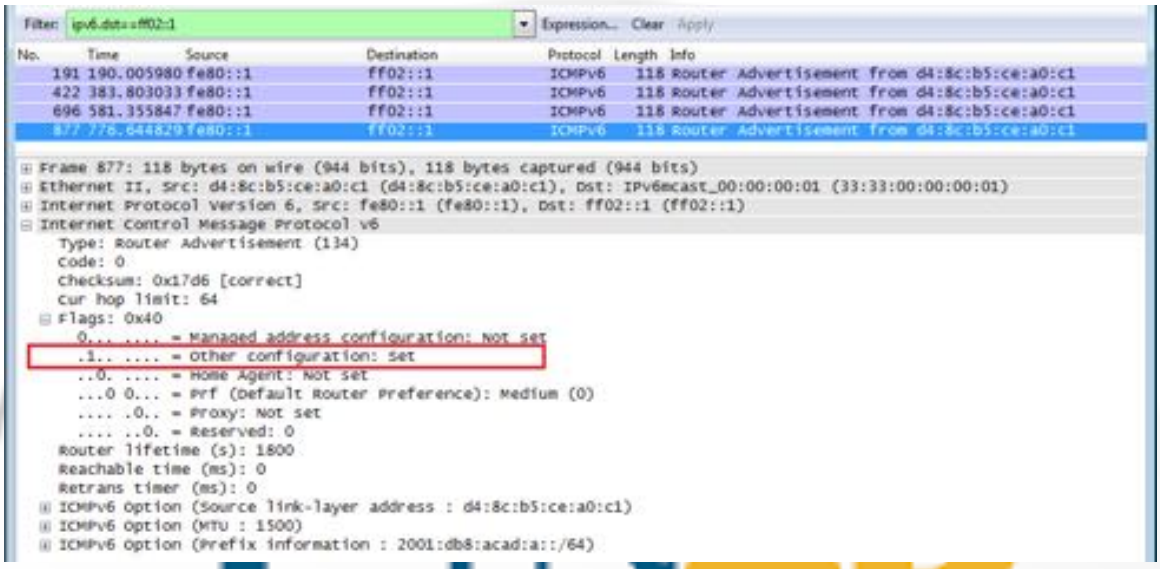
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
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.

Paso 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.

Paso 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.



Paso 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

Paso 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.

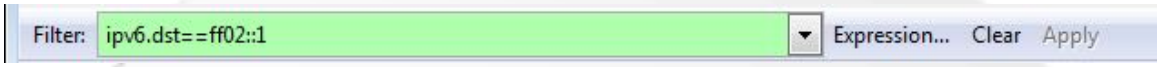
   2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

Parte 4. *configurar la red para DHCPv6 con estado*

Paso 1. preparar la PC-A.

a. Inicie una captura del tráfico en la NIC con Wireshark.

b. 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.



Paso 2. cambiar el pool de DHCPv6 en el R1.

a. Agregue el prefijo de red al pool.

R1(config)# **ipv6 dhcp pool IPV6POOL-A**
R1(config-dhcpv6)# **address prefix 2001:db8:acad:a::/64**

b. 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**

c. 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

d. 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)

Paso 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**

Paso 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**

Paso 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 unreachables 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

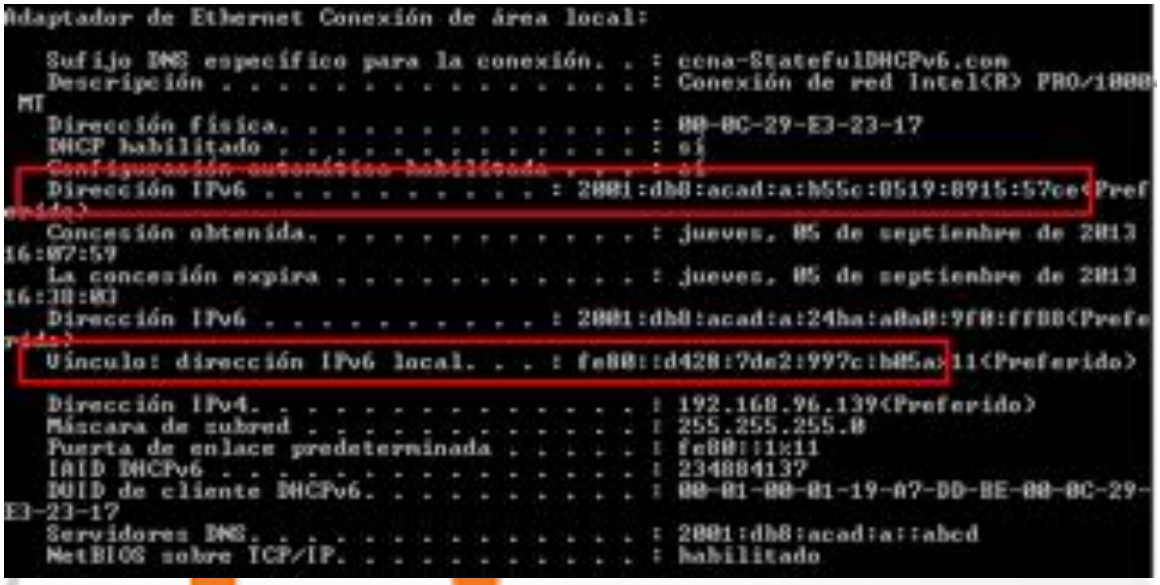
Username : unassigned

IA NA: IA ID 0x0E000C29, 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)



e. Emita el comando **undebug 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 **undebug 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

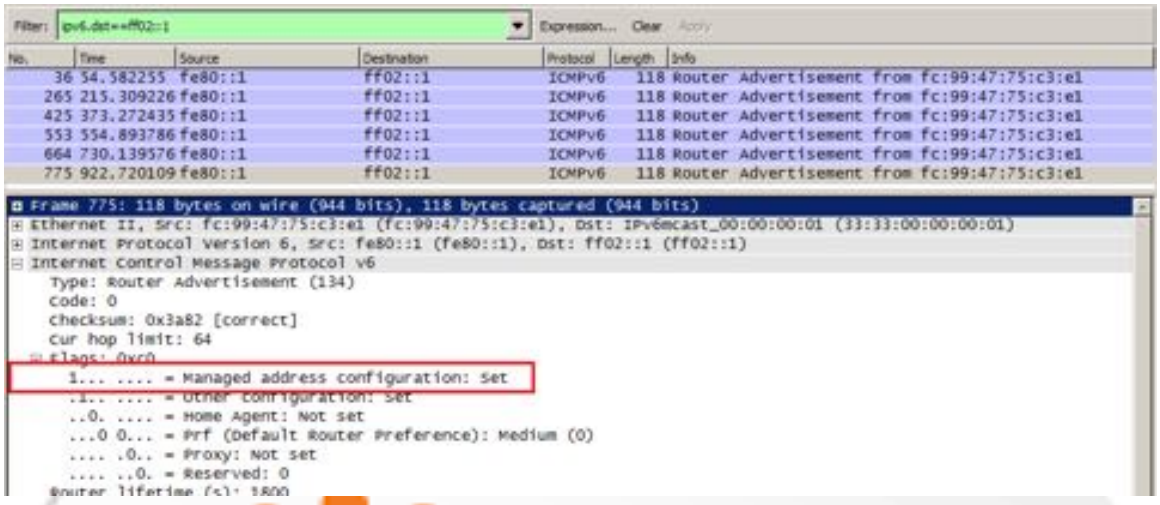
2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

*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

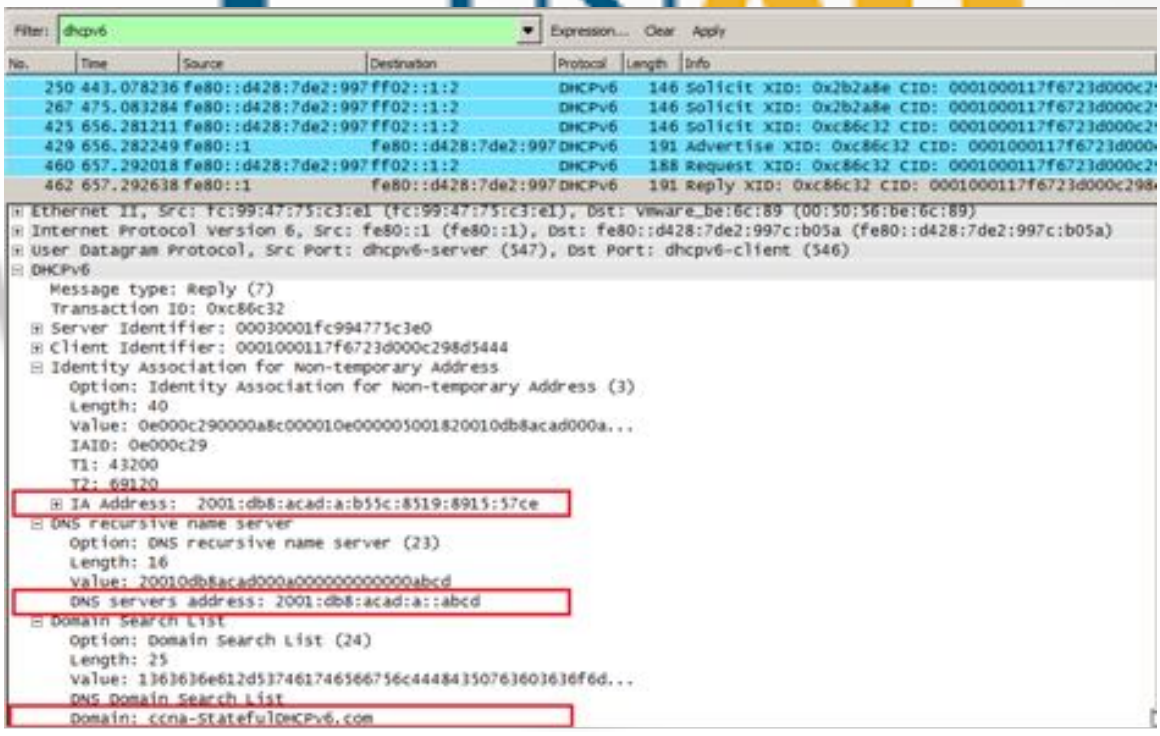
Paso 6. verificar DHCPv6 con estado en la PC-A.

a. Detenga la captura de Wireshark en la PC-A.

b. 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).



c. 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.



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?

   El protocolo DHCP permite configurar automáticamente los host de una red TCP/IP durante el arranque de los sistemas. DHCP utiliza un mecanismo de cliente-servidor, a la vez los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan. DHCPv6 requiere el router para almacenar la información de estado dinámica sobre los clientes DHCPv6, este método de direccionamiento con estado utiliza más recursos de memoria en el router que el método sin estado.

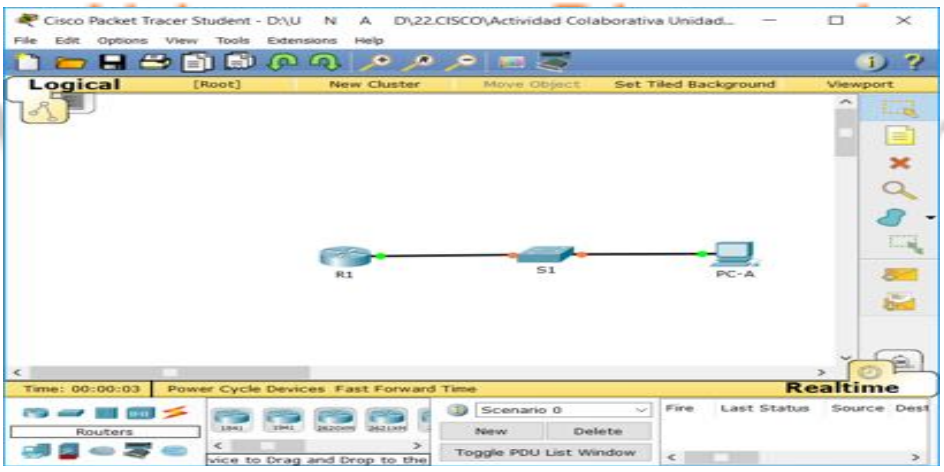
2. ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

   Se recomienda que los dispositivos ipv6 realicen detección de direcciones duplicadas en cualquier dirección, en la configuración automática de direcciones sin estado se utiliza para configurar las direcciones locales de vínculos y las direcciones no locales de vínculos adicionales mediante el intercambio de mensajes de solicitación de enrutador y anuncio de enrutador con los enrutadores vecinos.

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.				

Captura de evidencia



Informe 4

Laboratorio 10.3.1.1 IoE and DHCP Instructions

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.
- 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?

   Depende de muchos factores, por ejemplo si se tenía guardado un Router 1941 en desuso y se quería poner a trabajar, tan obvio que se pasa por alto. Puede ser también que el usuario desee mayor potencia, velocidad de procesamiento o seguridad para eso el Router es mejor, cuesta un poco más que un ISR pero a resumidas cuentas y a largo plazo el Router es mejor.

2. ¿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.

   - *Una empresa de Electrodomésticos puede vincular sus dispositivos inteligentes al servidor DHCP de la empresa para poder hacer reconocimiento y diagnóstico de los dispositivos en caso de daño o error.*

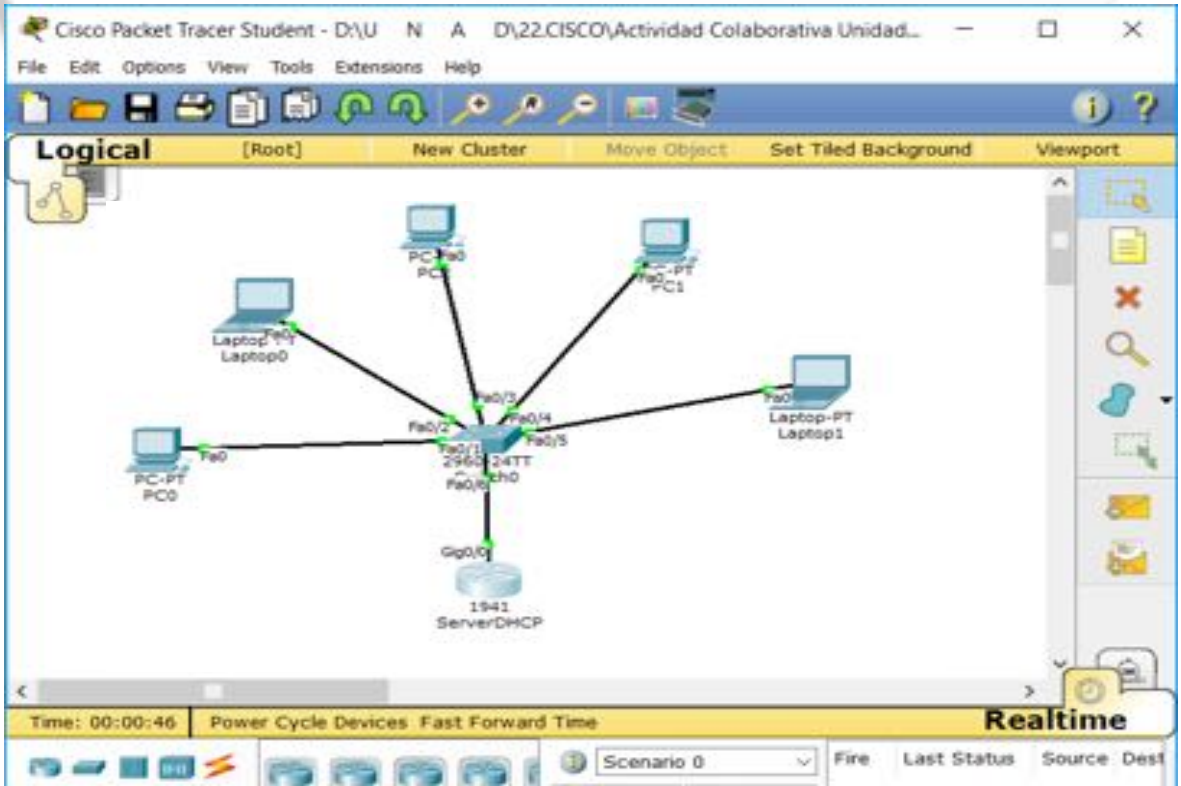
   - *Una empresa puede ofrecer direcciones asignadas por dhcp para que un cliente pueda manejar desde donde quiera su cocina, y poner a calentar la comida que dejo en el microondas, o encender el lavavajillas, o verificar que falta en la nevera.*

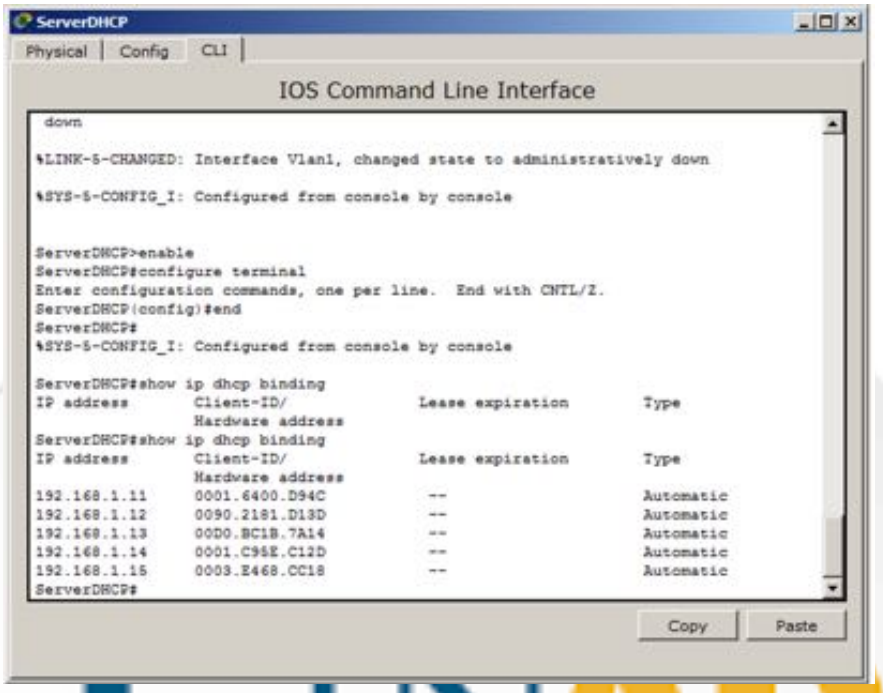
   - *De la misma forma Usando un DNS personal y un servidor DHCP se puede controlar en Centro de Entretenimiento para que grabe una película que están pasando en un canal, o ponga a descargar al disco duro un torrent para verlo al llegar a casa.*

   - *Una empresa de Automóviles puede vincular los vehículos directamente a un servidor DHCP de la empresa, Para hacer seguimiento del estado del vehículo y que informe en caso de algún daño.*

   - *Una empresa ofrece servicios de Seguridad por medio de cámaras, sensores de movimiento etc, este puede vincular los dispositivos al dhcp de la empresa para asignar las direcciones y poder controlar las cámaras o sensores y conocer el estado de los mismos.*

El Modelo Propuesto es el Siguiente:





Informe 5

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
	Lo0	192.31.7.1	255.255.255.255	N/A
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

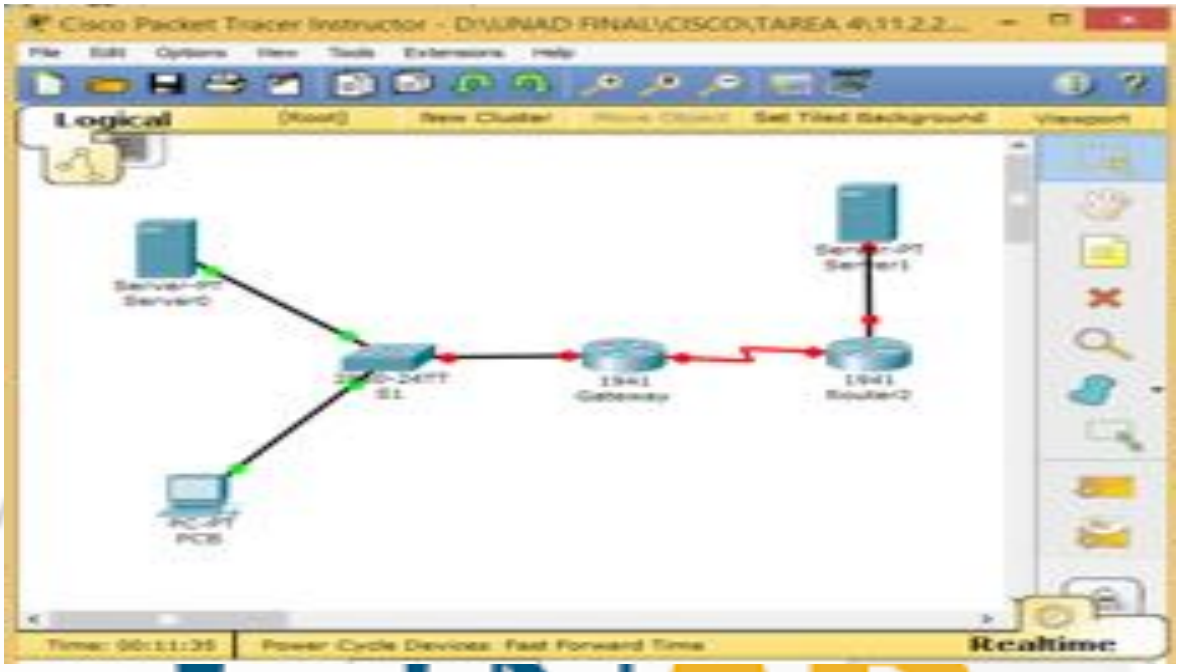
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

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.

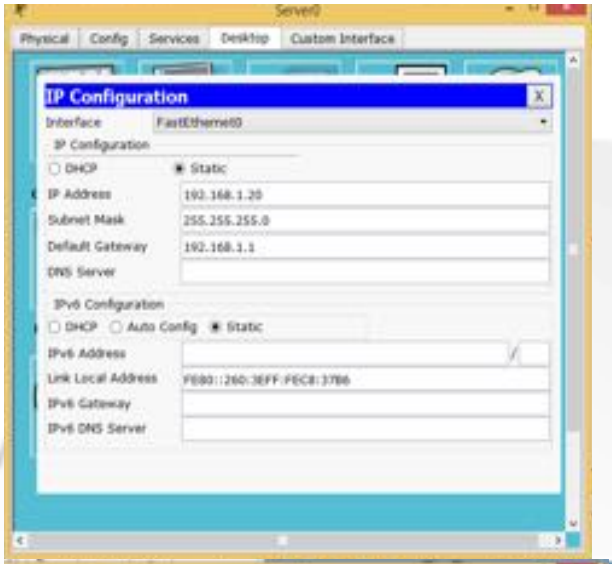
Paso 7. Realizar el cableado de red tal como se muestra en la topología.

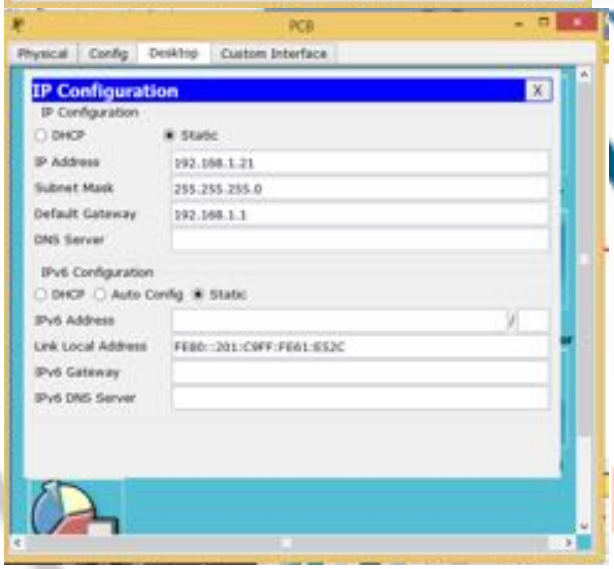
Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.



Universidad Nacional
Abierta y a Distancia

Paso 8. **configurar los equipos host.**





Paso 9. **Inicializar y volver a cargar los routers y los switches según sea necesario.**

Paso 10. **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 interrumpan la entrada del comando.

Paso 11. 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**

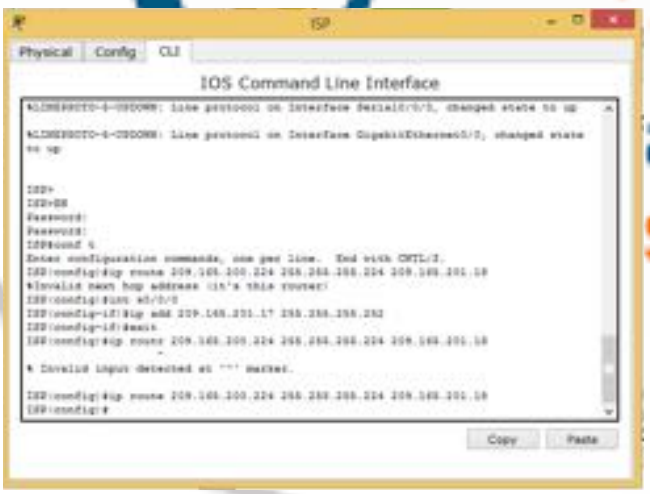
c. Configure el servicio HTTP para utilizar la base de datos local.

ISP(config)# **ip http authentication local**

Paso 12. 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**



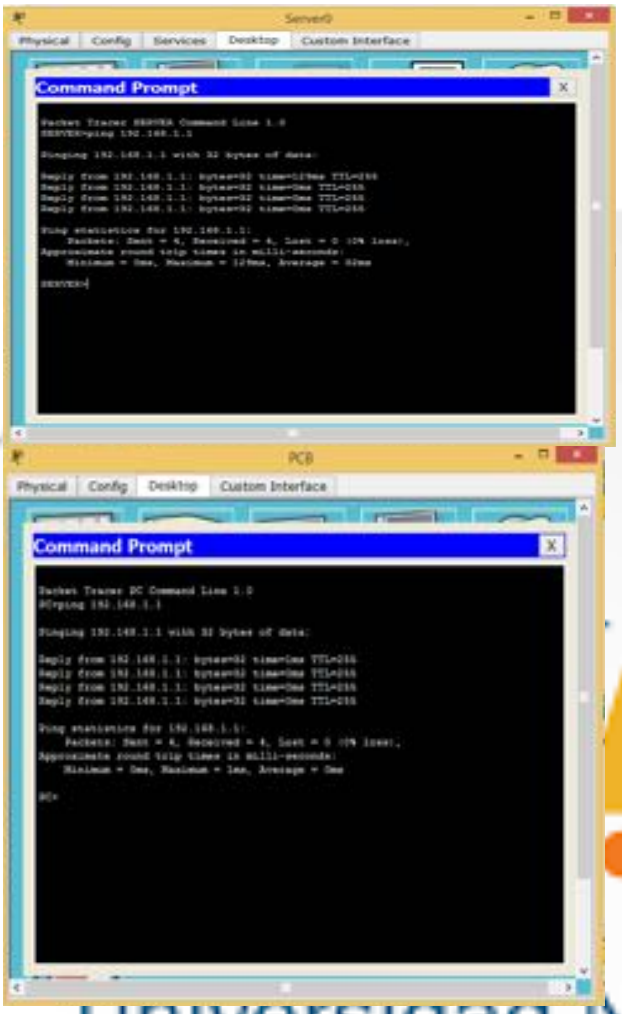
b. Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

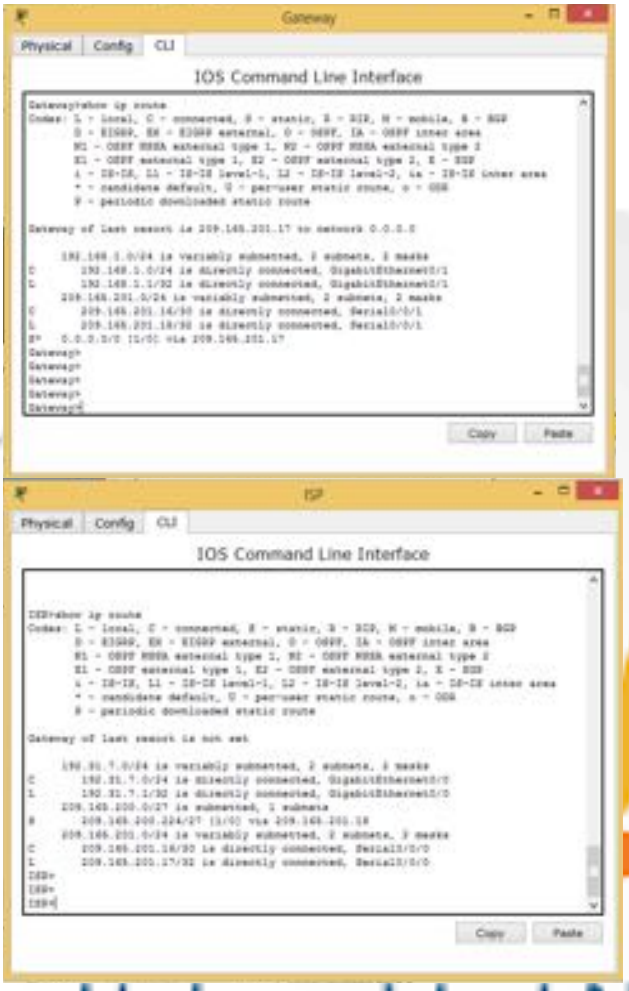
Paso 13. **Guardar la configuración en ejecución en la configuración de inicio.**

Paso 14. **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.



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.



Parte 5. 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.

Paso 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**

Paso 2. **<u>Especifique las interfaces.</u>**

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 3. Probar la configuración.

a. 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	---	---

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = 209.165.200.225

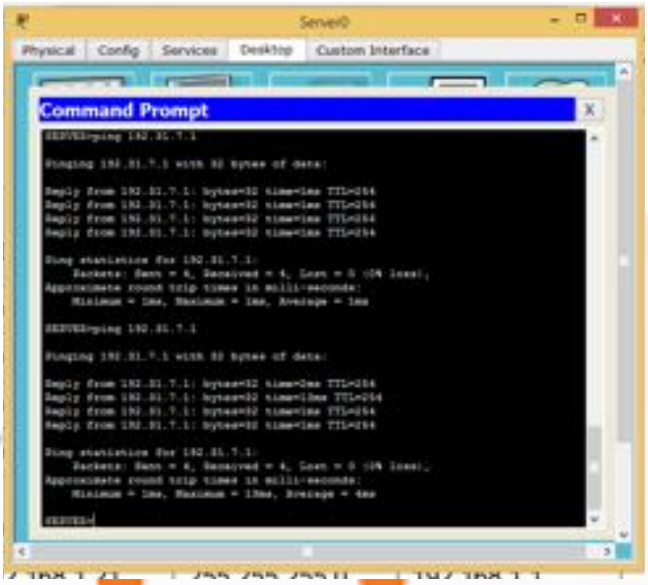
¿Quién asigna la dirección global interna?

Asignada por el Router que asigna el proveedor de internet

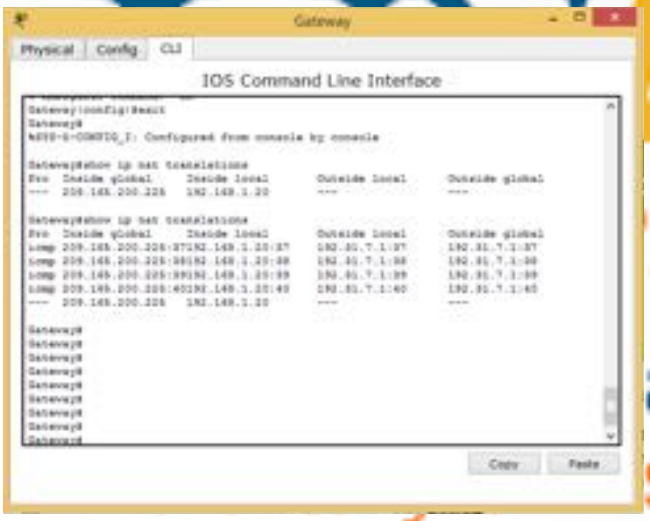
¿Quién asigna la dirección local interna?

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.



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 --- ---

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? _37_____

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 --- ---

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?

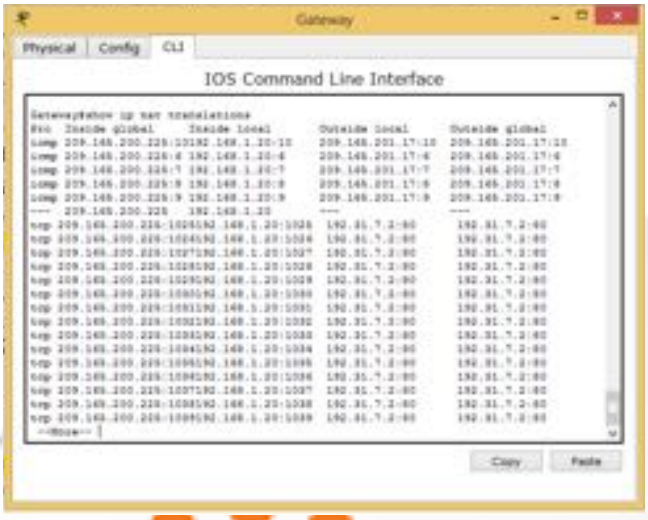
Global/local interno: _____1025/1025_____

Global/local externo: _____80/80_____

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.

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

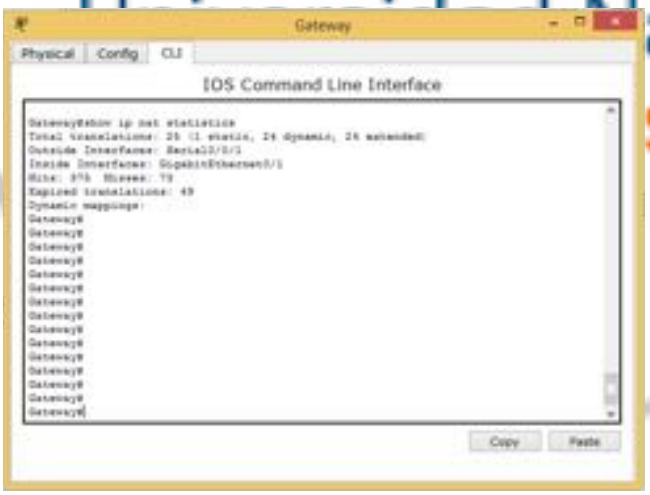
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12

--- 209.165.200.225 192.168.1.20 --- ---

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 statics**



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

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Parte 6. 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.

Paso 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**

Paso 2. **<u>Definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN.</u>**

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 3. **<u>Vverificar que la configuración de interfaces NAT siga siendo válida.</u>**

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

Paso 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**

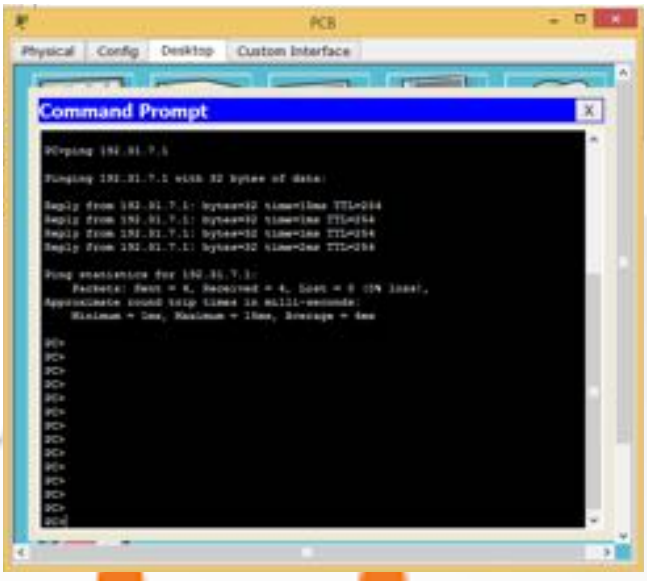
Paso 5. **Definir la NAT desde la lista de origen interna hasta el conjunto externo.**

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**

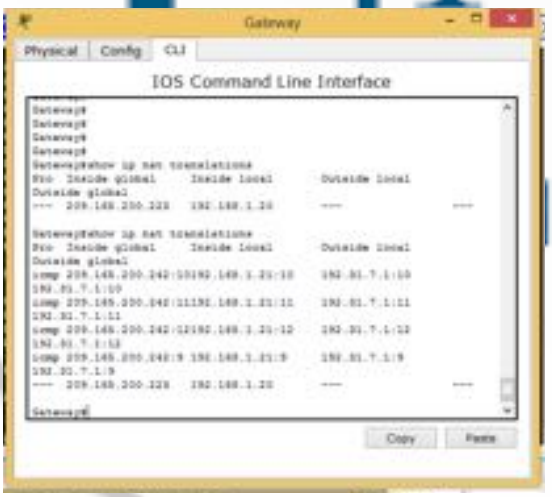
Paso 6. **Probar la configuración.**

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.



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	---	---



¿Cuál es la traducción de la dirección host local interna de la PC-B?

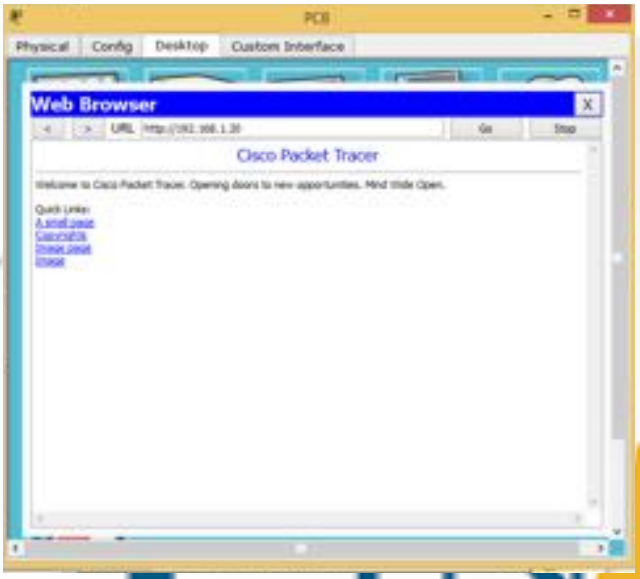
192.168.1.21 = ___ 209.165.200.242

_____

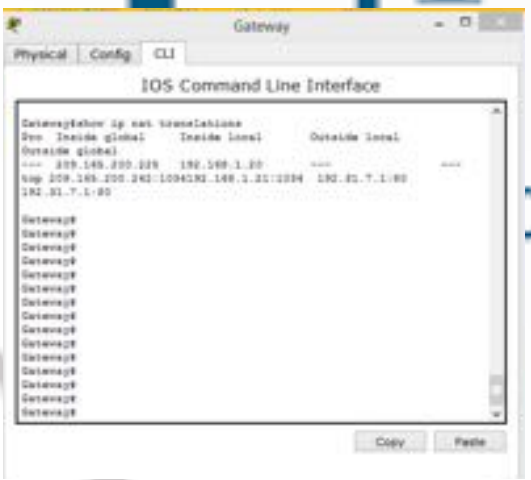
Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? _____10_____

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**.



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 --- ---

¿Qué protocolo se usó en esta traducción? ____http_____

¿Qué números de puerto se usaron?

Interno: _____1034_____

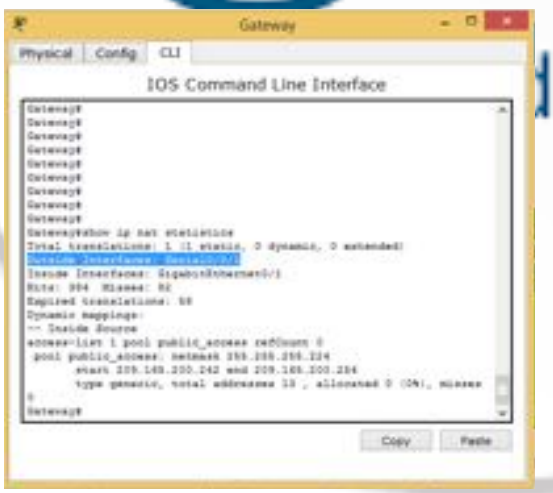
Externo: _____80_____

¿Qué número de puerto bien conocido y qué servicio se usaron?

_____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

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Paso 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.

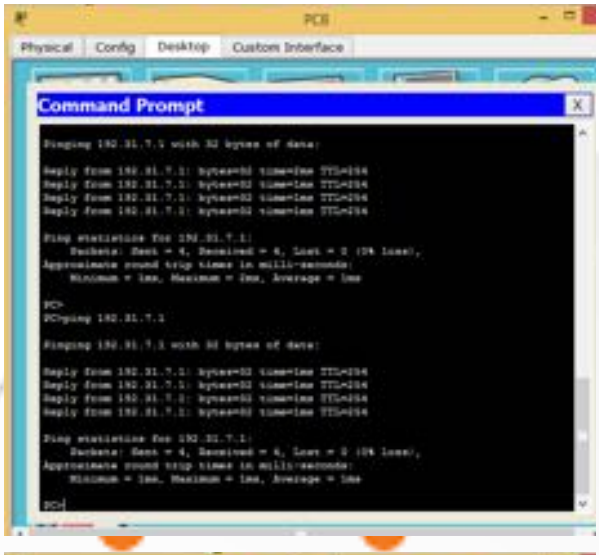
a. Elimine la NAT estática de la parte 2. Introduzca yes (sí) cuando se le solicite eliminar entradas secundarias.

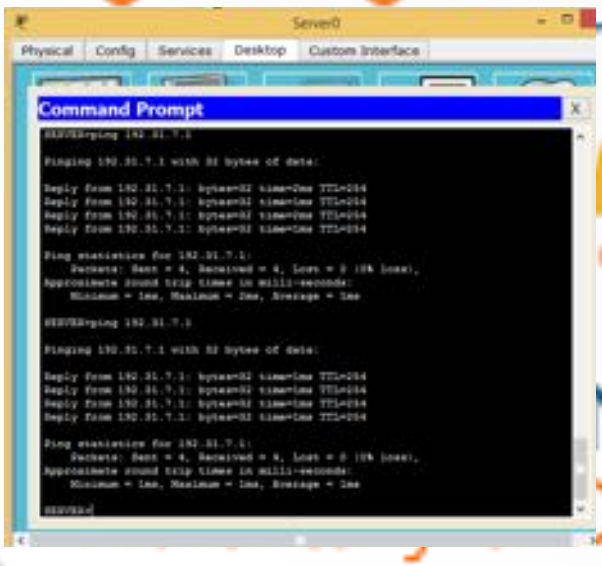
Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

b. Borre las NAT y las estadísticas.

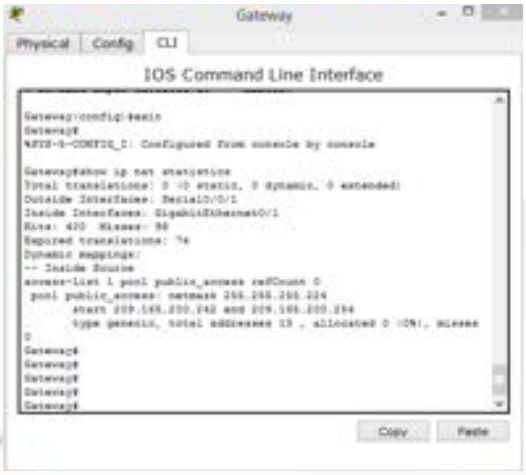
c. Haga ping al ISP (192.31.7.1) desde ambos hosts.





d. 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 --- ---

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?

   Por qué utilizando nat se ahorran ip versión 4 y algo muy importante la seguridad puesto que las ip de los equipos no se muestran

2. ¿Cuáles son las limitaciones de NAT?

   Demora un poco y ciertos servicios no pueden salir a internet

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.

Informe 6

Práctica de laboratorio: configuración de un conjunto de NAT con sobrecarga y PAT

Topología

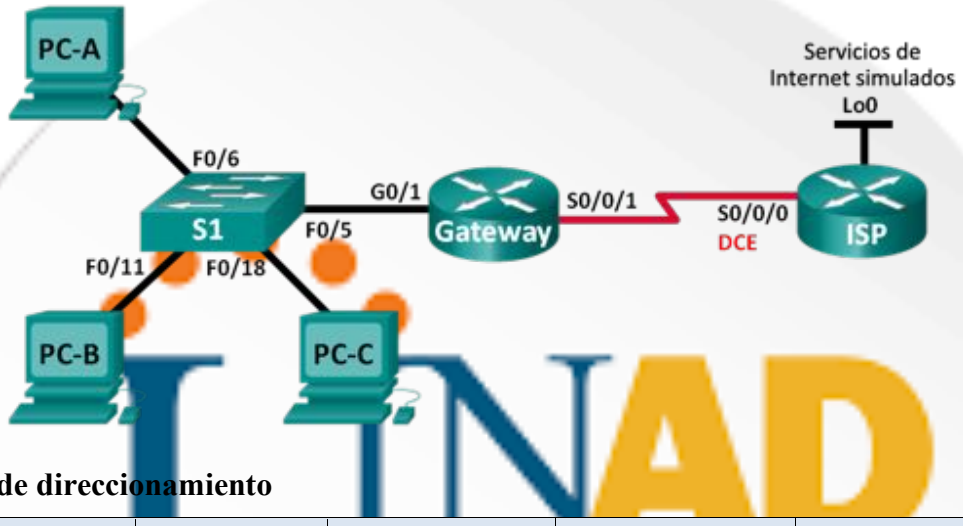


Tabla de direccionamiento

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

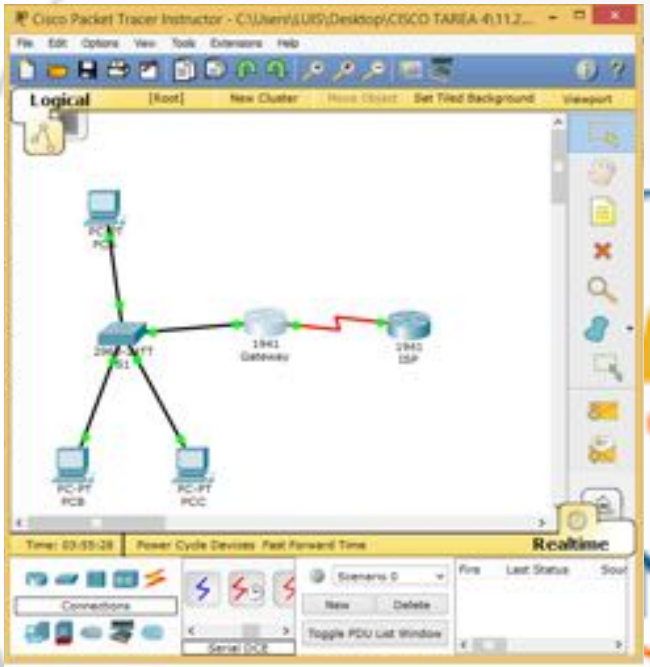
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

- 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.

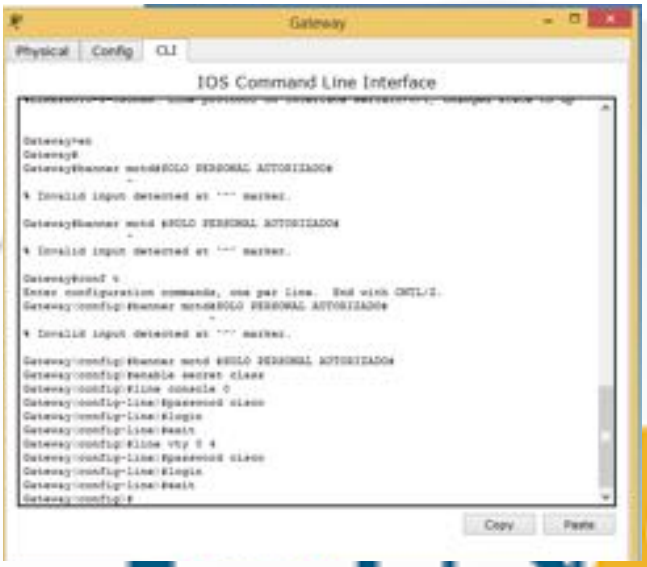
Paso 11. Configurar los parámetros básicos para cada router.

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 **128000** para la interfaz serial 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.

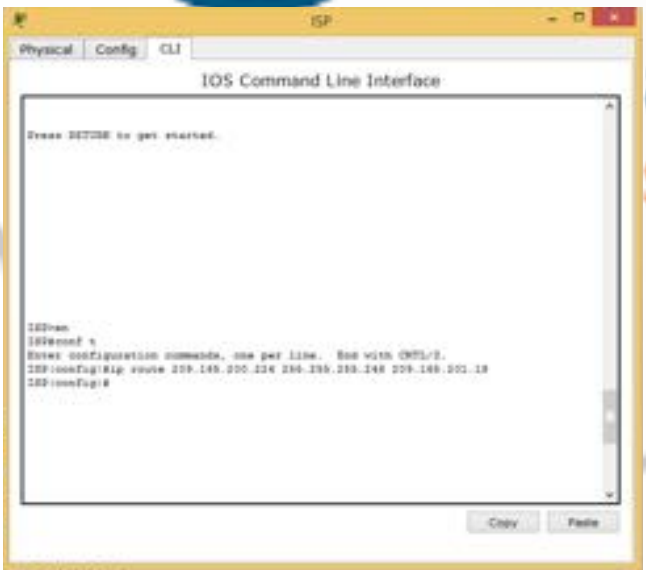
g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.



Paso 12. <u>Configurar el routing estático</u>.

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**

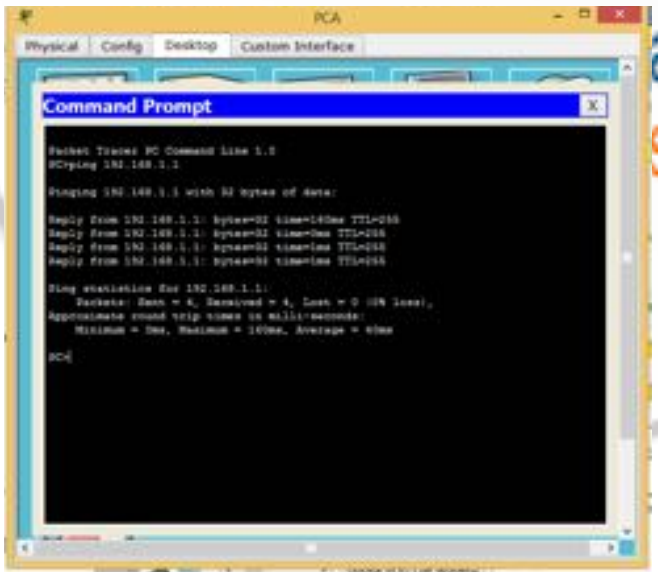


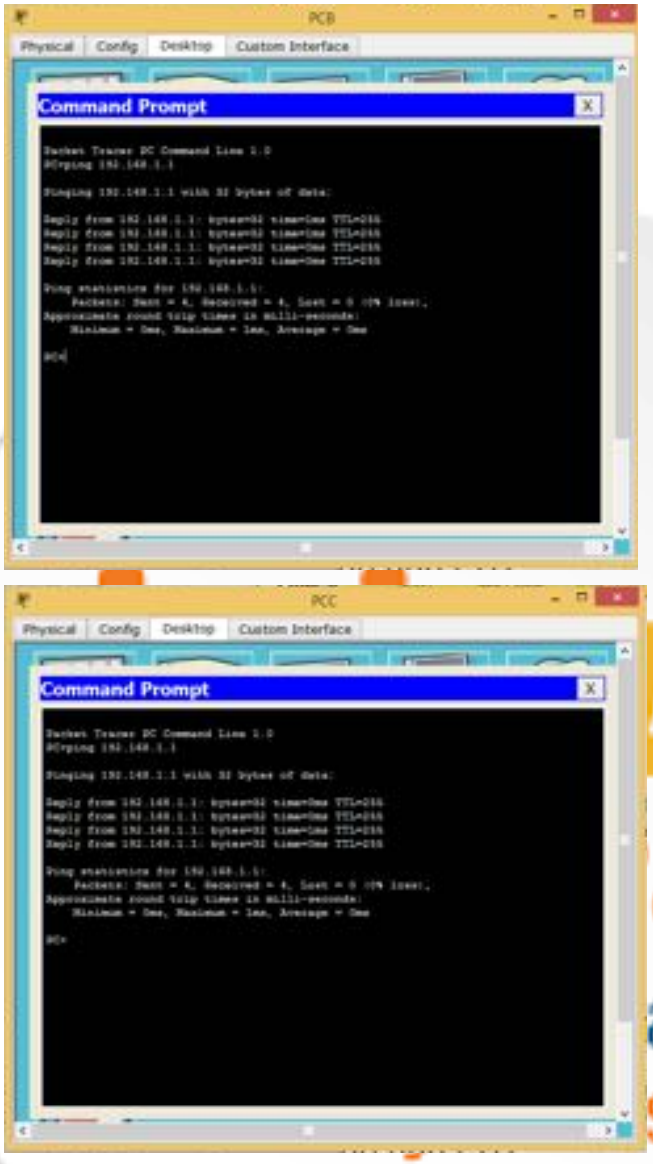
b. Cree una ruta predeterminada del router Gateway al router ISP.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

Paso 13. <u>Verificar la conectividad de la red</u>

a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.





b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.

Parte 7. *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 1. 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.

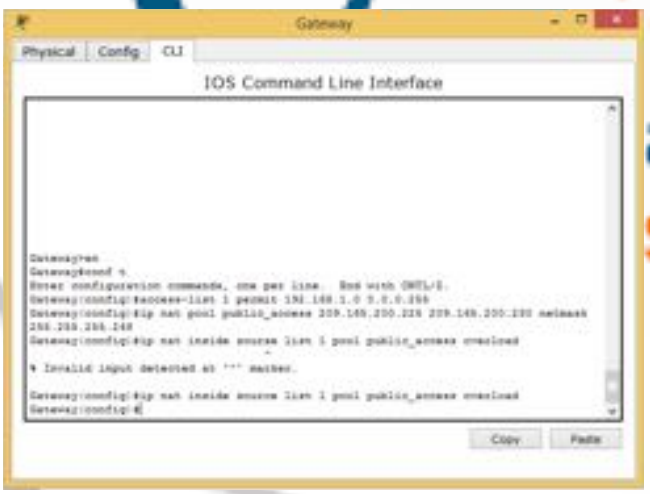
Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

Paso 2. **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 3. **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**



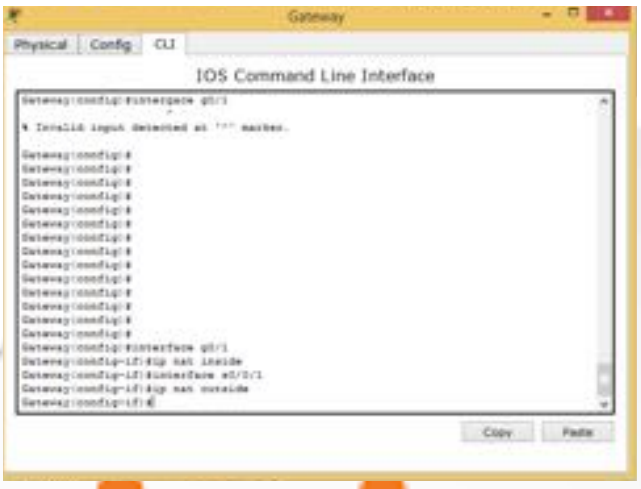
Paso 4. **Especifique las interfaces.**

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

Gateway(config)# **interface g0/1**

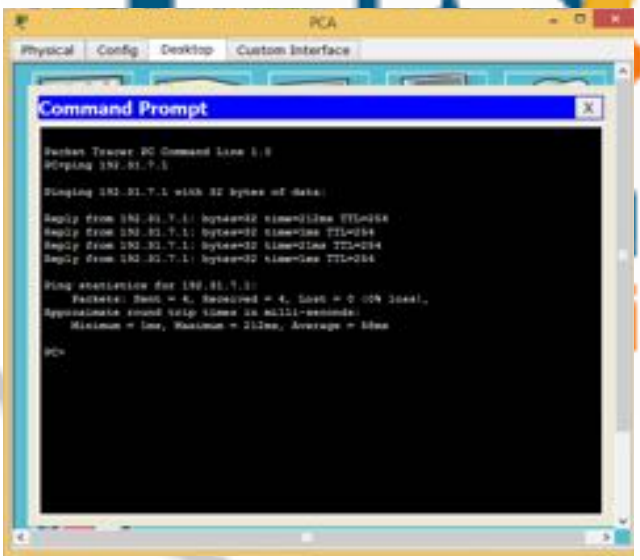
Gateway(config-if)# **ip nat inside**

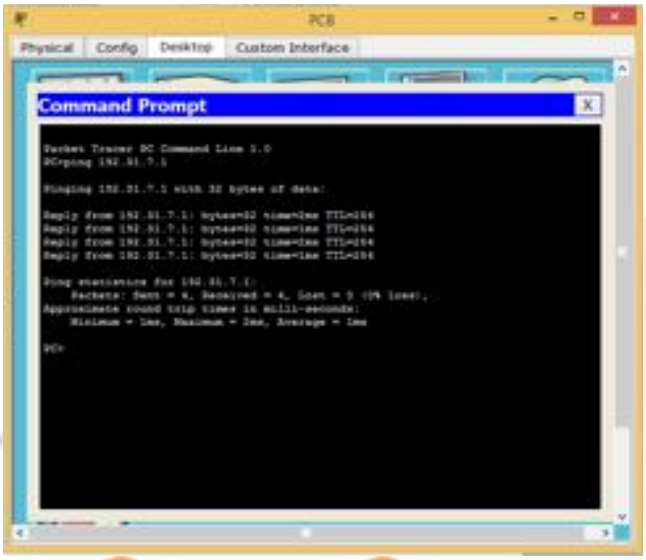
Gateway(config-if)# **interface s0/0/1**
Gateway(config-if)# **ip nat outside**

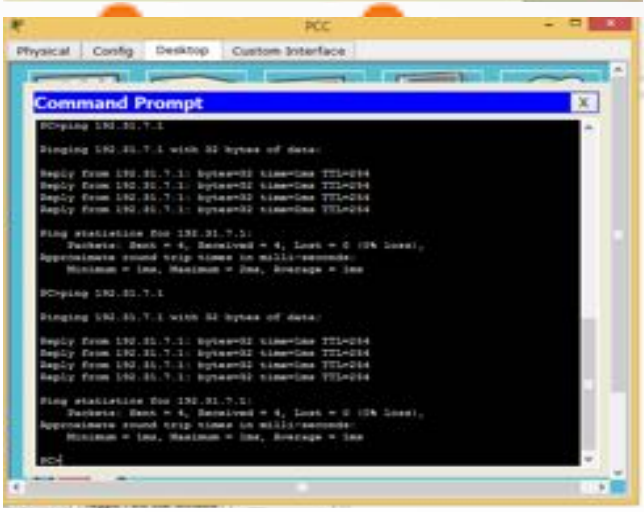


Paso 5. **<u>Verificar la configuración del conjunto de NAT con sobrecarga.</u>**

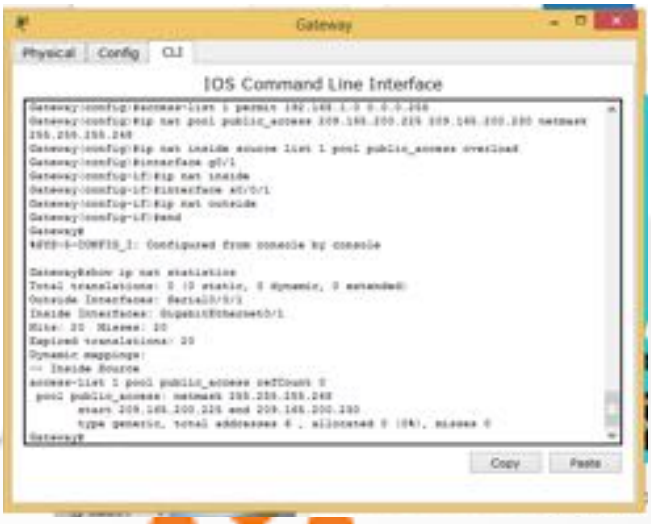
a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.







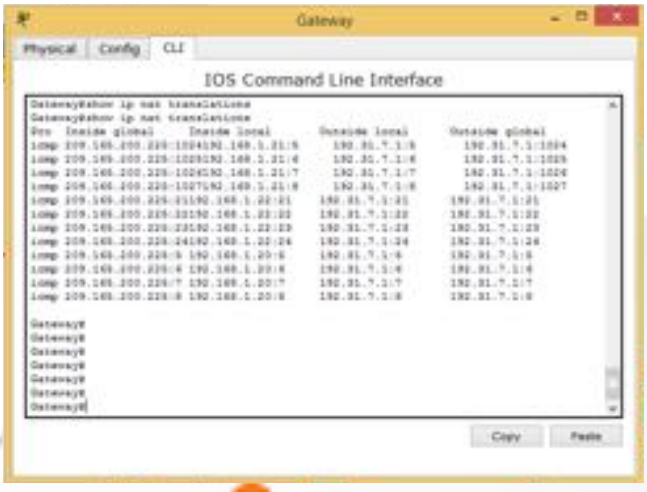
b. Muestre las estadísticas de NAT en el router Gateway.



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

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***

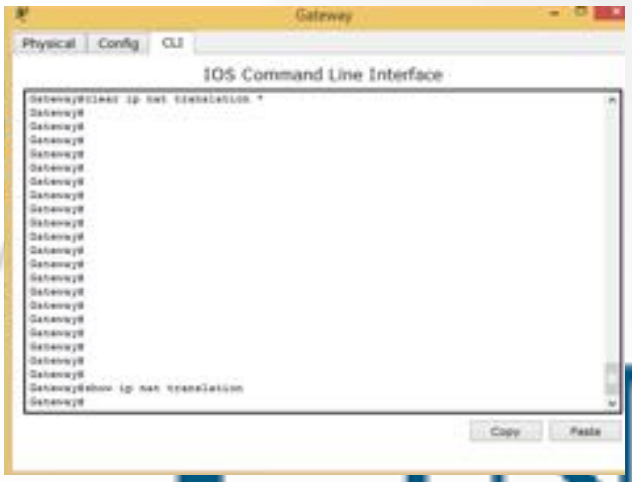
¿Cuál sería el resultado de hacer ping del router ISP a la dirección local interna de la PC-A? ¿Por qué?

El ping falla porque las computadoras no muestran su dirección ip por el nat. el ISP solo se puede comunicar con el Gateway

Parte 8. 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 1. Borrar las NAT y las estadísticas en el router Gateway.



Paso 2. Verificar la configuración para NAT.

a. Verifique que se hayan borrado las estadísticas.

b. Verifique que las interfaces externa e interna estén configuradas para NAT.

c. 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

Paso 3. Eliminar el conjunto de direcciones IP públicas utilizables.

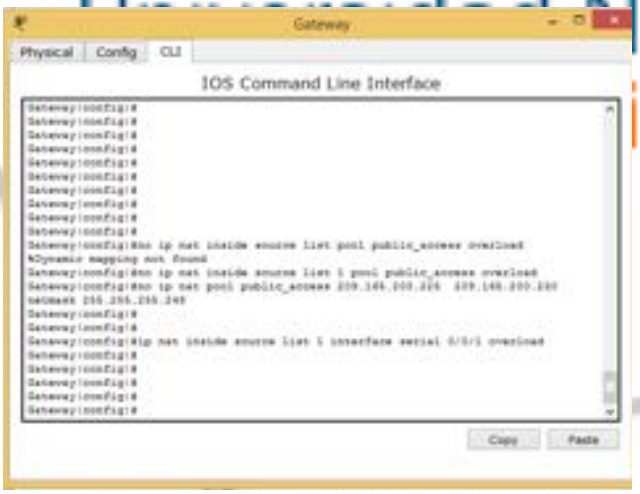
Gateway(config)# **no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

Paso 4. 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**

Paso 5. Asociar la lista de origen a la interfaz externa.

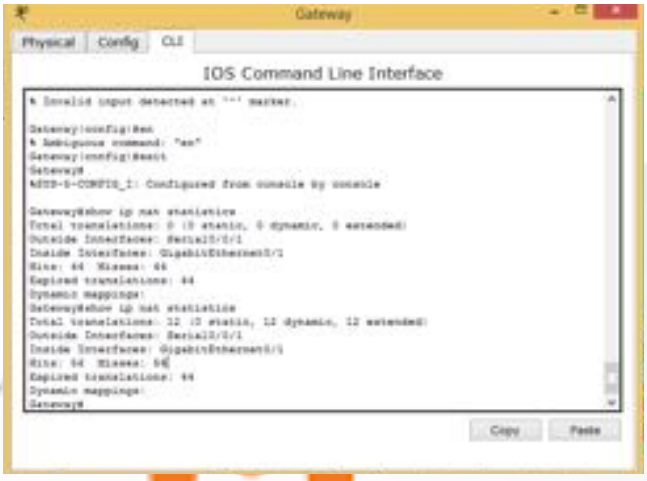
Gateway(config)# **ip nat inside source list 1 interface serial 0/0/1 overload**



Paso 6. Probar la configuración PAT.

a. Desde cada computadora, haga ping a la dirección 192.31.7.1 del router ISP.

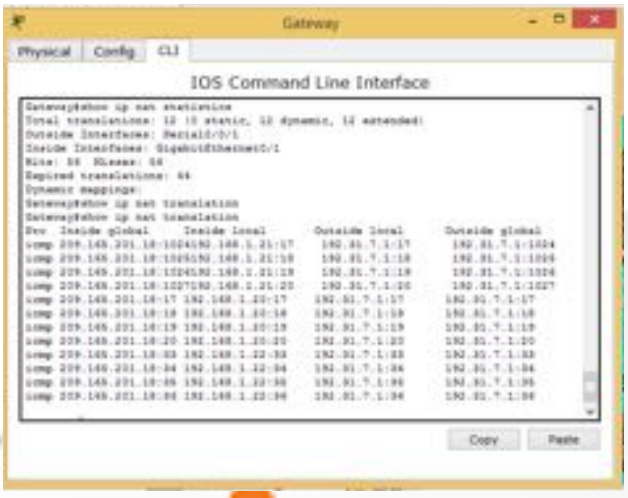
b. Muestre las estadísticas de NAT en el router Gateway.



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

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

Reflexión

¿Qué ventajas tiene la PAT?

Las respuestas varían, pero deben incluir que PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet y que los servicios de PAT, como los de NAT, sirven para "ocultar" las direcciones privadas de las redes externas. Solo utiliza una ip pública ahorrando las ip públicas utilizando puertos diferentes para identificar cada paquete

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)

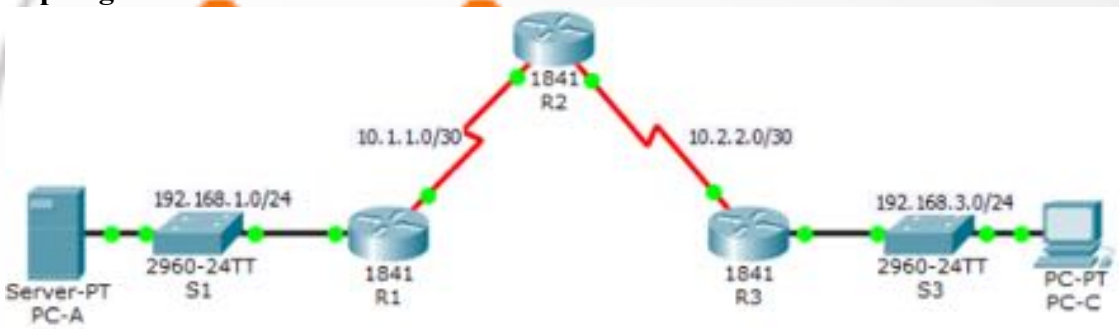
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores 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.

Informe 7

Laboratorio: 4.4.1.2. Configure IP ACLs to Mitigate Attacks.

Topología de la guía:

Topología del laboratorio:



Addressing Table: (Tabla de direccionamiento):

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: (Objetivos):

Verify connectivity among devices before firewall configuration. Verificar la conectividad entre los dispositivos antes de la configuración del firewall).

Use ACLs to ensure remote access to the routers is available only from management station PC-C. Utilice las ACL para asegurarse de que el acceso remoto a los enrutadores sólo está disponible en la estación de administración PC-C.

Configure ACLs on R1 and R3 to mitigate attacks. Configurar ACLs en R1 y R3 para mitigar los ataques).

Verify ACL functionality. (Verificar la funcionalidad de ACL).

Background / Scenario: Escenario:

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. (El acceso a los routers R1, R2 y R3 sólo se debe permitir desde PC-C, la estación de gestión. PC-C también se utiliza para pruebas de conectividad a PC-A, un servidor que proporciona servicios DNS, SMTP, FTP y HTTPS).

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. (El procedimiento operativo estándar consiste en aplicar ACLs en los routers de borde para mitigar las amenazas comunes basadas en la dirección IP de origen y / o destino. En esta actividad, se crean ACLs en los enrutadores de borde R1 y R3 para lograr este objetivo. A continuación, verifique la funcionalidad ACL de los hosts internos y externos).

The routers have been pre-configured with the following: (Los routers han sido preconfigurados con lo siguiente):

Enable password: **ciscoenpa55**

Password for console: **ciscoconpa55**

Username for VTY lines: **SSHadmin**

Password for VTY lines: **ciscosshpa55**

IP addressing

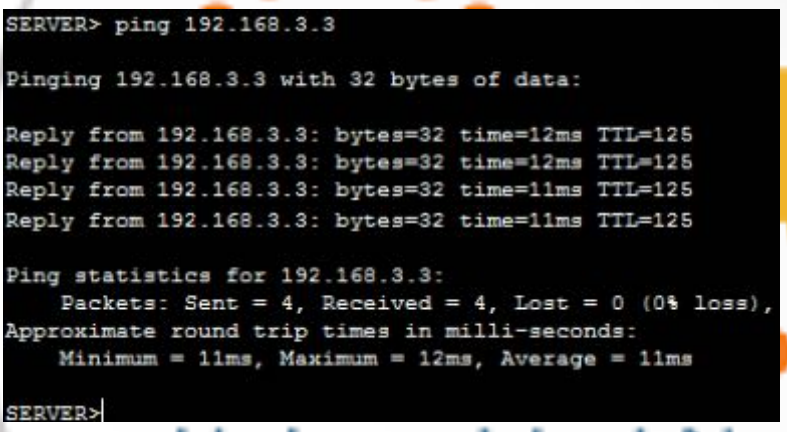
Static routing

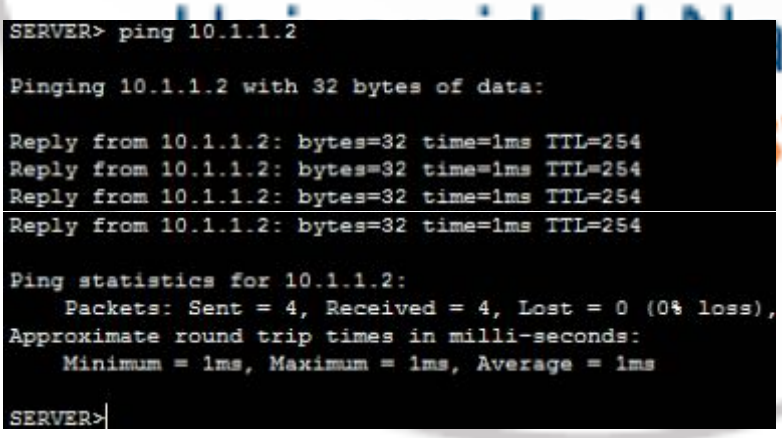
Parte 1. Verify Basic Network Connectivity. (Verificar la conectividad de red básica).

Verify network connectivity prior to configuring the IP ACLs. (Compruebe la conectividad de red antes de configurar las ACL de IP).

Step 1: From PC-A, verify connectivity to PC-C and R2. (Desde PC-A, verifique la conectividad con PC-C y R2).

a. From the command prompt, ping PC-C (192.168.3.3). (En el símbolo del sistema, haga ping a PC-C (192.168.3.3).





b. From the command prompt, establish a SSH session to R2Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. When finished, exit the SSH session. (En el símbolo del sistema, establezca una sesión SSH en la interfaz

R2 Lo0 (192.168.2.1) utilizando el nombre de usuario SSHadmin y la contraseña ciscosshpa55. Cuando haya terminado, salga de la sesión SSH).

PC> **ssh -l SSHadmin 192.168.2.1**

```
Packet Tracer PC Command Line 1.0
PC> ssh -l SSHadmin 192.168.2.1
Open
Password:



R2#
```

Step 2: From PC-C, verify connectivity to PC-A and R2. (Desde PC-C, verifique la conectividad a PC-A y R2).

a. From the command prompt, ping PC-A (192.168.1.3). (En el símbolo del sistema, haga ping PC-A (192.168.1.3).

```
PC> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=12ms TTL=125
Reply from 192.168.1.3: bytes=32 time=10ms TTL=125
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms

PC>
```

b. From the command prompt, establish a SSH session to R2 Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. Close the SSH session when finished. (En el símbolo del sistema, establezca una sesión SSH en la interfaz R2 Lo0 (192.168.2.1) utilizando el nombre de usuario SSHadmin y la contraseña ciscosshpa55. Cierre la sesión SSH cuando termine).

```
PC> ssh -l SSHadmin 192.168.2.1
Open
Password:
```

```
R2# exit

[Connection to 192.168.2.1 closed by foreign host]
PC>
```

c. Open a web browser to the PC-A server (192.168.1.3) to display the web page. Close the browser when done. (Abra un navegador web al servidor PC-A (192.168.1.3) para mostrar la página web. Cierre el navegador cuando haya terminado).

Parte 2. Secure Access to Routers. (Acceso seguro a los routers).

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C. (Configure ACL 10 para bloquear todo el acceso remoto a los enrutadores, excepto de PC-C).

Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**. (Utilice el comando access-list para crear una ACL IP numerada en R1, R2 y R3).

- **R1:**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 10 permit 192.168.3.3
R1(config)#
```

- **R2:**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# access-list 10 permit 192.168.3.3
R2(config)#
```

- **R3:**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# access-list 10 permit 192.168.3.3
R3(config)#
```

Step 2: Apply ACL 10 to ingress traffic on the VTY lines. (Aplique ACL 10 al tráfico de entrada en las líneas VTY).

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines. (Utilice el comando access-class para aplicar la lista de acceso al tráfico entrante en las líneas VTY).

R1:

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# line vty 0 4
R1(config-line)# access-class 10 in
R1(config-line)#exit
R1(config)#
```

- **R2:**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# line vty 0 4
R2(config-line)# access-class 10 in
R2(config-line)# exit
R2(config)#
```

- **R3:**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# line vty 0 4
R3(config-line)# access-class 10 in
R3(config-line)# exit
R3(config)#
```


Step 3: Verify exclusive access from management station PC-C. (Verificar el acceso exclusivo desde la estación de administración PC-C).

a. Establish a SSH session to 192.168.2.1 from PC-C (should be successful). (Establecer una sesión SSH a 192.168.2.1 desde PC-C (debería tener éxito).

```
PC> ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

[Connection to 192.168.2.1 closed by foreign host]
PC>
```

b. Establish a SSH session to 192.168.2.1 from PC-A (should fail). (Establecer una sesión SSH a 192.168.2.1 desde PC-A (si falla).

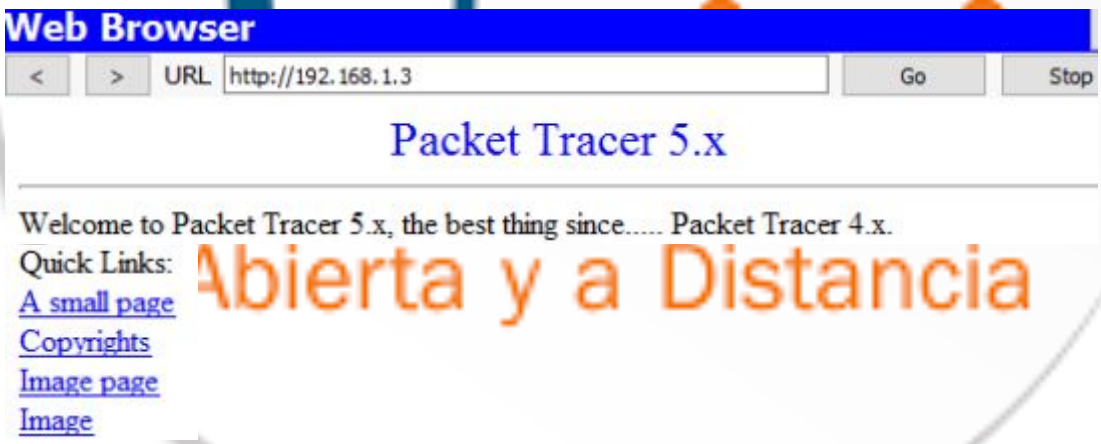
```
SERVER> ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
SERVER>
```

Parte 3. Create a Numbered IP ACL 120 on R1. (Crear una ACL 120 IP numerada en 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. (Permitir que cualquier host externo tenga acceso a servicios de DNS, SMTP y FTP en el servidor PC-A, denegar cualquier acceso de host externo a servicios HTTPS en PC-A y permitir que PC-C acceda a R1 vía SSH).

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser. (Verifique que PC-C puede acceder a la PC-A a través de HTTPS mediante el navegador web).

Be sure to disable HTTP and enable HTTPS on server **PC-A**. (Asegúrese de desactivar HTTP y habilitar HTTPS en el servidor PC-A).



Step 2: Configure ACL 120 to specifically permit and deny the specified traffic. (Configure ACL 120 para permitir y denegar específicamente el tráfico especificado).

Use the access-list command to create a numbered IP ACL. (Utilice el comando access-list para crear una ACL IP numerada).

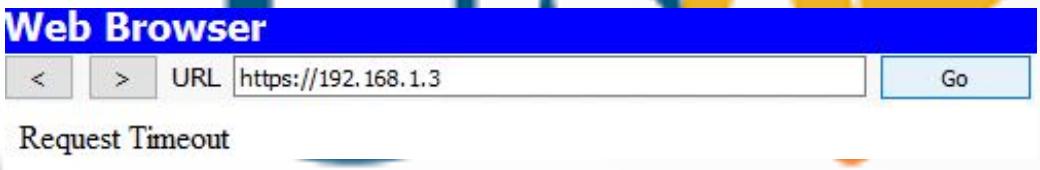
```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)# access-list 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)#
```

Step 3: Apply the ACL to interface S0/0/0. (Aplique la ACL a la interfaz S0 / 0/0).

Use the ip access-group command to apply the access list to incoming traffic on interface S0/0/0. (Utilice el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz S0 / 0/0).

```
R1(config)# interface serial0/0/0
R1(config-if)# ip access-group 120 in
R1(config-if)#exit
R1(config)#
```

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser. (Verifique que PC-C no puede acceder a PC-A a través de HTTPS mediante el navegador web).



Parte 4. Modify An Existing ACL on R1. (Modificar una ACL existente en R1).

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**); deny all other incoming ICMP packets. (Permitir respuestas de eco ICMP y mensajes inaccesibles de destino desde la red externa (en relación con R1); Deniegue todos los demás paquetes ICMP entrantes).

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2. (Compruebe que PC-A no puede realizar ping satisfactoriamente en la interfaz de bucle invertido en R2).

```
SERVER> ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>
```

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic. (Realice los cambios necesarios en ACL 120 para permitir y denegar el tráfico especificado).

Use the access-list command to create a numbered IP ACL. (Utilice el comando access-list para crear una ACL IP numerada).

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

Step 3: Verify that PC-A can successfully ping the loopback interface on R2. (Compruebe que PC-A puede hacer ping exitosamente en la interfaz de bucle invertido en R2).

```
SERVER> 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

SERVER>
```

Parte 5. Create a Numbered IP ACL 110 on R3. (Crear una ACL 110 IP numerada en R3).

Deny all outbound packets with source address outside the range of internal IP addresses on R3. (Denegar todos los paquetes salientes con dirección de origen fuera del rango de direcciones IP internas en R3).

Step 1: Configure ACL 110 to permit only traffic from the inside network. (Configure ACL 110 para permitir sólo el tráfico desde la red interna).

Use the **access-list** command to create a numbered IP ACL. (Utilice el comando access-list para crear una ACL IP numerada).

```
R3# config 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. (Aplique la ACL a la interfaz F0 / 1).

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1. (Utilice el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz F0 / 1).

```
R3(config-if)# exit
R3(config)# interface fa0/1
R3(config-if)# ip access-group 110 in
R3(config-if)# exit
R3(config)#
```

Parte 6. Create a Numbered IP ACL 100 on R3. (Crear una IP Numbered IP 100 en 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. (En R3, bloquee todos los paquetes que contengan la dirección IP de origen del siguiente conjunto de direcciones: 127.0.0.0/8, cualquier dirección privada RFC 1918 y cualquier dirección de multidifusión IP).

Step 1: Configure ACL 100 to block all specified traffic from the outside network. (Configure ACL 100 para bloquear todo el tráfico especificado de la red externa).

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). (También debe bloquear el tráfico proveniente de

su propio espacio de direcciones interno si no es una dirección RFC 1918 (en esta actividad, su espacio de direcciones interno es parte del espacio de direcciones privadas especificado en RFC 1918).

Use the **access-list** command to create a numbered IP ACL. (Utilice el comando access-list para crear una ACL IP numerada).

```
R3(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
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(config)#
```

Step 2: Apply the ACL to interface Serial 0/0/1. (Aplicar la ACL a la interfaz Serial 0/0/1).

Use the ip access-group command to apply the access list to incoming traffic on interface Serial 0/0/1. (Utilice el comando ip access-group para aplicar la lista de acceso al tráfico entrante en la interfaz Serial 0/0/1).

```
R3(config)# interface serial0/0/1
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. (Confirme que se ha caído el tráfico especificado que entra en la interfaz Serial 0/0/1).

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. (En el símbolo del sistema PC-C, haga ping al servidor PC-A. Las respuestas de eco ICMP están bloqueadas por la ACL, ya que se obtienen del espacio de direcciones 192.168.0.0/16).

```
PC> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Step 4: Check results. (Comprobar los resultados).

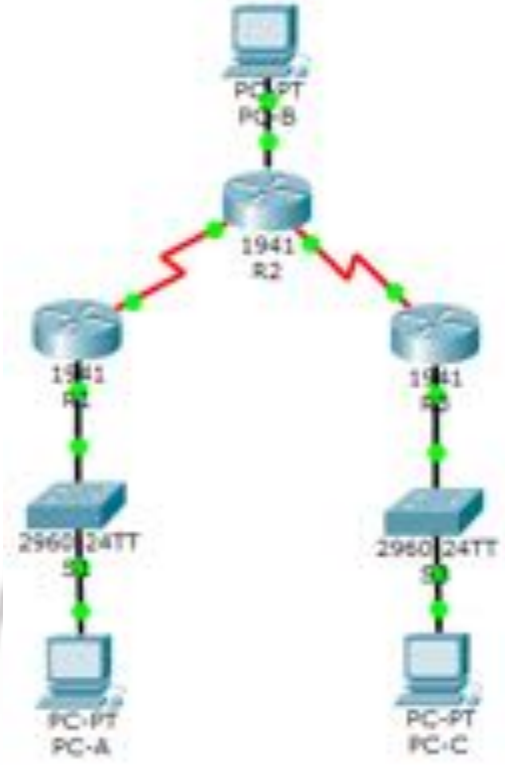
Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed. (Su porcentaje de finalización debe ser del 100%. Haga clic en Comprobar resultados para ver la retroalimentación y la verificación de los componentes necesarios que se han completado).

Informe 8

Laboratorio: 7.3.2.4. Configuración básica de RIPv2 y RIPng.

Topología de la guía:

Topología del laboratorio:



Universidad Nacional
Abierta y a Distancia

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
	S0/0/1	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 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.

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).

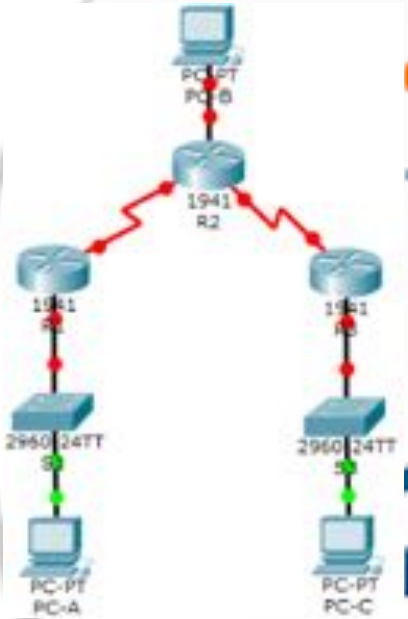
* Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola.

* 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.

Paso 3: Configurar los parámetros básicos para cada router y switch.

a. Desactive la búsqueda del DNS.

R1	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# no ip domain-lookup Router(config)# exit Router#

R2	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# no ip domain-lookup Router(config)# exit Router#
R3	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# no ip domain-lookup Router(config)# exit Router#
S1	Switch# config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# no ip domain-lookup Switch(config)# exit Switch#
S3	Switch# config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# no ip domain-lookup Switch(config)# exit Switch#

b. Configure los nombres de los dispositivos como se muestra en la topología.

R1	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# hostname R1 R1(config)# EXIT R1#
R2	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# hostname R2 R2(config)# exit R2#
R3	Router# config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# hostname R3 R3(config)# exit R3#

S1	Switch# config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# hostname S1 S1(config)# exit S1#
S3	Switch# config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# hostname S3 S3(config)# exit S3#

c. Configurar la encriptación de contraseñas.

R1	R1# config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)# service password-encryption R1(config)#
R2	R2# config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)# service password-encryption R2(config)#
R3	R3# config t Enter configuration commands, one per line. End with CNTL/Z. R3(config)# service password-encryption R3(config)#
S1	S1# config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)# service password-encryption S1(config)#
S3	S3# config t Enter configuration commands, one per line. End with CNTL/Z. S3(config)# service password-encryption S3(config)#

d. Asigne class como la contraseña del modo EXEC privilegiado.

R1	R1# config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)# enable password class R1(config)#

R2	R2# config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)# enable password class R2(config)#
R3	R3# config t Enter configuration commands, one per line. End with CNTL/Z. R3(config)# enable password class R3(config)#
S1	S1# config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)# enable password class S1(config)#
S3	S3# config t Enter configuration commands, one per line. End with CNTL/Z. S3(config)# enable password class S3(config)#

e. Asigne cisco como la contraseña de consola y la contraseña de vty.

R1	R1(config)# line console 0 R1(config-line)# password cisco R1(config-line)# login R1(config-line)# exit	R1(config)# line vty 0 15 R1(config-line)# password cisco R1(config-line)# login R1(config-line)# exit R1(config)#
R2	R2(config)# line console 0 R2(config-line)# password cisco R2(config-line)# login R2(config-line)# exit	R2(config)# line vty 0 15 R2(config-line)# password cisco R2(config-line)# login R2(config-line)#exit R2(config)#
R3	R3(config)# line console 0 R3(config-line)# password cisco R3(config-line)# login R3(config-line)# exit	R3(config)# line vty 0 15 R3(config-line)# password cisco R3(config-line)# login R3(config-line)#
S1	S1(config)# line console 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)#exit	S1(config)# line vty 0 15 S1(config-line)# password cisco S1(config-line)# login S1(config-line)#exit S1(config)#

S3	S3(config)# line console 0 S3(config-line)# password cisco S3(config-line)# login S3(config-line)# exit	S3(config)# line vty 0 15 S3(config-line)# password cisco S3(config-line)# login S3(config-line)# exit S3(config)#

f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

R1	R1# config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)# banner motd "El Acceso no Autorizado esta Prohibido!" R1(config)#
R2	R2# config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)# banner motd " El Acceso no Autorizado esta Prohibido!" R2(config)#
R3	R3# config t Enter configuration commands, one per line. End with CNTL/Z. R3(config)# banner motd "El acceso no Autorizado esta Prohibido!" R3(config)#
S1	S1# config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)# banner motd " El Acceso no Autorizado esta Prohibido!" S1(config)#
S3	S3# config t Enter configuration commands, one per line. End with CNTL/Z. S3(config)# banner motd "El Acceso no Autorizado esta Prohibido!" S3(config)#

g. Configure logging synchronous para la línea de consola.

R1	R1(config)# line console 0 R1(config-line)# logging synchronous R1(config-line)# exit R1(config)#
R2	R2(config)# line console 0 R2(config-line)# logging synchronous R2(config-line)# exit R2(config)#

R3	R3(config)# line console 0 R3(config-line)# logging synchronous R3(config-line)# exit R3(config)#
S1	S1(config)# line console 0 S1(config-line)# logging synchronous S1(config-line)# exit S1(config)#
S3	S3(config)# line console 0 S3(config-line)# logging synchronous S3(config-line)# exit S3(config)#

h. Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.

R1:

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface g0/1
R1(config-if)# Description Connection to S1
R1(config-if)# ip address 172.30.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(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
R1(config-if)# exit
R1(config)# interface serial0/0/0
R1(config-if)# Description DCE Connection to R2
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# no shutdown
```

R2:

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface g0/0
R2(config-if)# Description Connection to PC-B
R2(config-if)# ip address 209.165.201.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)# exit
R2(config)# interface serial0/0/0
R2(config-if)# Description Connection to R1
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# exit
R2(config)# interface serial0/0/1
R2(config-if)# Description Connection to R3
R2(config-if)# Description DCE Connection to R3
R2(config-if)# ip address 10.2.2.2 255.255.255.252
R2(config-if)#exit
R2(config)#
```

R3:

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface g0/1
R3(config-if)# Description Connection to S3
R3(config-if)# ip address 172.30.30.1 255.255.255.0
R3(config-if)# no shutdown
R3(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
R3(config-if)# exit
R3(config)# interface serial0/0/1
R3(config-if)# Description Connection to R2
R3(config-if)# ip address 10.2.2.1 255.255.255.252
R3(config-if)# exit
R3(config)#
```

i. Configure una descripción para cada interfaz con una dirección IP.

R1:

```
R1(config)# interface g0/1
R1(config-if)# Description Connection to S1

R1(config)# interface serial0/0/0
R1(config-if)# Description DCE Connection to R2
```

R2:

```
R2(config)# interface g0/0
R2(config-if)# Description Connection to PC-B

R2(config)# interface serial0/0/0
R2(config-if)# Description Connection to R1

R2(config)# interface serial0/0/1

R2(config-if)# Description DCE Connection to R3
```

R3:

```
R3(config)# interface g0/1
R3(config-if)# Description Connection to S3

R3(config)# interface serial0/0/1
R3(config-if)# Description Connection to R2
```

S1:

```
S1(config)# interface f0/5
S1(config-if)# Description Connection to R1

S1(config)# Interface f0/6
S1(config-if)# Description Connection to PC-A
```

S3:

```
S3(config)# interface f0/5
S3(config-if)# Description Connection to R3
S3(config)# interface f0/18
S3(config-if)# Description Connection to PC-C
```

j. Configure la frecuencia de reloj, si corresponde, para la interfaz serial DCE.

R1:

```
R1# clock set 07:40:00 15 Nov 2016
R1#
```

```
R1(config)#interface serial0/0/0
R1(config-if)# clock rate 128000
R1(config-if)# exit
R1(config)#
```

R2:

```
R2# clock set 07:42:00 15 Nov 2016
R2#
```

```
R2(config)# interface serial0/0/1
R2(config-if)# clock rate 128000
R2(config-if)#exit
R2(config)#
```

k. Copie la configuración en ejecución en la configuración de inicio.

R1:

```
R1# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

R2:

```
R2# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

R3:

```
R3# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

S1:

```
S1#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

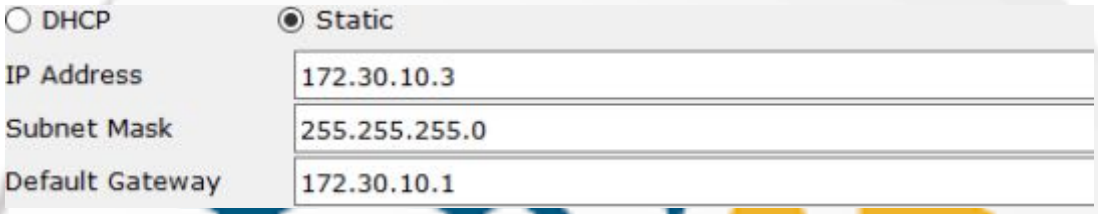
S3:

```
S3# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

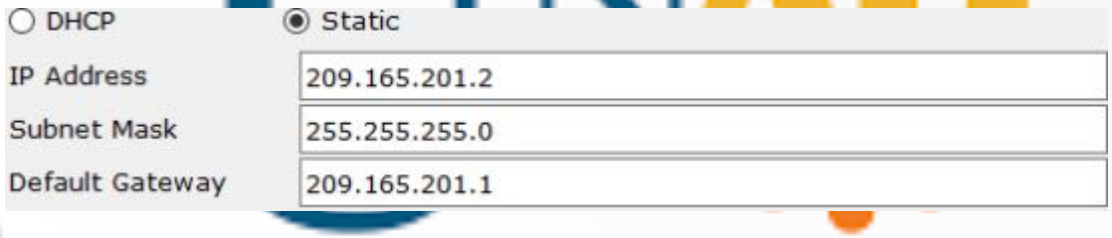
Paso 4: Configurar los equipos host.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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

- **PC-A:**



- **PC-B:**



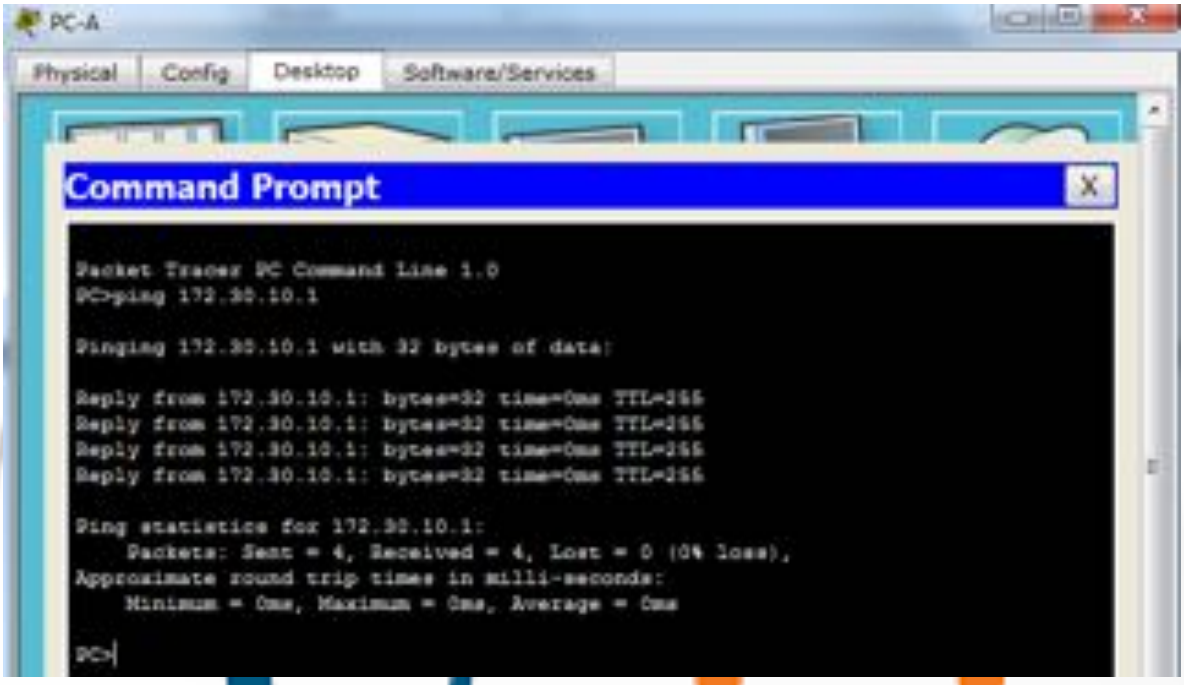
- **PC-C:**

Paso 5: Probar la conectividad.

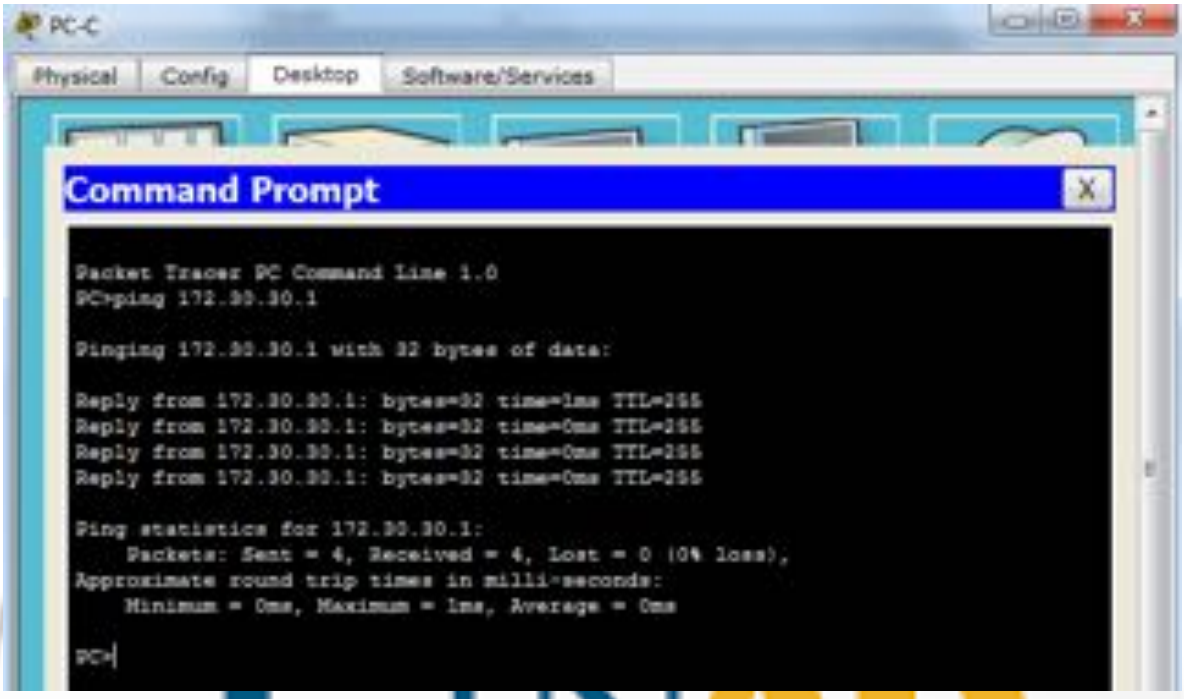
En este momento, las computadoras no pueden hacerse ping entre sí.

a. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

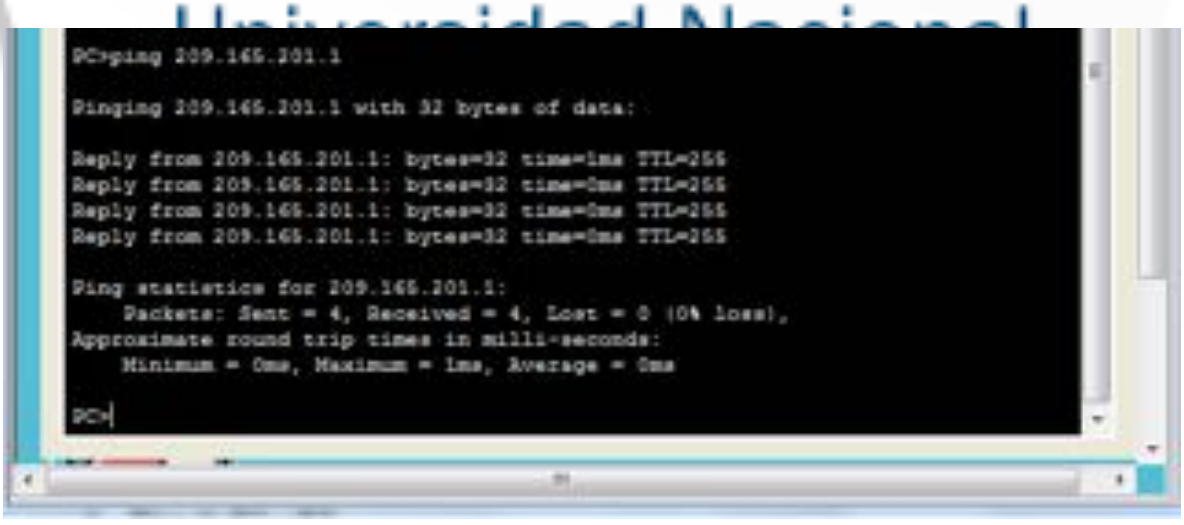
Ping de PC-A a R1:



Ping de PC-C a R3:



Ping de PC-B a R2:



b. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

Ping de R2 a R1:

```
R2# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/17 ms

R2#
```

Ping de R2 a R3:

```
R2# ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/26 ms

R2#
```

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.

a. 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 t
Enter configuration commands, one per line.  End with CNTL/Z.
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**

```
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
R1(config-router)#exit
R1(config)#
```

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.

b. Configure RIPv2 en el R3 y utilice la instrucción network para agregar las redes apropiadas y evitar actualizaciones de routing en la interfaz LAN.

```
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# passive-interface  g0/1
R3(config-router)# network 172.30.0.0
R3(config-router)# network 10.0.0.0
R3(config-router)# exit
R3(config)#
```

c. Configure RIPv2 en el R2. No anuncie la red 209.165.201.0.

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 10.0.0.0
R2(config-router)# exit
R2(config)#
```

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# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     209.165.201.1   YES manual up                    up

GigabitEthernet0/1     unassigned      YES unset  up                    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? ¿Por qué?

Rta: No. Porque no hay una ruta que llegue a PC-B.

```
PC> 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),

PC>
```

¿Es posible hacer ping de la PC-A a la PC-C? ¿Por qué?

Rta: No, porque no hay rutas que las conecte.

```
PC> ping 172.30.30.3

Pinging 172.30.30.3 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 172.30.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

¿Es posible hacer ping de la PC-C a la PC-B? ¿Por qué?

Rta: No. Porque la PC-B no está participando en red.

```
PC> 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),

PC>
```

¿Es posible hacer ping de la PC-C a la PC-A? ¿Por qué?

Rta: No, porque R1 y R3 no tienen rutas estáticas definidas.

```
PC>  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),

PC>
```

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**
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)

```
R1# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 25 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
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      00:00:01
Distance: (default is 120)
R1#
```

Al emitir el comando debug ip rip en el R2,

```
R2# debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

R2#
```

¿Qué información se proporciona que confirma que RIPv2 está en ejecución?

Rta: Al ver que se envían paquetes via serial 0/0/0 y 0/0/1.

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

Al emitir el comando show run en el R3,

```
R3# show run
Building configuration...

Current configuration : 1133 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3

!
router rip
 version 2
 passive-interface GigabitEthernet0/1
 network 10.0.0.0
 network 172.30.0.0
```

¿Qué información se proporciona que confirma que RIPv2 está en ejecución?

Rta: Se encuentra router rip con su versión configurada.

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

```
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

     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 10.1.1.1, 00:00:23, Serial0/0/0
                   [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
     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
R2#
```

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
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
172.30.0.0/16 is variably subnetted, 2 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

```
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
```

```
     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, 00:00:26, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 2 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
R1#
```

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

R3# **show ip route**

<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

```
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:11, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, 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
R3#
```

Utilice el comando **debug ip rip** en el R2 para determinar las rutas recibidas en las actualizaciones RIP del R3 e indíquelas a continuación.

```
R2# debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops
```

Rta: El R3 no está envía ninguna de las subredes 172.30.0.0, solo la ruta resumida 172.30.0.0/16, incluida la máscara de subred. Por lo tanto, las tablas de routing del R1 y el R2 no muestran las subredes 172.30.0.0 en el R3.

Paso 3: Desactivar la sumarización automática.

a. El comando no auto-summary se utiliza para desactivar la sumarización automática en RIPv2. Deshabilite la sumarización automática en todos los routers. Los routers ya no resumirán las rutas en los límites de las redes principales con clase. Aquí se muestra R1 como ejemplo.

R1(config)# **router rip**

R1(config-router)# **no auto-summary**

- **R1:**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)# no auto-summary
R1(config-router)#
```

- **R2:**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# router rip
R2(config-router)# no auto-summary
R2(config-router)#
```

- **R3:**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# router rip
R3(config-router)# no auto-summary
R3(config-router)#
```

b. Emita el comando clear ip route * para borrar la tabla de routing.

R1(config-router)# **end**

R1# **clear ip route ***

- **R1:**

```
R1(config-router)# end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1# clear ip route *
R1#
```

- **R2:**

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

R2# clear ip route *
R2#
```

- **R3:**

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

R3# clear ip route *
R3#
```

c. Examinar las tablas de enrutamiento Recuerde que la convergencia de las tablas de routing demora un tiempo después de borrarlas.

Las subredes LAN conectadas al R1 y el R3 ahora deberían aparecer en las tres tablas de routing.

R2# **show ip route**
<Output Omitted>
Gateway of last resort is not set

```
     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
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1
                      [120/1] via 10.1.1.1, 00:01:15, Serial0/0/0
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1
     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
```

```
     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
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:18, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
     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
R2#
```

R1# **show ip route**

<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

```
     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, 00:00:06, 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, 00:00:06, Serial0/0/0
R1#
```

R3# **show ip route**

<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
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:18, Serial0/0/1
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R        172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:18, Serial0/0/1
C        172.30.30.0/24 is directly connected, GigabitEthernet0/1
L        172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3#
```

d. Utilice el comando debug ip rip en el R2 para examinar las actualizaciones RIP.

R2# debug ip rip

```
R2# debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops

R2#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops
R2#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
```

Después de 60 segundos, emita el comando no debug ip rip.

```
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

R2#no debug ip rip
RIP protocol debugging is off
R2#
```

¿Qué rutas que se reciben del R3 se encuentran en las actualizaciones RIP?

Rta: La red 172.30.10.0/24.

¿Se incluyen ahora las máscaras de las subredes en las actualizaciones de enrutamiento?

Rta: Si.

Paso 4: Configure y redistribuya una ruta predeterminada para el acceso a Internet.

a. Desde el R2, cree una ruta estática a la red 0.0.0.0 0.0.0.0, con el comando ip route. Esto envía todo tráfico de dirección de destino desconocida a la interfaz G0/0 del R2 hacia la PC-B y simula Internet al establecer un gateway de último recurso en el router R2.

R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.2**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#
```

b. El R2 anunciará una ruta a los otros routers si se agrega el comando default-information originate a la configuración de RIP.

R2(config)# router rip

R2(config-router)# default-information originate

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

Paso 5: Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

R1# **show ip route**

<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
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, 00:00:27, 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, 00:00:27, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:27, Serial0/0/0
R1#
```

¿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?

Rta: Hay un Gateway de ultimo alcance, es decir la puerta de enlace que nos conecta a internet, y la ruta por defecto que se muestra en la tabla de ruteo esta aprehendida en el rip.

d. Consulte la tabla de routing en el R2.

```
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     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
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:14, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:03, Serial0/0/1
     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
S*   0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

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

Rta: R2 tiene una ruta estatica por defecto que esta conectada a la g0/0

Paso 6: Verifique la conectividad.

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

- **Ping de PC-A a 209.165.201.2:**

```
PC> ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

PC>
```

- **Ping de PC-C a 209.165.201.2:**

```
PC> ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=11ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

PC>
```

¿Tuvieron éxito los pings?

Rta: Si.

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

```
PC> ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=12ms TTL=125
Reply from 172.30.30.3: bytes=32 time=10ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 8ms

PC>
```

¿Tuvieron éxito los pings?

Rta: 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.

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

- **R1:**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)# ipv6 address FE80::1 Link-Local
R1(config-if)#exit
R1(config)# interface serial0/0/0
R1(config-if)# ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)# ipv6 address FE80::1 Link-Local
R1(config-if)# exit
R1(config)#
```

- **R2:**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface g0/0
R2(config-if)# ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)# ipv6 address FE80::2 Link-Local
R2(config-if)# exit
R2(config)# interface serial0/0/0
R2(config-if)# ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)# ipv6 address FE80::2 Link-Local
R2(config-if)# exit
R2(config)# interface serial0/0/1
R2(config-if)# ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)# ipv6 address FE80::2 Link-Local
R2(config-if)# exit
R2(config)#
```

- **R3:**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface g0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)# ipv6 address FE80::3 Link-Local
R3(config-if)# exit
R3(config)# interface serial0/0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:23::3/63
R3(config-if)# ipv6 address FE80::3 Link-Local
R3(config-if)# exit
R3(config)#
```

b. Habilite el routing IPv6 en cada router.

- **R1:**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ipv6 unicast-routing
R1(config)#
```

- **R2:**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ipv6 unicast-routing
R2(config)#
```

- **R3:**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# ipv6 unicast-routing
R3(config)#
```

c. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace.

- **R1:**

```
R1# show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial0/0/0                [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial0/0/1                [administratively down/down]
Vlan1                      [administratively down/down]
R1#
```

- **R2:**

```
R2# show ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1         [up/down]
Serial0/0/0                [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1                [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1                      [administratively down/down]
R2#
```

- **R3:**

```
R3# show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::3
    2001:DB8:ACAD:C::3
Serial0/0/0                [administratively down/down]
Serial0/0/1                [up/up]
    FE80::3
    2001:DB8:ACAD:23::3
Vlan1                      [administratively down/down]
R3#
```

Escriba el comando en el espacio que se incluye a continuación.

Rta: El comando utilizado fue: show ipv6 interface brief.

d. Cada estación de trabajo debe tener capacidad para hacer ping al router conectado. Verifique y resuelva los problemas, si es necesario.

- **Ping de PC-A a R1:**

```
Packet Tracer PC Command Line 1.0
PC> ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=85ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
```

```
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 85ms, Average = 21ms

PC>
```

- **Ping de PC-C a R3:**

```
Packet Tracer PC Command Line 1.0
PC> ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=2ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```

- **Ping de PC-B a R2:**

```
PC> ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=2ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

PC>
```

e. Los routers deben poder hacerse ping entre sí. Verifique y resuelva los problemas, si es necesario.

- **Ping de R1 a R2:**

```
R1# ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

R1#
```

- **Ping de R2 a R1:**

```
R2# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/17 ms

R2#
```

- **Ping de R1 a R3:**

```
R1# ping 172.30.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/34 ms

R1#
```

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.

a. 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**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface g0/1
R1(config-if)# ipv6 rip Test1 enable
R1(config)# interface serial0/0/0
R1(config-if)# ipv6 rip Test1 enable
R1(config-if)# exit
R1(config)#
```

b. Configure RIPng para las interfaces seriales en el R2, con Test2 como el nombre de proceso. No lo configure para la interfaz G0/0

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface serial0/0/0
R2(config-if)# ipv6 rip Test2 enable
R2(config-if)# exit
R2(config)# interface serial0/0/1
R2(config-if)# ipv6 rip Test2 enable
R2(config-if)# exit
R2(config)#
```

c. Configure RIPng para cada interfaz en el R3, con Test3 como el nombre de proceso.

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface g0/1
R3(config-if)# ipv6 rip Test3 enable
R3(config-if)# exit
R3(config)# interface serial0/0/1
R3(config-if)# ipv6 rip Test3 enable
R3(config-if)#exit
R3(config)#
```

d. 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

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

R1#
```

¿En qué forma se indica RIPng en el resultado?

Rta: Se indica como el nombre del proceso.

e. Emita el comando show ipv6 rip Test1.

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 RIPng?

Rta: Ambas tienen la distancia administrativa de 120, usan un conteo de salto como la métrica y envían actualizaciones cada 30 segundos.

f. Inspecciones la tabla de routing IPv6 en cada router.

- **R1:**

```
R1# show ipv6 route
IPv6 Routing Table - 8 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 GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
     via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:C::/64 [120/3]
     via FE80::2, Serial0/0/0, 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
R   2001:DB8:ACAD:22::/63 [120/3]
     via FE80::2, Serial0/0/0, receive
R   2001:DB8:ACAD:23::/64 [120/2]
     via FE80::2, Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

- **R2:**

```
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
R   2001:DB8:ACAD:A::/64 [120/2]
     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
R   2001:DB8:ACAD:C::/64 [120/2]
     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
R   2001:DB8:ACAD:22::/63 [120/2]
     via FE80::3, Serial0/0/1, 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:**

```
R3# show ipv6 route
IPv6 Routing Table - 8 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
R   2001:DB8:ACAD:A::/64 [120/3]
     via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:C::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
     via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:12::/64 [120/2]
     via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:22::/63 [0/0]
     via Serial0/0/1, directly connected
R   2001:DB8:ACAD:23::/64 [120/2]
     via FE80::2, Serial0/0/1, receive
L   2001:DB8:ACAD:23::3/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R3#
```

Escriba el comando apropiado que se usa para ver la tabla de routing en el espacio a continuación.

Rta: El comando que se utilizó fue: show ipv6 route

En el R1, ***¿cuántas rutas se descubrieron mediante RIPng?***

Rta: Mediante RIPng, se descubrieron 2 rutas, en el ruteo de R1.

En el R2, ***¿cuántas rutas se descubrieron mediante RIPng?***

Rta: Mediante RIPng, se descubrieron 2 rutas, en el ruteo de R2.

En el R3, ***¿cuántas rutas se descubrieron mediante RIPng?***

Rta: Mediante RIPng, se descubrieron 2 rutas, en el ruteo de R3.

g. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B?

Rta: No.

```
PC> PING 2001:DB8:ACAD:B::B

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

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

¿Es posible hacer ping de la PC-A a la PC-C?

Rta: Si.

```
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=78ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=10ms TTL=125

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 = 2ms, Maximum = 78ms, Average = 25ms

PC>
```

¿Es posible hacer ping de la PC-C a la PC-B?

Rta: No.

```
PC> PING 2001:DB8:ACAD:B::B

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

Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B::B:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

¿Es posible hacer ping de la PC-C a la PC-A?

Rta: Si.

```
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=12ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=14ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125

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 = 2ms, Maximum = 14ms, Average = 9ms

PC>
```

¿Por qué algunos pings tuvieron éxito y otros no?

Rta: Porque no hay ruta que se notifique para la red de PC-B.

Paso 2: Configurar y volver a distribuir una ruta predeterminada.

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.

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#
```

Escriba el comando que utilizó en el espacio a continuación.

Rta: El comando utilizado fue: ipv6 route ::/0 2001:DB8:ACAD:B::B

b. 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**

```
R2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface serial0/0/0
R2(config-if)# ipv6 rip Test2 default-information originate
R2(config-if)# exit
R2(config)# interface serial0/0/1
R2(config-if)# ipv6 rip Test2 default-information originate
R2(config-if)# exit
R2(config)#
```

Paso 3: Verificar la configuración de enrutamiento.

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

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

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
```

```
R2# show ipv6 route
IPv6 Routing Table - 11 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
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via 2001:DB8:ACAD:B::B, receive
R   2001:DB8:ACAD:A::/64 [120/2]
     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
R   2001:DB8:ACAD:C::/64 [120/2]
     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
R   2001:DB8:ACAD:22::/63 [120/2]
     via FE80::3, Serial0/0/1, 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#
```

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

Rta: Tiene una ruta por defecto estática que se muestra en R2.

b. 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?

Rta: Se muestra distribuidas gracias a RIPng en 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.

- **Ping de PC-A a 2001:DB8:ACAD:B::B/64:**

```
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=1ms 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 de PC-C a 2001:DB8:ACAD:B::B/64:**

```
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=1ms 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
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 = 1ms, Average = 1ms

PC>
```

¿Tuvieron éxito los pings?

Rta: Si, fueron exitosos los pings.

Reflexión:

1. ***¿Por qué desactivaría la sumarización automática para RIPv2?***

Rta: Con el fin de que los routers no sumaricen la ruta hacia la clase mayor y conseguir la conectividad entre las demás redes.

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

Rta: Se aprendieron de actualizaciones de rip recibidas desde el router donde se configure la ruta por defecto.

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

Rta: Ripv2 se configura como notificando las redes y RIPng se configura en las interfaces.

Informe 9

8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2

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

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 en los equipos host y los routers.

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

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

Paso 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

Paso 4. configurar los equipos host.

Paso 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.

Parte 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.

Paso 6. 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
```

Paso 7. 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#
```

Paso 8. 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
```

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
```

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

showiprouteospf

Paso 9. 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)
```

Paso 10. 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 msecs
 Minimum hold time between two consecutive SPFs 10000
msecs
 Maximum wait time between two consecutive SPFs 10000
msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 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 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
```

Paso 11. 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)
```

Paso 12. 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.

Parte 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.

Paso 1. Cambie las ID de router con direcciones de loopback.

b. 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
```

c. 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.

d. Guarde la configuración en ejecución en la configuración de inicio de todos los routers.

e. 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.

f. 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)
```

g. 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#
```

Paso 13. 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
```

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.

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)
```

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
```

Parte 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.

Paso 14. 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)
```

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)
```

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, l - 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
```

Paso 15. 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
```

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
```

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
```

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)
```

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**.

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
```

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? **Serial0/0/0**

¿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? **La interfaz S 0/0/1 es pasiva**

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

R2(config)#routerospf 1

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

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? **Serial0/0/1**

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

65 =Costo del enlace serial del R1 al R2 = 64 +Costo del enlace Gigabit Ethernet en el R2 = 1

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

Parte 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.

Paso 16. 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.

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, l - 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,
00:00:57, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2,
00:00:57, 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.

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)
```

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**.

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.
```

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

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)
```

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, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/6486] via 192.168.12.2,
00:05:40, Serial0/0/0
O     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
O        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/
```

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?

El objetivo es ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda de referencia a un valor superior, a fin de admitir redes con enlaces más rápidos que 100 Mb/s

Paso 17. 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>
```

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, l - 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
```

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, l - 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
```

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
```

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, l - 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
```

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.

CostointSe0/0/0=781+costo int G0/0=1 entonces costo deR1 a la red 192.168.3.0/24=782

Costo intSe0/0/0=781+costoint S0/0/1=64 entonces costo del R1 a la red 192.168.23.0/30 =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, l - 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
```

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__Costo = 781 + 781 =1562

Paso 18. 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, l - 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, l - 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,
00:02:06, Serial0/0/0
O     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
O        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.

Porque se Aplico el comando ipospfcost 1565 a la interfaz S0/0/1 en el R1quedando un costo de 1565 que es mayor al costo acumulado de la ruta a través del R2, que es 1563.

Reflexión

1. ¿Por qué es importante controlar la asignación de ID de router al utilizar el protocolo OSPF?

   El router con OSPF habilitado usa la ID para Identificar el router de manera exclusiva, otros routers usan la ID del router para identificar de forma exclusiva cada router dentro del dominio OSPF y todos los paquetes que se originan en ellos.

2. ¿Por qué el proceso de elección de DR/BDR no es una preocupación en esta práctica de laboratorio?

   La configuración de red es punto a punto y no multiacceso

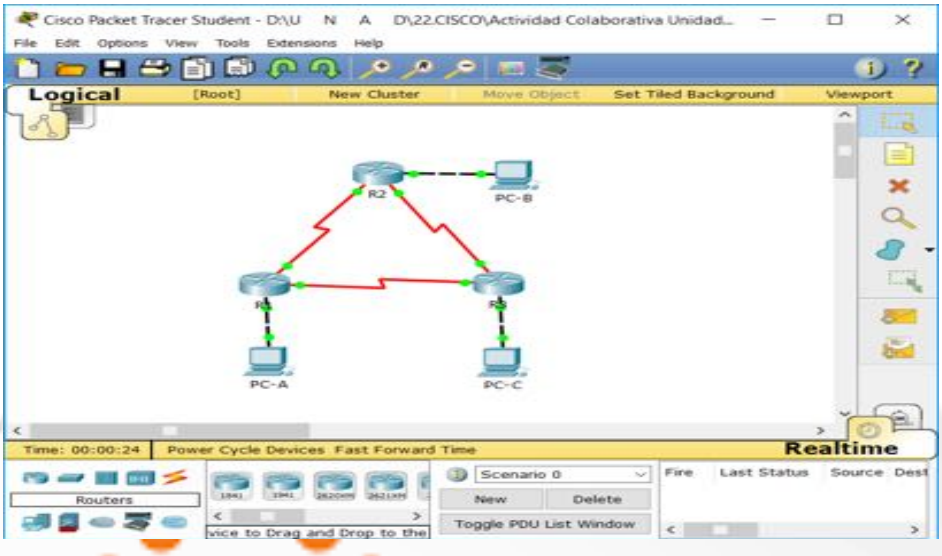
3. ¿Por qué querría configurar una interfaz OSPF como pasiva?

   Para no enviar paquetes hello por esa interfaz y ahorrar 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.				

Captura de evidencia



Universidad Nacional Abierta y a Distancia

Informe 10

8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3

Práctica de laboratorio: configuración de OSPFv3 básico de área única

Topología

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

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.

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

Parte 2. 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.

Paso 19. realizar el cableado de red tal como se muestra en la topología.

Paso 20. inicializar y volver a cargar los routers según sea necesario.

Paso 21. 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 vty.

e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

f. Configure **logging synchronous** para la línea de consola.

g. Cifre las contraseñas de texto no cifrado.

h. Configure las direcciones link-local y de unidifusión IPv6 que se indican en la tabla de direccionamiento para todas las interfaces.

i. Habilite el routing de unidifusión IPv6 en cada router.

j. Copie la configuración en ejecución en la configuración de inicio

Paso 22. configurar los equipos host.

Paso 23. 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.

Parte 2. 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.

Paso 24. 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**

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**

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.

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>

Paso 25. 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**

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

Paso 26. 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

Paso 27. 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

Paso 28. verificar las interfaces OSPFv3.

a. 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
```

Paso 29. 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

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

Show ipv6 ospf route

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.

Parte 3: 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.

Paso 30. 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::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
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**

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

Paso 31. 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**

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

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)

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**.

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

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.

¿Qué interfaz usa el R1 para enrutarse a la red 2001:DB8:ACAD:B::/64? **S0/0/1**

¿Cuál es la métrica de costo acumulado para la red 2001:DB8:ACAD:B::/64 en el R1? **129**

¿El R2 aparece como vecino OSPFv3 en el R1? **NO**

¿El R2 aparece como vecino OSPFv3 en el R3? **SÍ**

¿Qué indica esta información?

Todo el tráfico a la red 2001:DB8:ACAD:B::/64 desde R1 será enrutado a través de R3.

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.

h. Verifique que el R1 y el R2 ahora sean vecinos OSPFv3.

Reflexión

1. 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?

   SÍ, El ID de proceso de OSPFv3 solo es usado localmente en el router, no tiene que ser igual al ID de proceso usado en los otros router del área OSPFv3

2. ¿Cuál podría haber sido la razón para eliminar el comando **network** en OSPFv3?

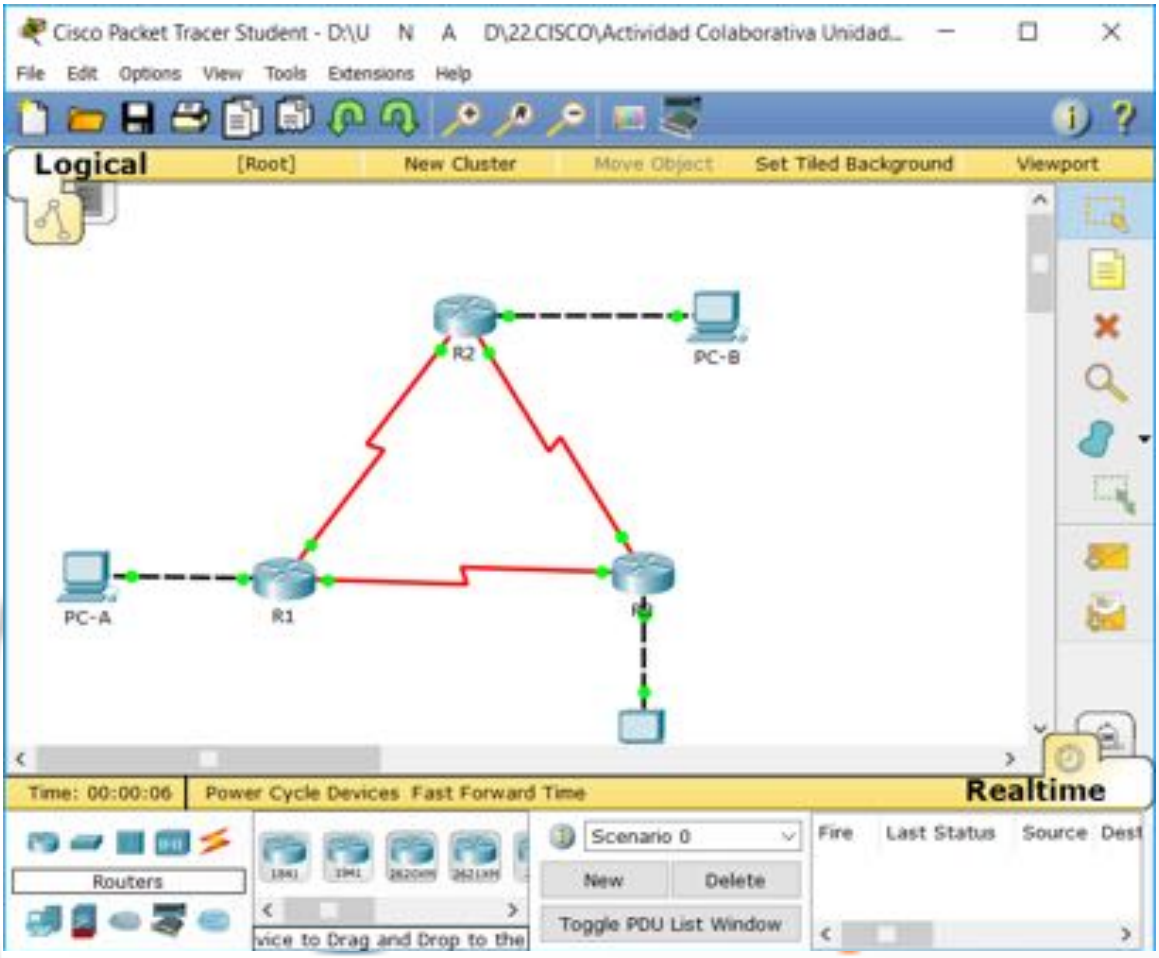
   El comando network no fue completamente eliminado, simplemente se puede obviar y se toma la configuración de red del dispositivo, puede que esta modificación se halla implementado para evitar errores de escritura de las direcciones IPv6.

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.

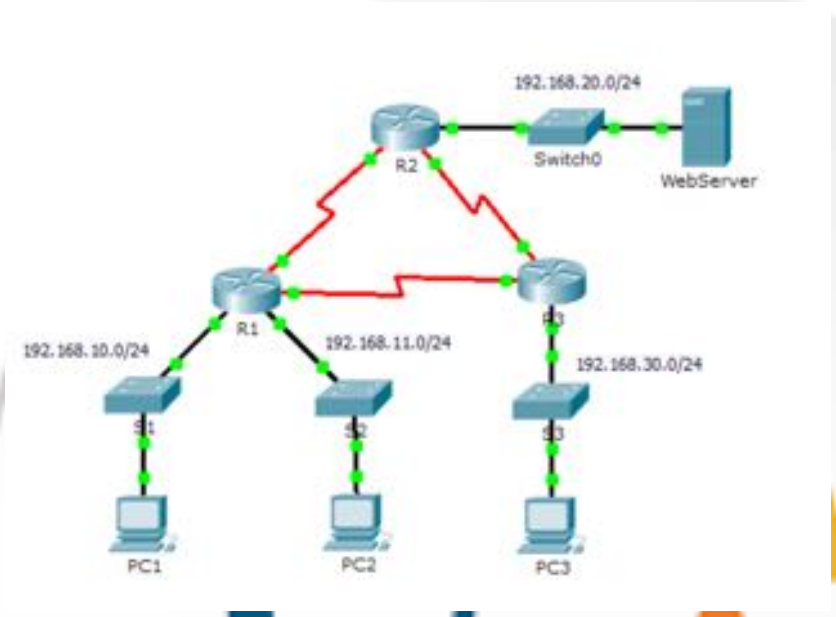
Captura de Evidencia



Universidad Nacional
Abierta y a Distancia

Informe 11

Práctica 9.2.1.10 Packet Tracer Configuring Standard ACLs Instructions IG



Addressing Table

Packet Tracer - Configuring Standard ACLs

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	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objectives
Part 1: Plan an ACL Implementation
Part 2: Configure, Apply, and Verify a Standard ACL
Background / Scenario
Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Parte 1. Plan an ACL Implementation

Step 1: Investigate the current network configuration.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.
Step 2: Evaluate two network policies and plan ACL implementations.
a. The following network policies are implemented on R2:

- The 192.168.11.0/24 network is not allowed access to the WebServer on the 192.168.20.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.11.0/24 network to the WebServer at 192.168.20.254 without interfering with other traffic, an ACL must be created on R2. The access list must be placed on the outbound interface to the WebServer. A second rule must be created on R2 to permit all other traffic.
b. The following network policies are implemented on R3:

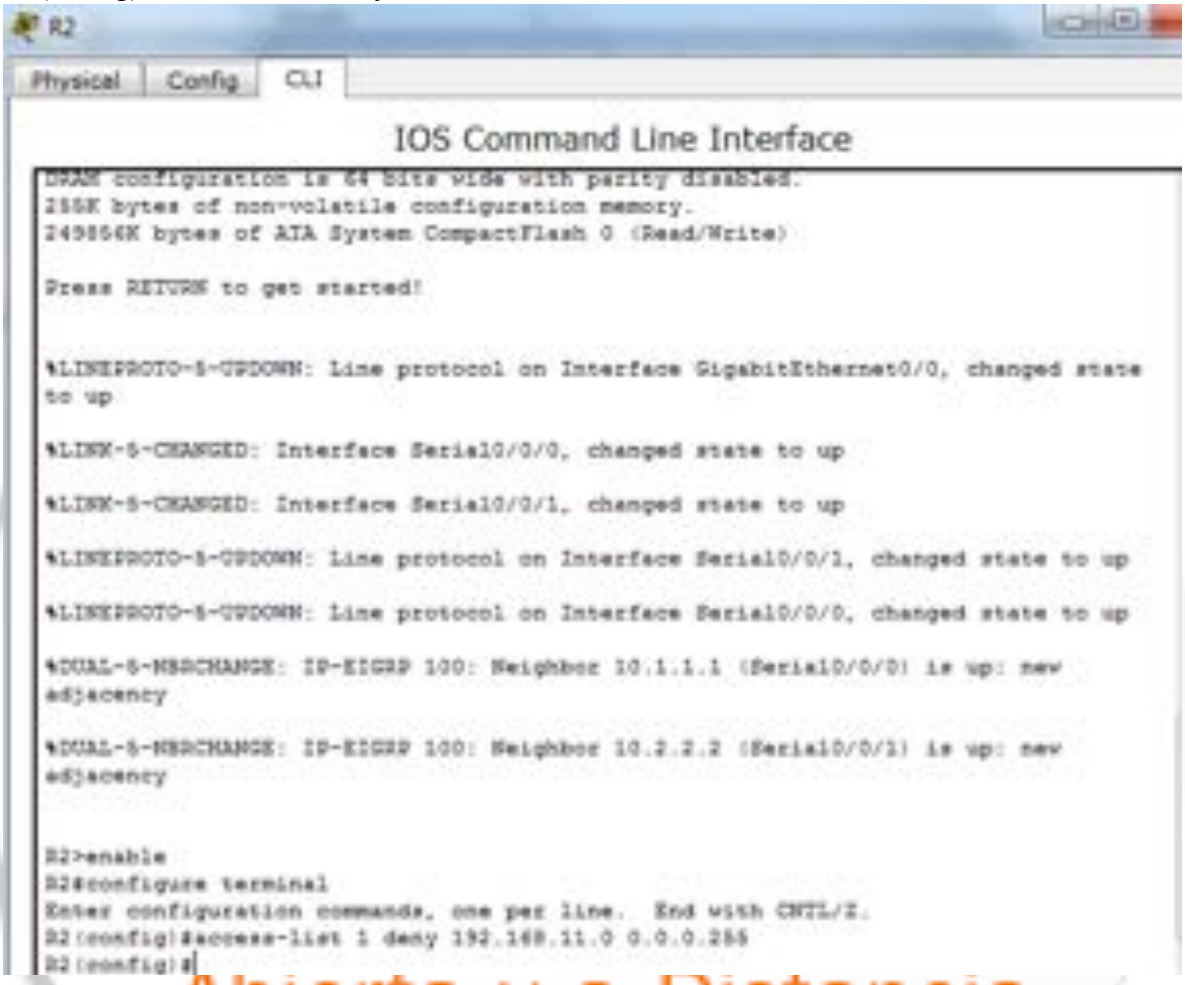
- The 192.168.10.0/24 network is not allowed to communicate to the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on R3. The ACL must placed on the outbound interface to PC3. A second rule must be created on R3 to permit all other traffic.

Parte 2. Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

a. Create an ACL using the number 1 on R2 with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255



b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:
R2(config)# access-list 1 permit any

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 permit any
R2(config)#
```

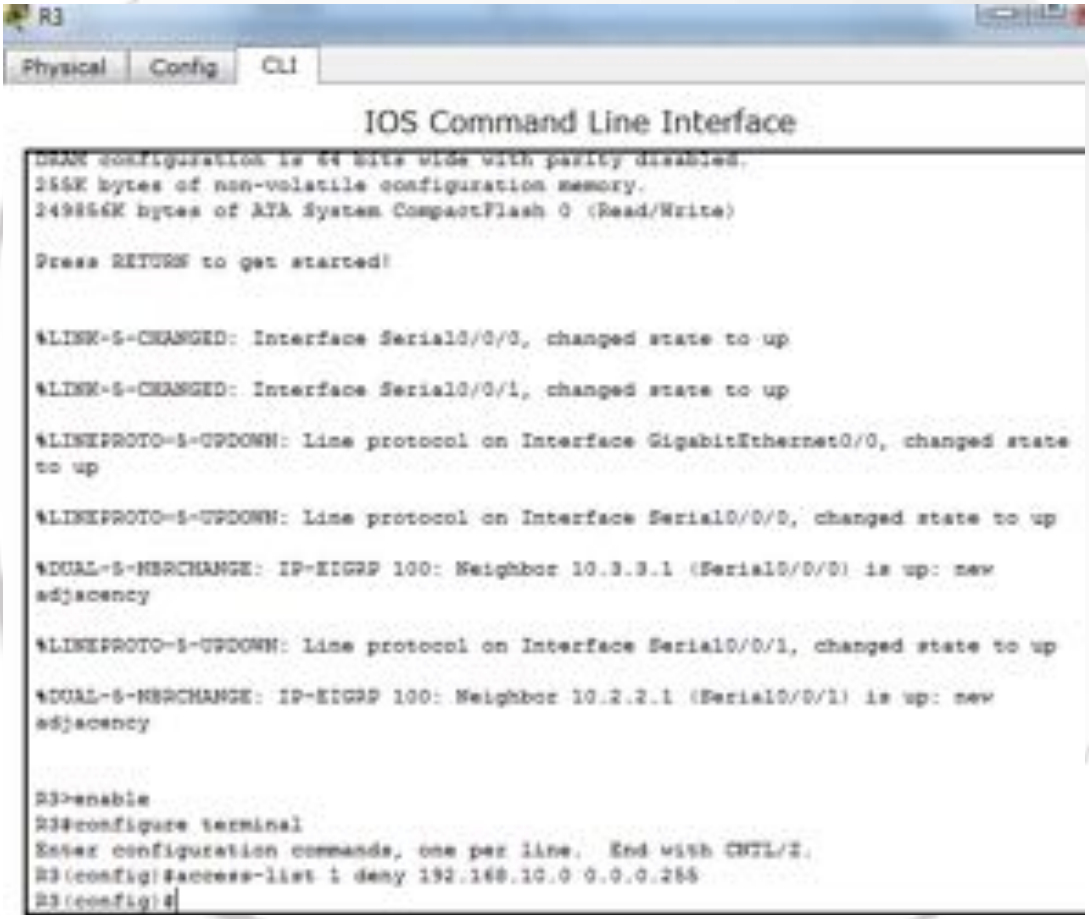
c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 permit any
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

Step 2: Configure and apply a numbered standard ACL on R3.

a. Create an ACL using the number 1 on R3 with a statement that denies access to the 192.168.30.0/24 network from the PC1 (192.168.10.0/24) network.

R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255



b. By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

R3(config)# access-list 1 permit any

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 permit any
R3(config)#
```

c. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.
R3(config)# interface GigabitEthernet0/0

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0
R3(config-if)#
```

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

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

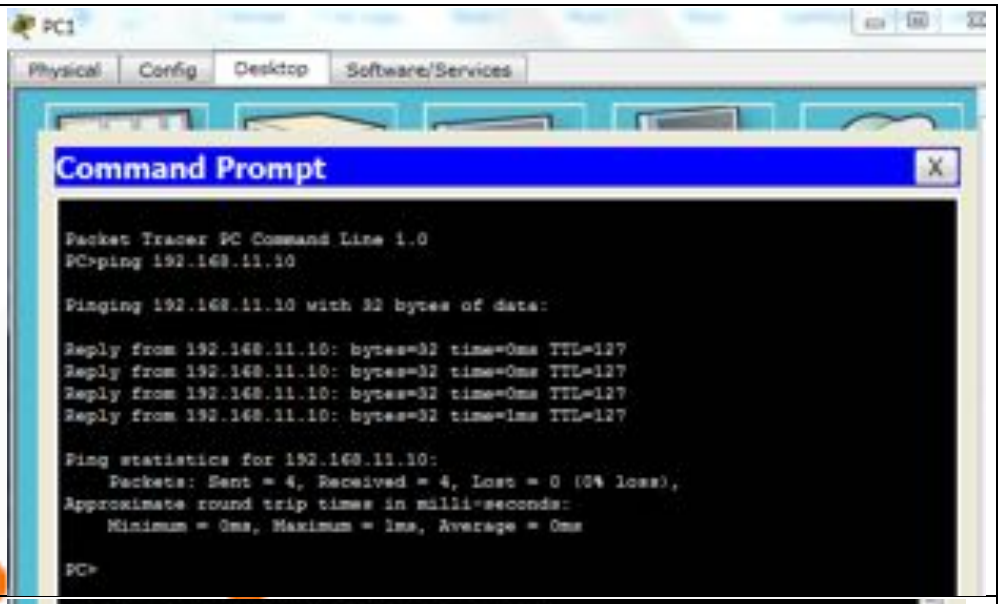
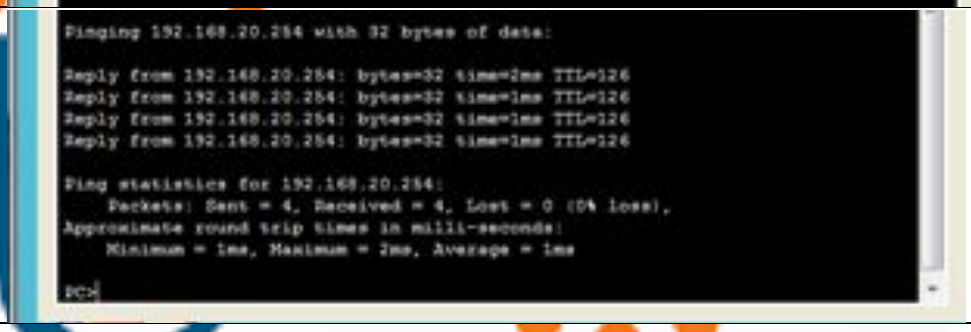
Parte 3. Verify ACL configuration and functionality.

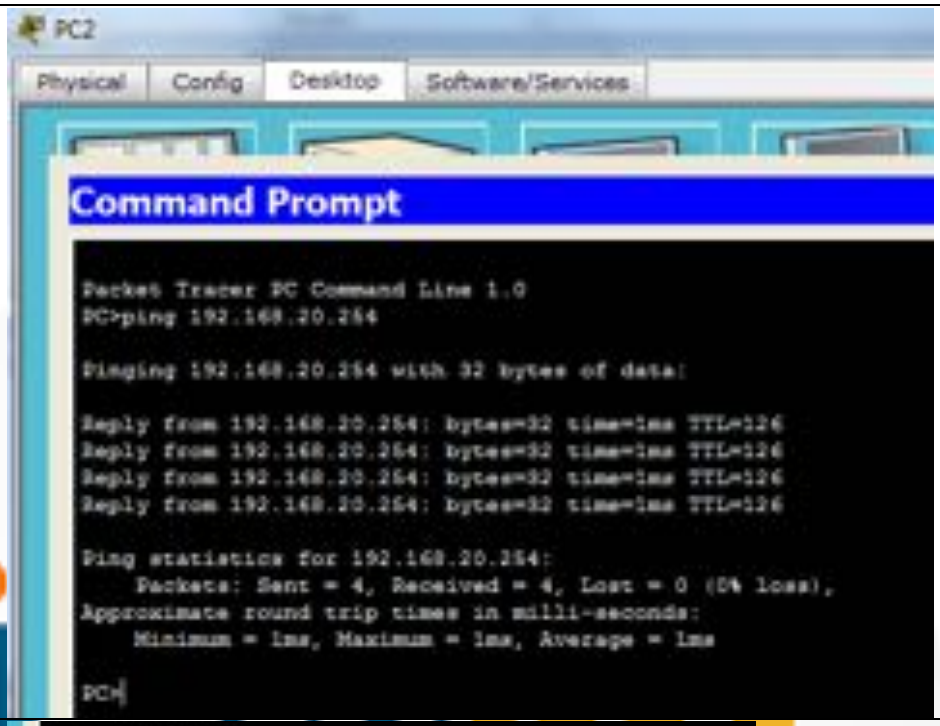
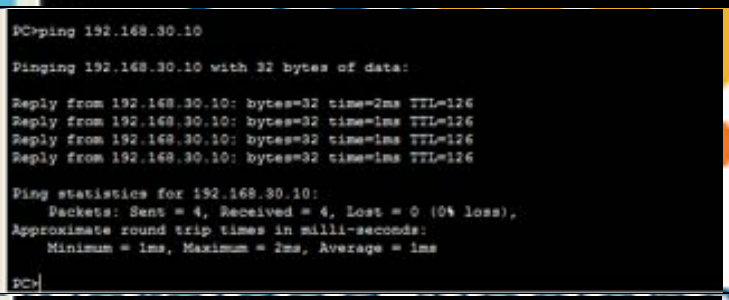
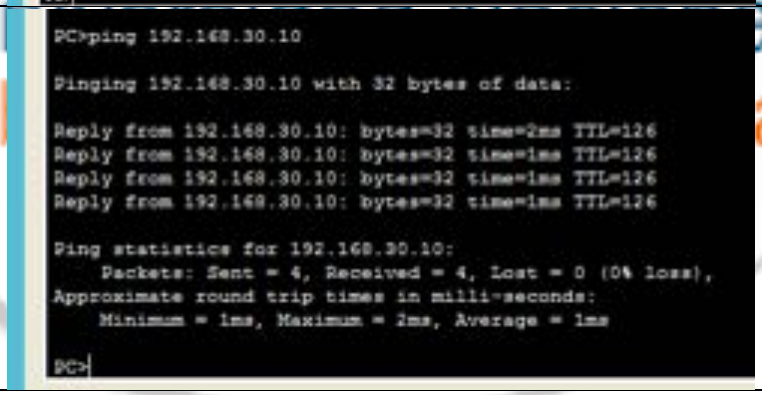
a. On R2 and R3, enter the show access-list command to verify the ACL configurations. Enter the show run or show ip interface gigabitethernet 0/0 command to verify the ACL placements.

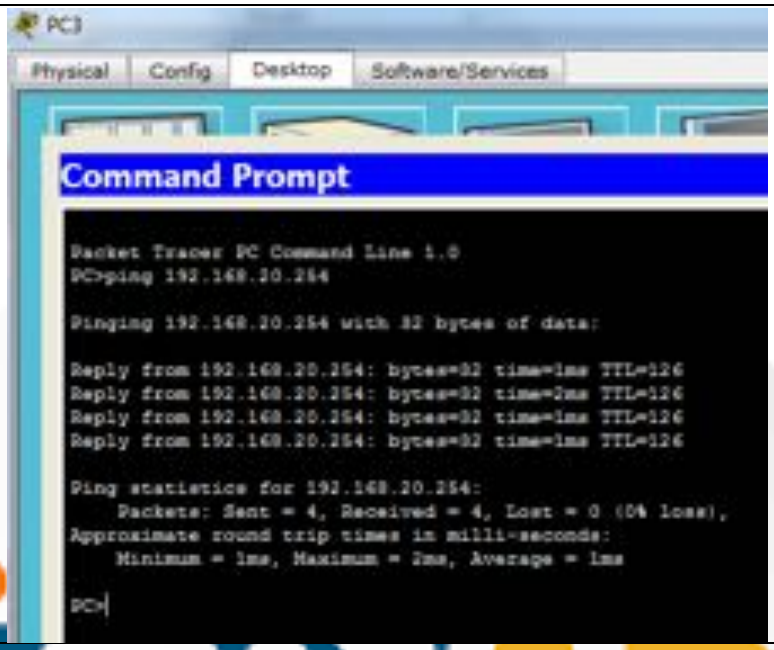
```
R3#show access lists
R3#show access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
R3#
```

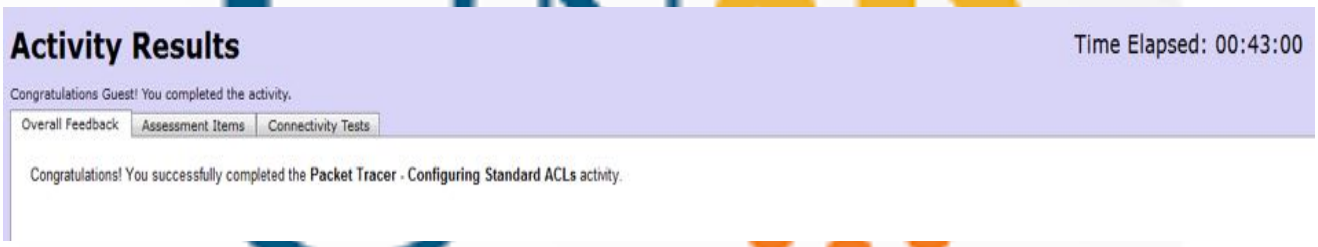
Comando Show run

b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

A ping from 192.168.10.10 to 192.168.11.10 succeeds.	
A ping from 192.168.10.10 to 192.168.20.254 succeeds.	

A ping from 192.168.11.10 to 192.168.20.254 fails.	
A ping from 192.168.10.10 to 192.168.30.10 fails.	
A ping from 192.168.11.10 to 192.168.30.10 succeeds.	

A ping from 192.168.30.10 to 192.168.20.254 succeeds.	



Informe 12

Práctica 9.2.1.11 Configuración de ACL estándar con nombre

Topología

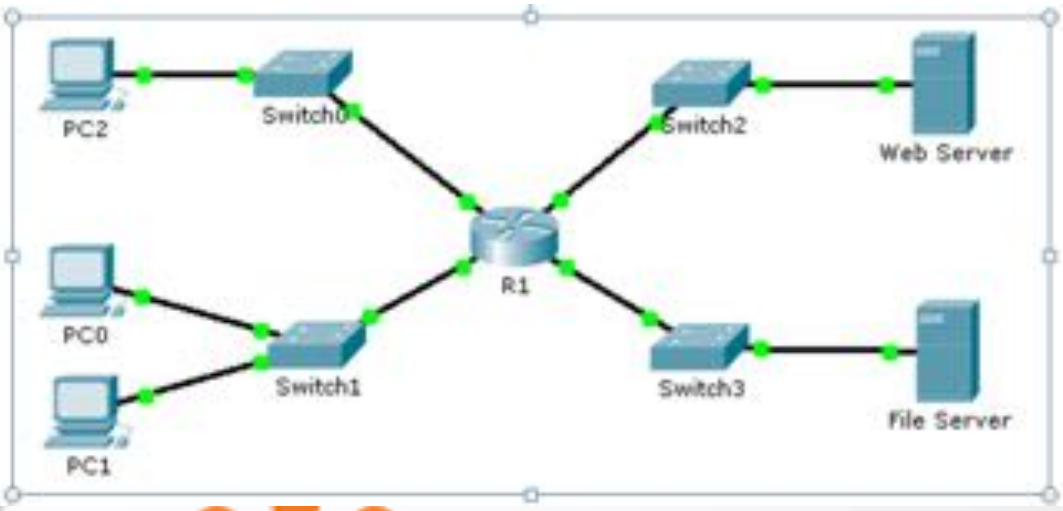


Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
Servidor de archivos	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Servidor web	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Objetivos

Parte 1: Configurar y aplicar una ACL estándar con nombre

Parte 2: Verificar la implementación de la ACL

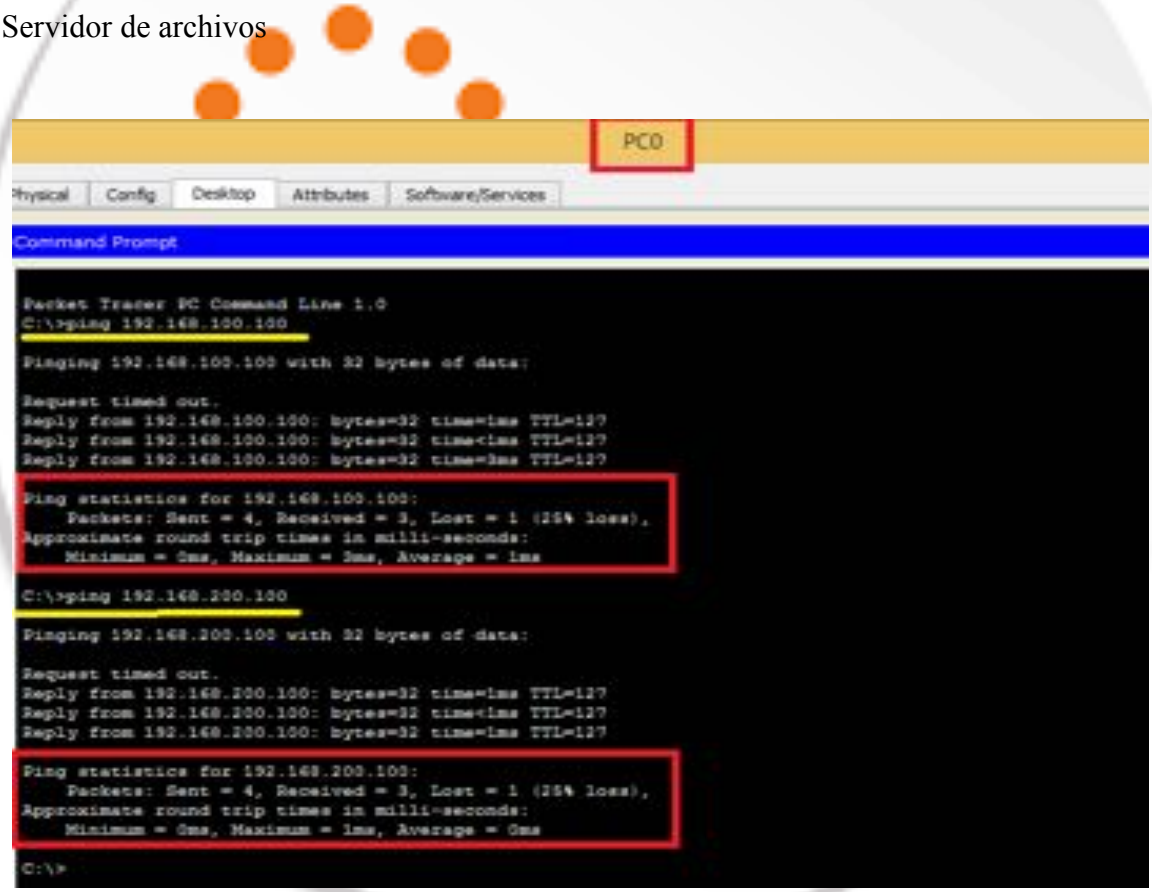
Información Básica

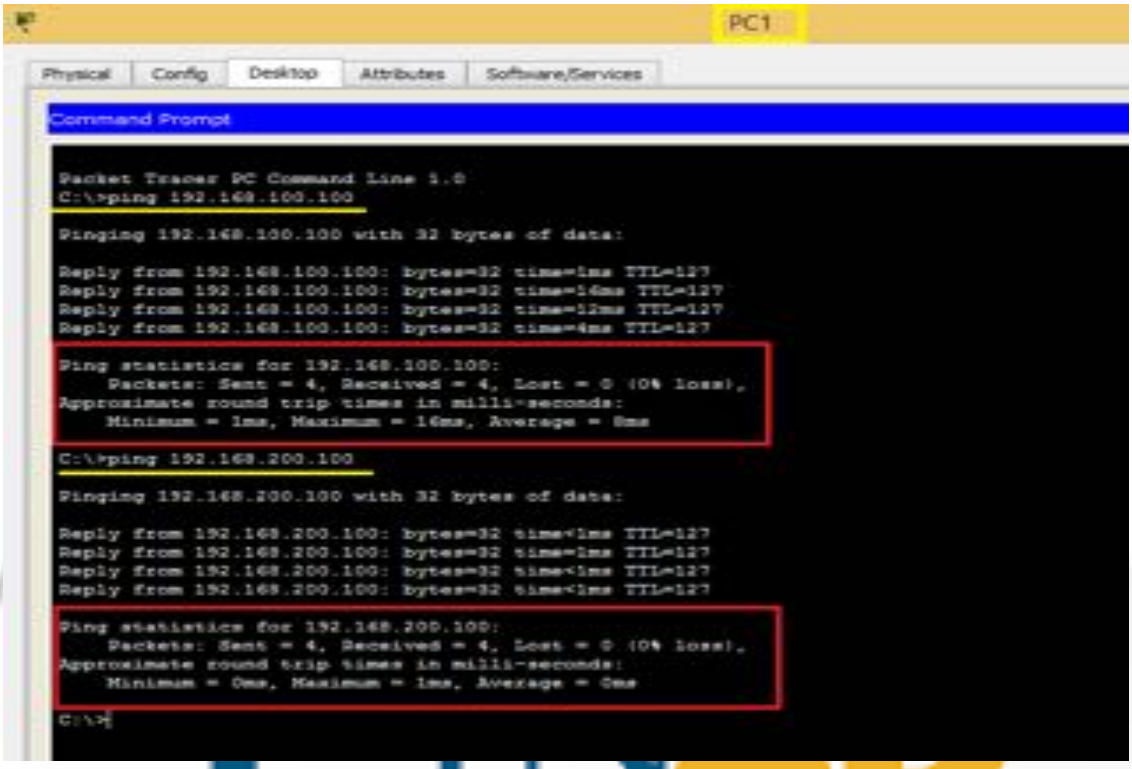
El administrador de red sénior le solicitó que cree una ACL estándar con nombre para impedir el acceso a un servidor de archivos. Se debe denegar el acceso de todos los clientes de una red y de una estación de trabajo específica de una red diferente

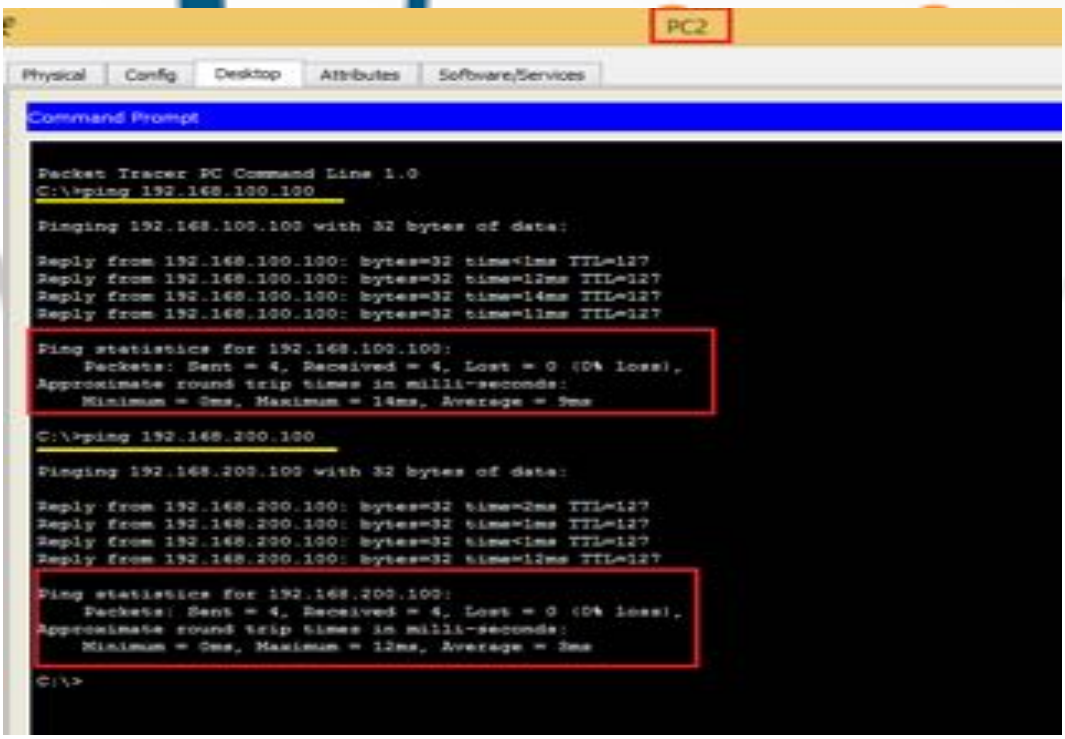
Parte 1: Configurar y aplicar una ACL estándar con nombre

Paso 1: Verificar la conectividad antes de configurar y aplicar la ACL.

Las tres estaciones de trabajo deben poder hacer ping tanto al Servidor web como al Servidor de archivos




PC1
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=16ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=4ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 16ms, Average = 8ms
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<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 = 1ms, Average = 0ms
C:\>


PC2
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.100
Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=12ms TTL=127
Reply from 192.168.100.100: bytes=32 time=14ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127
Ping statistics for 192.168.100.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 9ms
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=2ms 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=12ms 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 = 12ms, Average = 3ms
C:\>

Paso 2: Configurar una ACL estándar con nombre

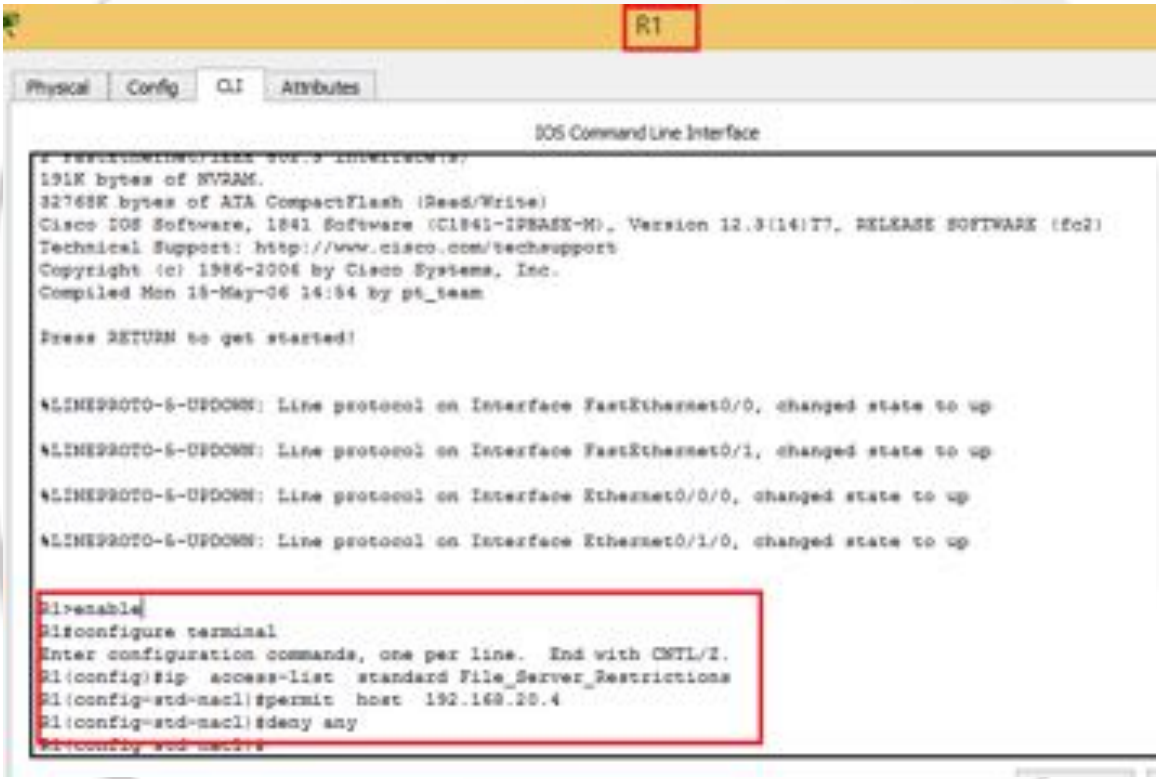
Configure la siguiente ACL con nombre en el R1.

R1(config)# ip access-list standard File_Server_Restrictions

R1(config-std-nacl)# permit host 192.168.20.4

R1(config-std-nacl)# deny any

Nota: a los fines de la puntuación, el nombre de la ACL distingue mayúsculas de minúsculas.



Paso 3: Aplicar la ACL con nombre.

a. Aplique la ACL de salida a la interfaz Fast Ethernet 0/1.

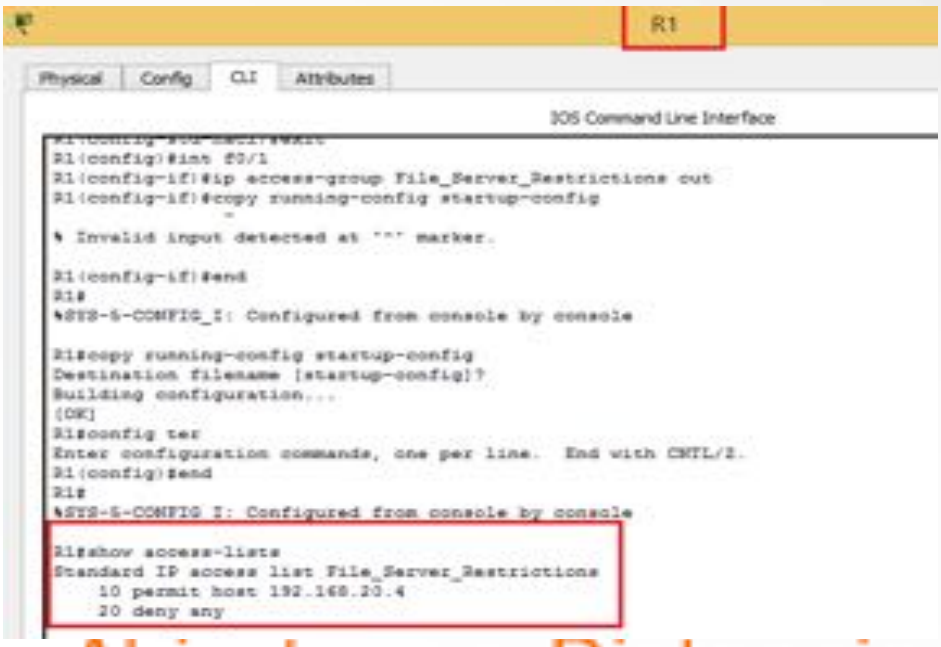
R1(config-if)# ip access-group File_Server_Restrictions out

b. Guarde la configuración.

Parte 2: Verificar la implementacion de la ACL

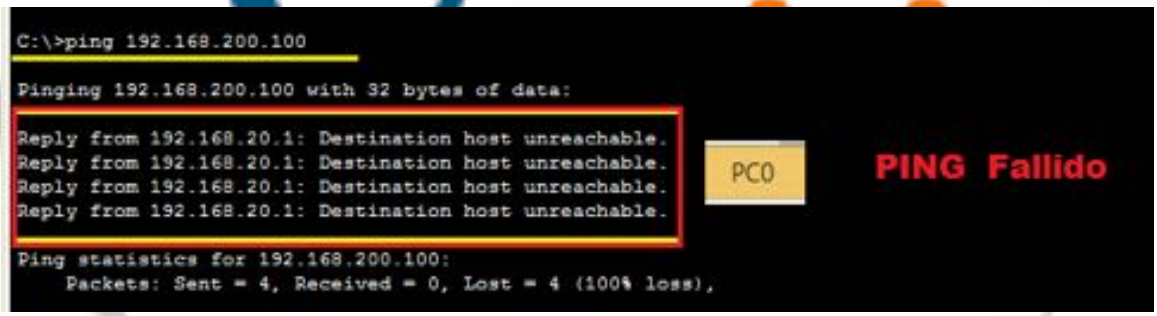
Paso 1: Verificar la configuracion de la ACL y su aplicación a la interfaz

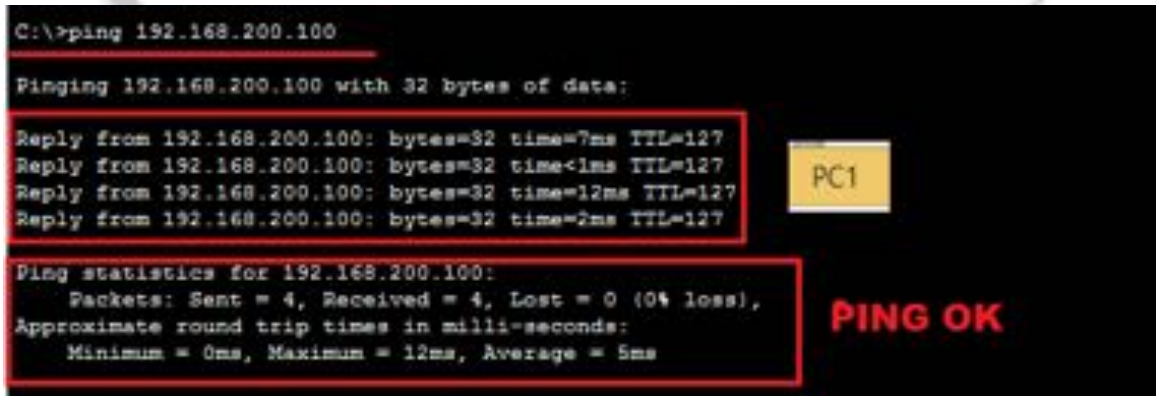
Utilice el comando *show access-lists* para verificar la configuración de la ACL. Utilice el comando *show run* o *show ip interface fastethernet 0/1* para verificar que la ACL se haya aplicado de forma correcta a la interfaz.

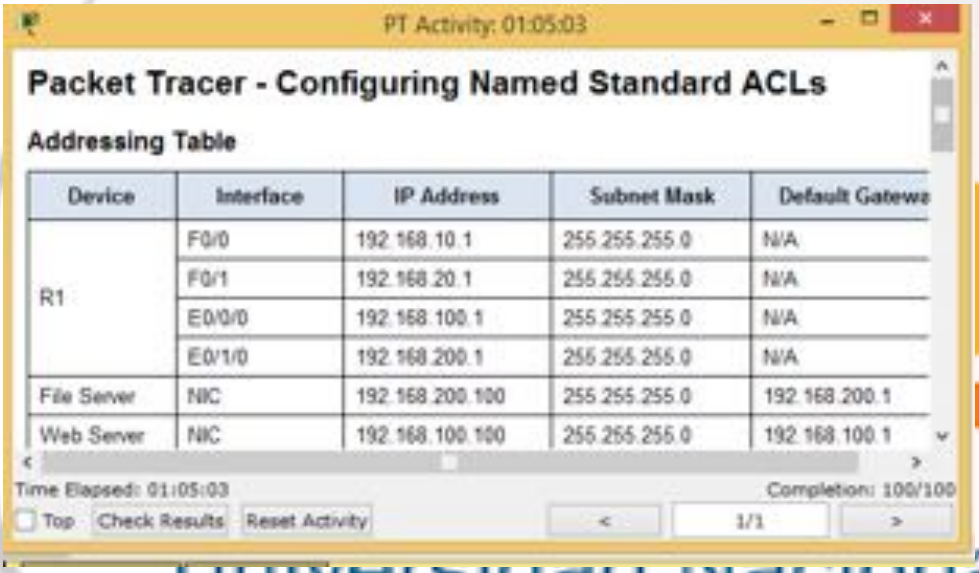


Paso 2: verificar que la ACL funcione correctamente.

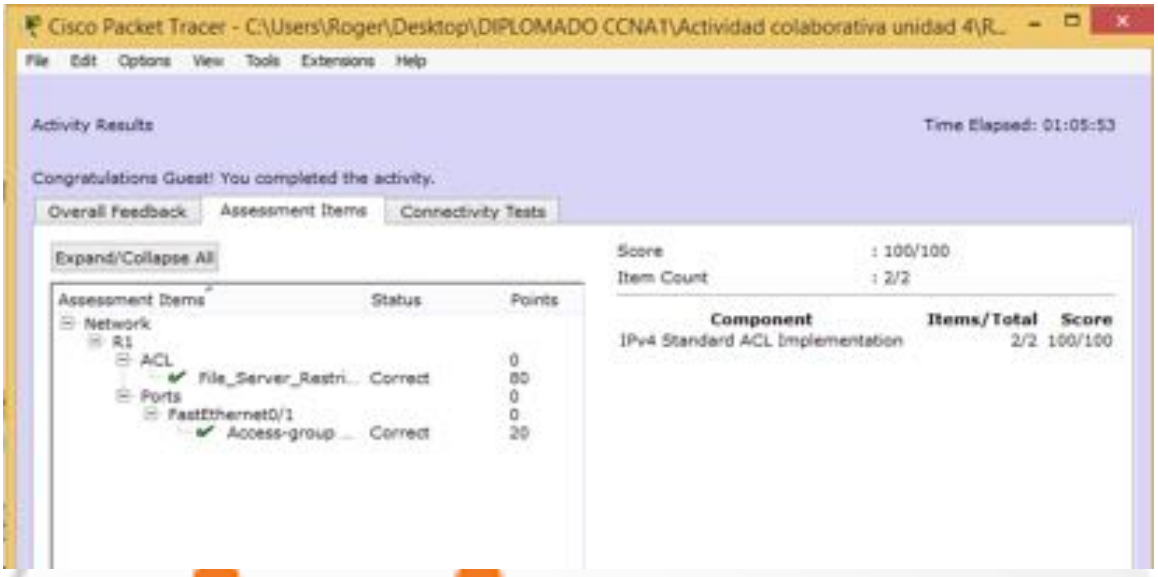
Aunque las tres estaciones de trabajo deberían poder hacer ping al servidor web, pero sólo PC1 debería poder hacer ping al servidor web.







Universidad Nacional
Abierta y a Distancia



Informe 13

Práctica .9.2.3.3 Configuración de ACL el líneas VTY

Topología

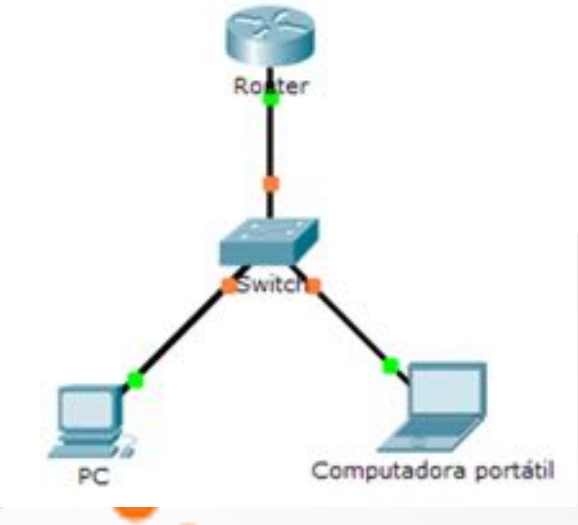


Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Router	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Computadora portátil	NIC	10.0.0.2	255.0.0.0	10.0.0.254

Objetivos

Parte 1: Configurar y aplicar una ACL a las líneas VTY

Parte 2: Verificar la implementación de la ACL

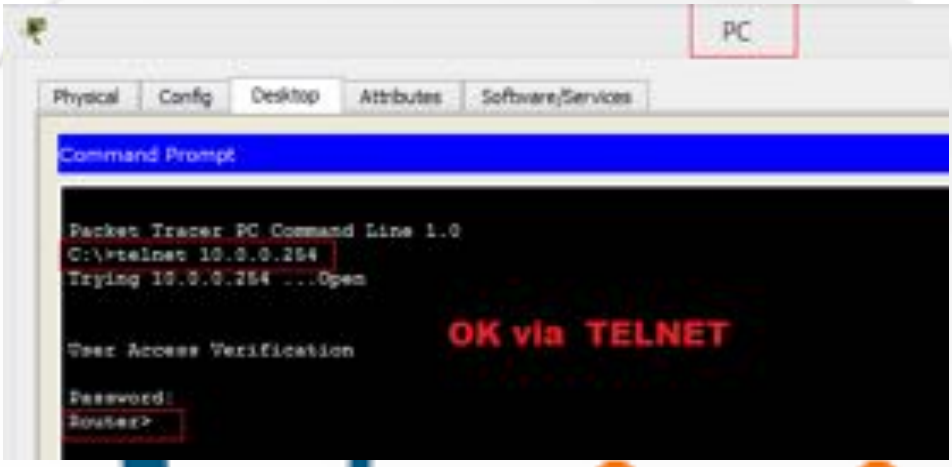
Información Básica

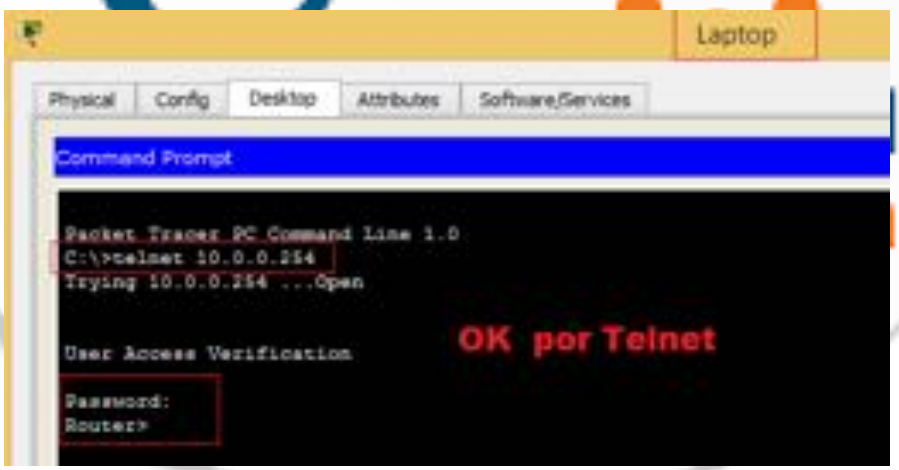
Como administrador de red, debe tener acceso remoto al router. Este acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, configurará y aplicará una lista de control de acceso (ACL) que permita el acceso de una computadora (PC) a las líneas Telnet, pero que deniegue el resto de las direcciones IP de origen.

Parte 1: Configurar y aplicar una ACLa las líneas VTY

Paso 1: Verificar el acceso por Telnet antes de configurar la ACL

Ambas computadoras deben poder acceder al Router mediante Telnet. La contraseña es cisco

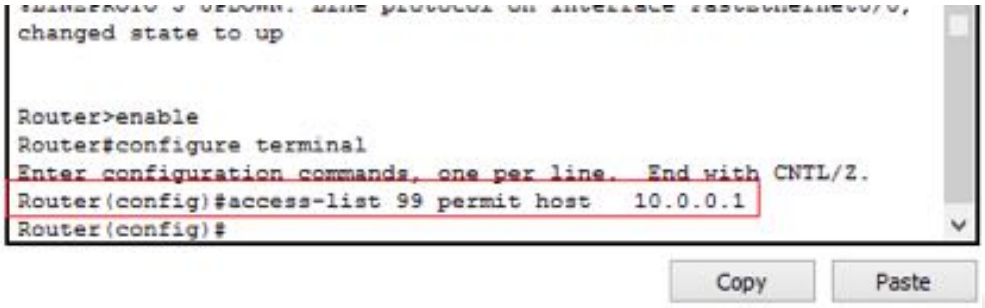




Paso 2: Configurar una ACL estándar numerada

Configure la siguiente ACL numerada en el Router.

Router(config)# access-list 99 permit host 10.0.0.1.



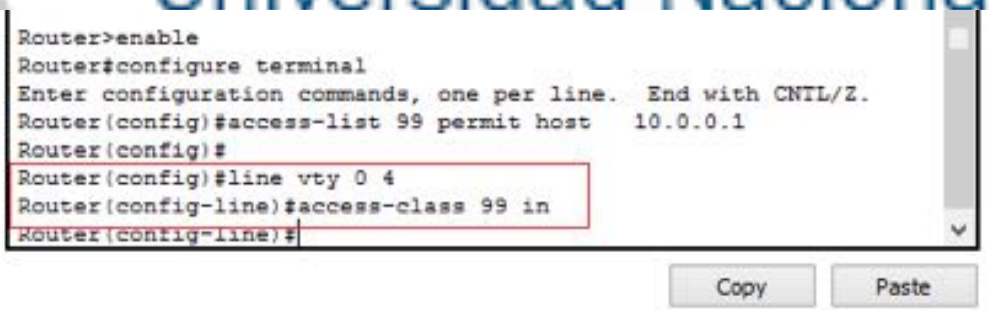
Ya que no deseamos permitir el acceso desde ninguna otra computadora, la propiedad de denegación implícita de la lista de acceso cumple nuestros requisitos.

Paso 3: Colocar una ACL estándar con nombre en el router.

Se debe permitir el acceso a las interfaces del Router y se debe restringir el acceso por Telnet. Por lo tanto, debemos colocar la ACL en las líneas Telnet que van de 0 a 4. Desde la petición de entrada de configuración del Router, acceda al modo de configuración de línea de las líneas 0 a 4 y utilice el comando access-class para aplicar la ACL a todas las líneas VTY:

Router (config) # line vty 0 4

Router (config-line) # access-class 99 in



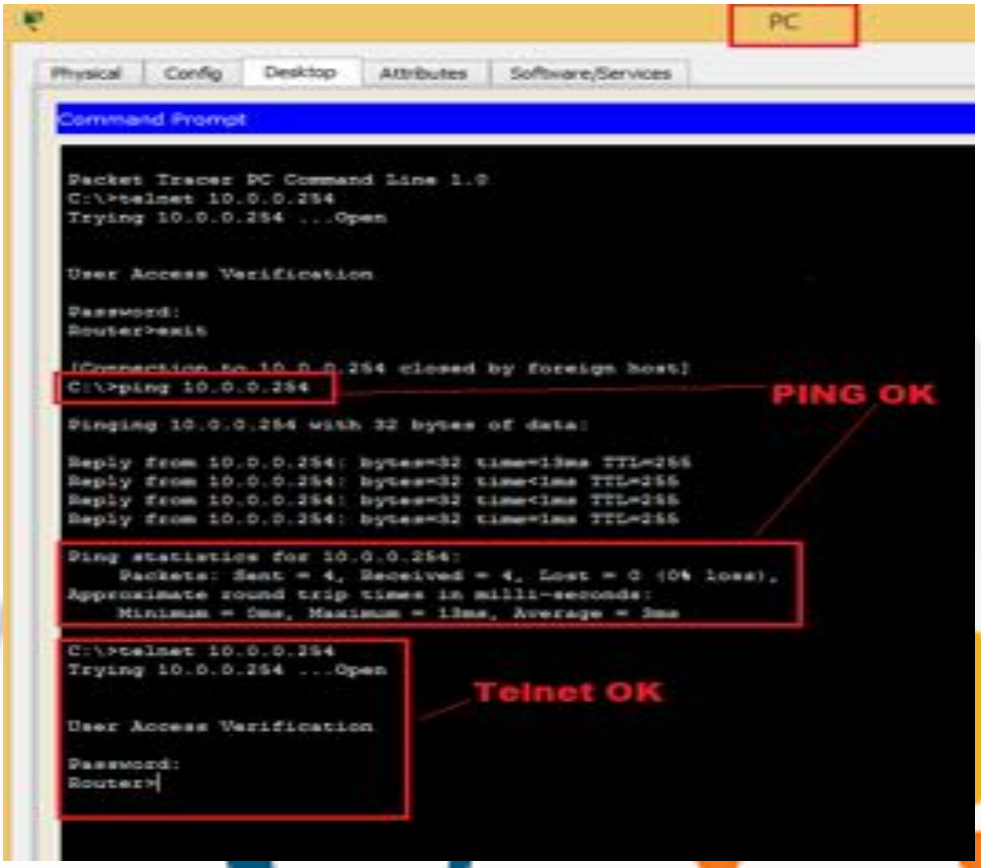
Parte 2: Verificar la implementación de la ACL

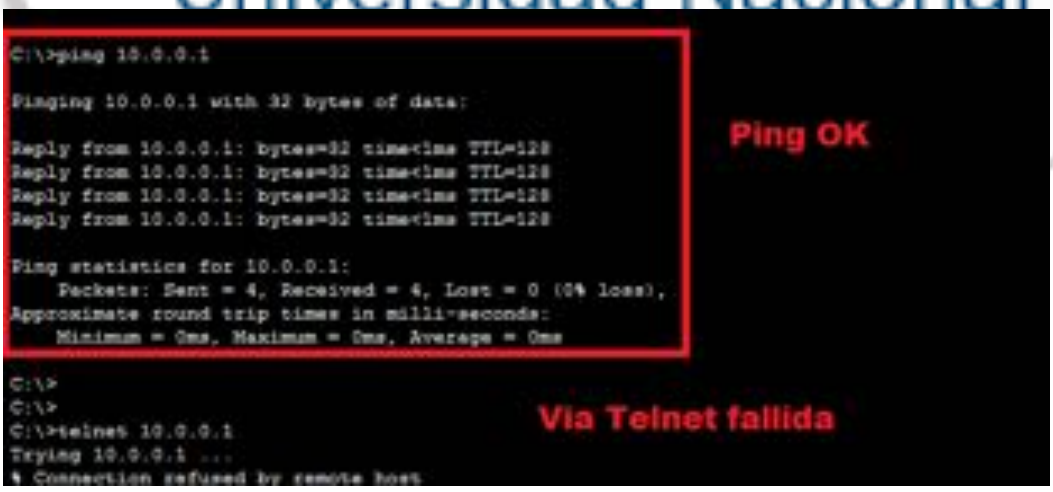
Paso 1: Verificar el acceso por Telnet antes de configurar la ACL

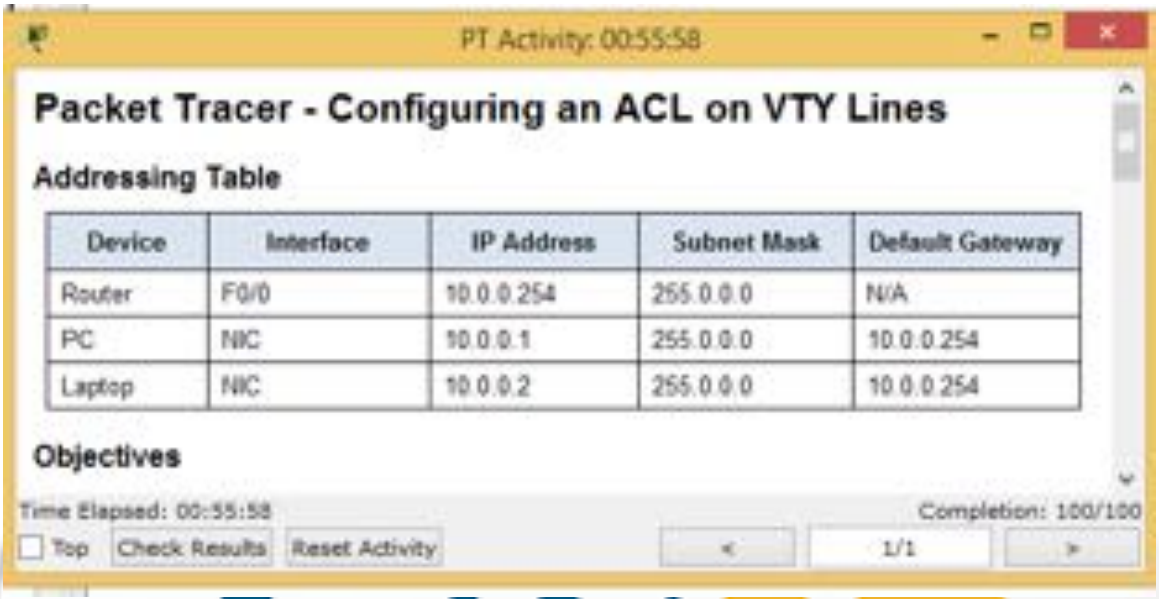
Utilice el comando *show access-lists* para verificar la configuración de la ACL. Utilice el comando *show run* para verificar que la ACL esté aplicada a las líneas VTY.

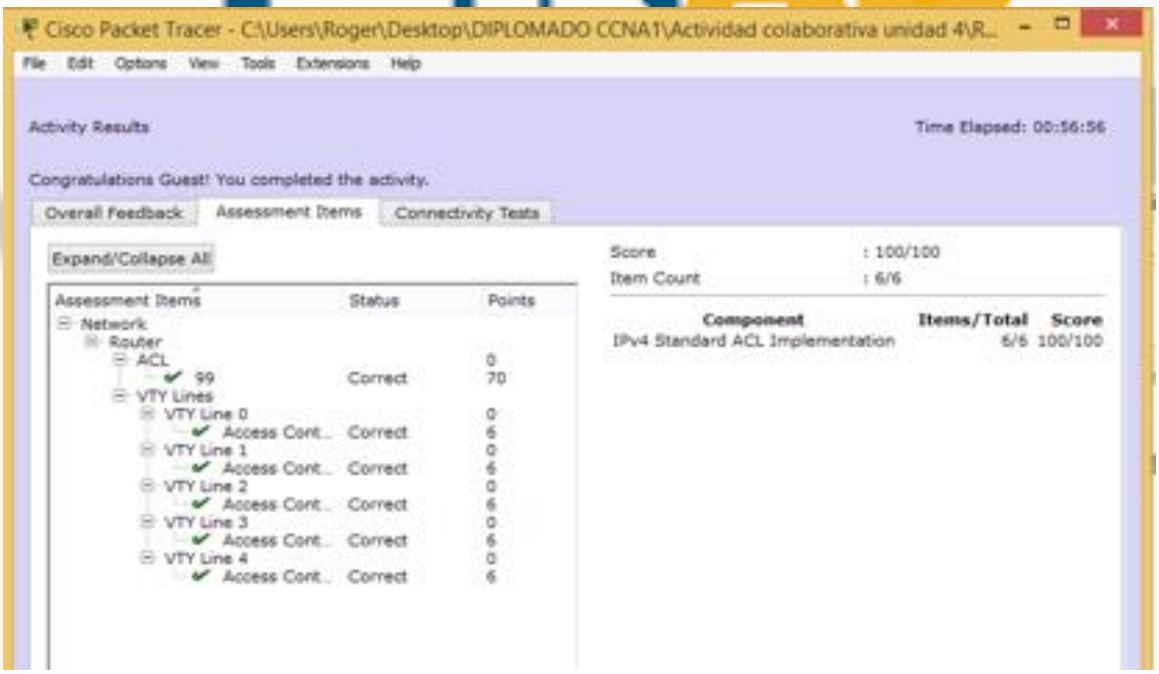
Paso 2: Verificar que la ACL funcione correctamente.

Ambas computadoras deben poder hacer ping al Router, pero solo la computadora PC debería poder acceder al Router mediante Telnet.






PT Activity: 00:55:58
Packet Tracer - Configuring an ACL on VTY Lines
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
Time Elapsed: 00:55:58
Completion: 100/100
Top
Check Results
Reset Activity
1/1


Cisco Packet Tracer - C:\Users\Roger\Desktop\DIPLOMADO CCNA1\Actividad colaborativa unidad 4\R...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:56:56
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items | Status | Points
Network
Router
ACL 0
99 Correct 70
VTY Lines
VTY Line 0 0
Access Cont... Correct 6
VTY Line 1 0
Access Cont... Correct 6
VTY Line 2 0
Access Cont... Correct 6
VTY Line 3 0
Access Cont... Correct 6
VTY Line 4 0
Access Cont... Correct 6
Score : 100/100
Item Count : 6/6
Component | Items/Total | Score
IPv4 Standard ACL Implementation 6/6 100/100

Informe 14

Práctica 9.5.2.6 Configuración de ACL de IPv6

Topología

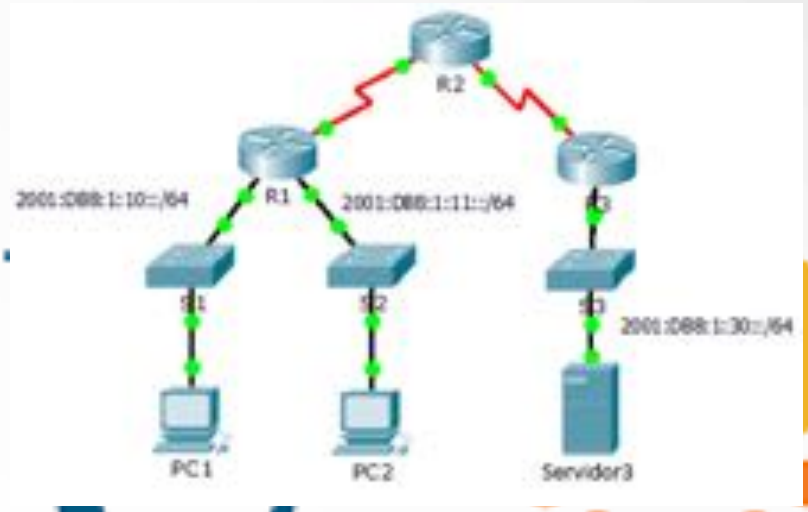


Tabla de Direccionamiento

Dispositivo	**Interfaz**	**Dirección/Prefijo IPv6**	**Gateway predeterminado**
Servidor3	NIC	2001:DB8:1:30::30/64	FE80::30

Objetivos

Parte 1: Configurar, aplicar y verificar una ACL de IPv6

Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

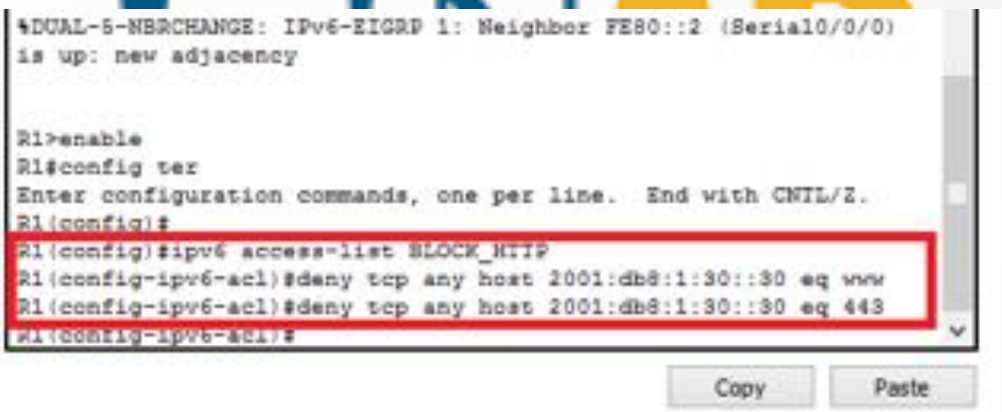
Parte 1: Configurar, aplicar y verificar una ACL de IPv6

Según los registros, una computadora en la red 2001:DB8:1:11::0/64 actualiza repetidamente su página web, lo que ocasiona un ataque por denegación de servicio (DoS) contra el Servidor3. Hasta que se pueda identificar y limpiar el cliente, debe bloquear el acceso HTTP y HTTPS a esa red mediante una lista de acceso.

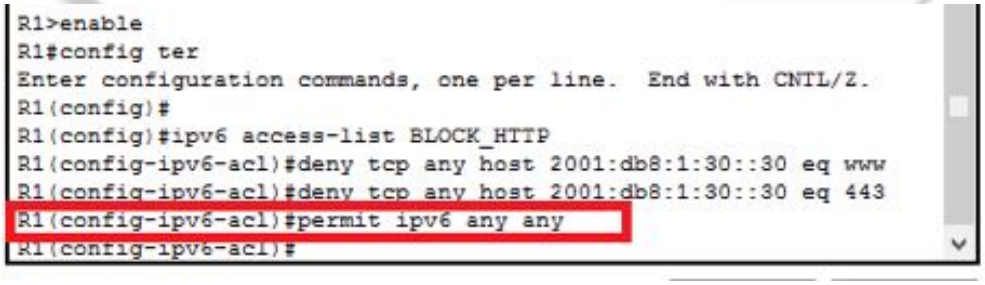
Paso 1: configurar una ACL que bloquee el acceso HTTP y HTTPS.

Configure una ACL con el nombre BLOCK_HTTP en el R1 con las siguientes instrucciones.

a) Bloquear el tráfico HTTP y HTTPS para que no llegue al Servidor3.
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443



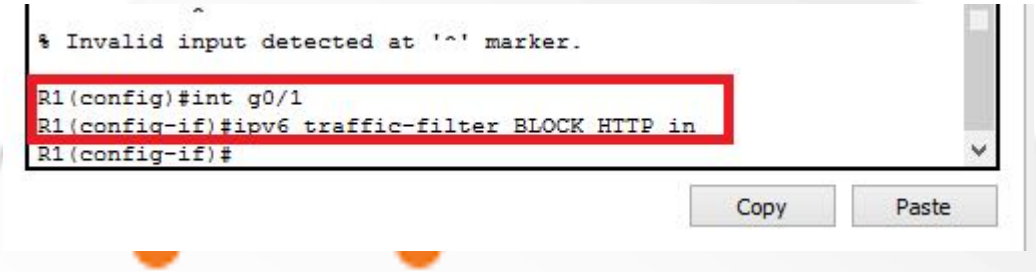
b) Permitir el paso del resto del tráfico IPv6.
R1(config)# permit ipv6 any any



Paso 2: aplicar la ACL a la interfaz correcta.

Aplique la ACL a la interfaz más cercana al origen del tráfico que se desea bloquear.

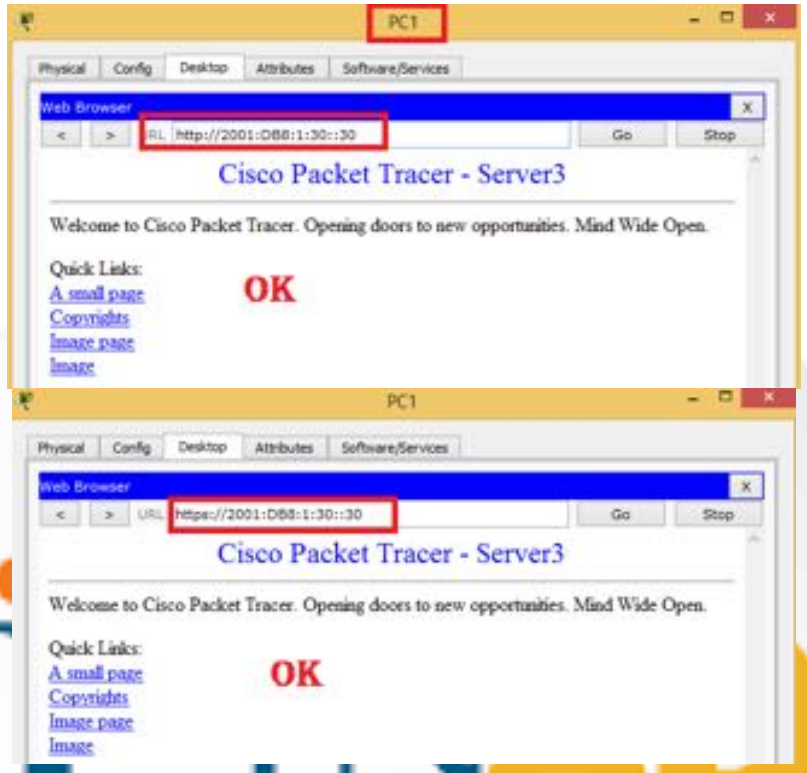
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in



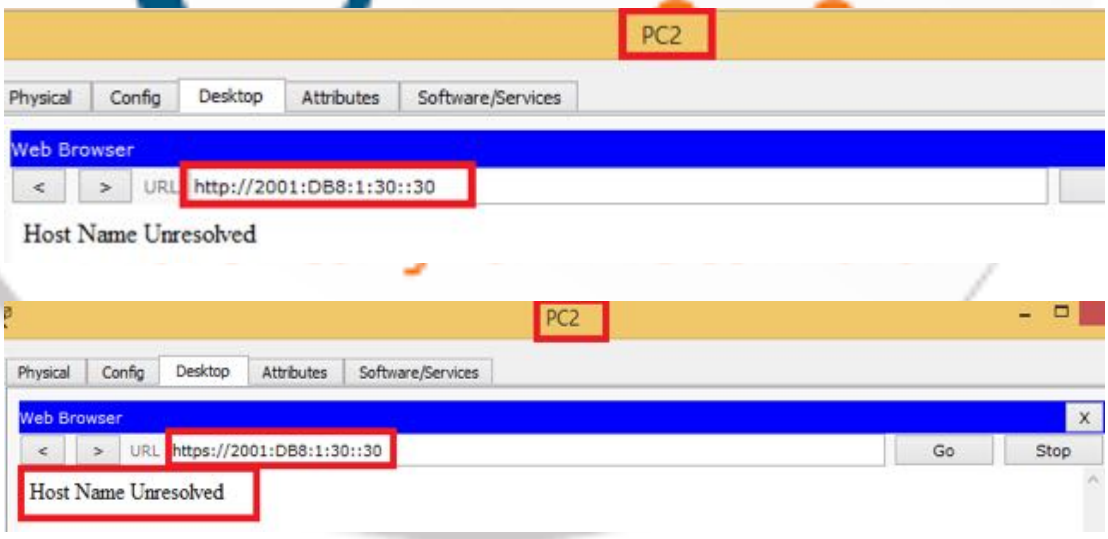
Paso 3: verificar la implementación de la ACL.

Realice las siguientes pruebas para verificar que la ACL funcione de manera correcta:

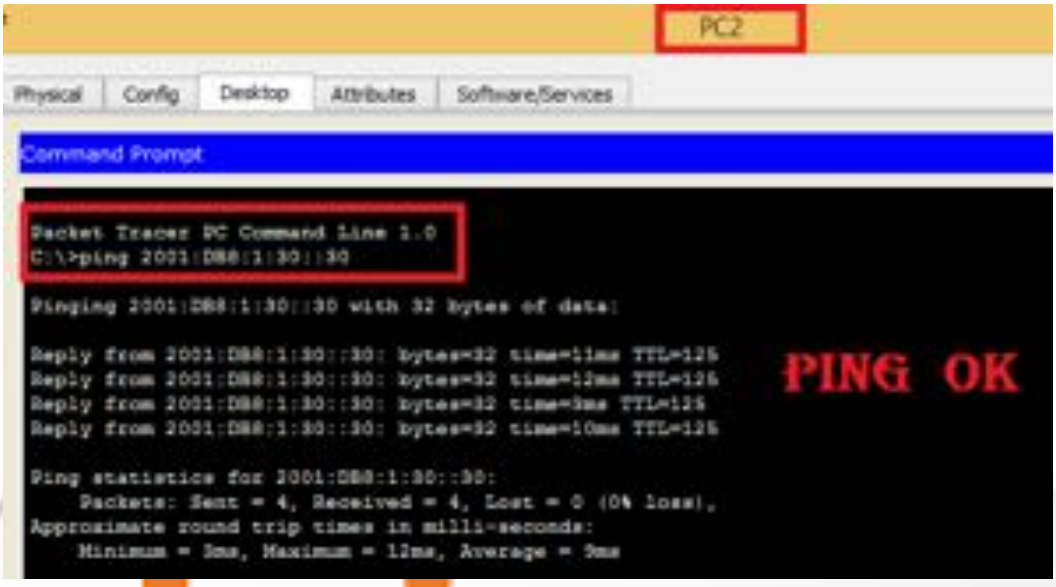
a) Abra el navegador web de la PC1 con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. Debería aparecer el sitio web.



b) Abra el navegador web de la PC2 con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. El sitio web debería estar bloqueado.



c) Haga ping de la PC2 a 2001:DB8:1:30::30. El ping debería realizarse correctamente.



Parte 2: Configurar, aplicar y verificar una segunda ACL de IPv6

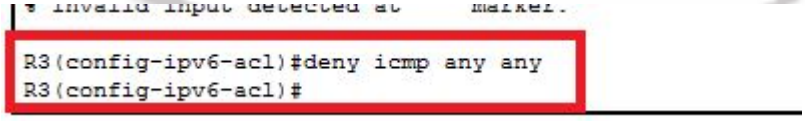
Ahora, en los registros se indica que su servidor recibe pings de diversas direcciones IPv6 en un ataque por denegación de servicio distribuido (DDoS). Debe filtrar las solicitudes de ping ICMP a su servidor.

Paso 1: crear una lista de acceso para bloquear ICMP.

Configure una ACL con el nombre BLOCK_ICMP en el R3 con las siguientes instrucciones:

a) Bloquear todo el tráfico ICMP desde cualquier host hasta cualquier destino.

R3(config)# deny icmp any any



b) Permitir el paso del resto del tráfico IPv6.

R3(config)# permit ipv6 any any

```
% Invalid input detected at '^' marker.

R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
```

Paso 2: aplicar la ACL a la interfaz correcta.

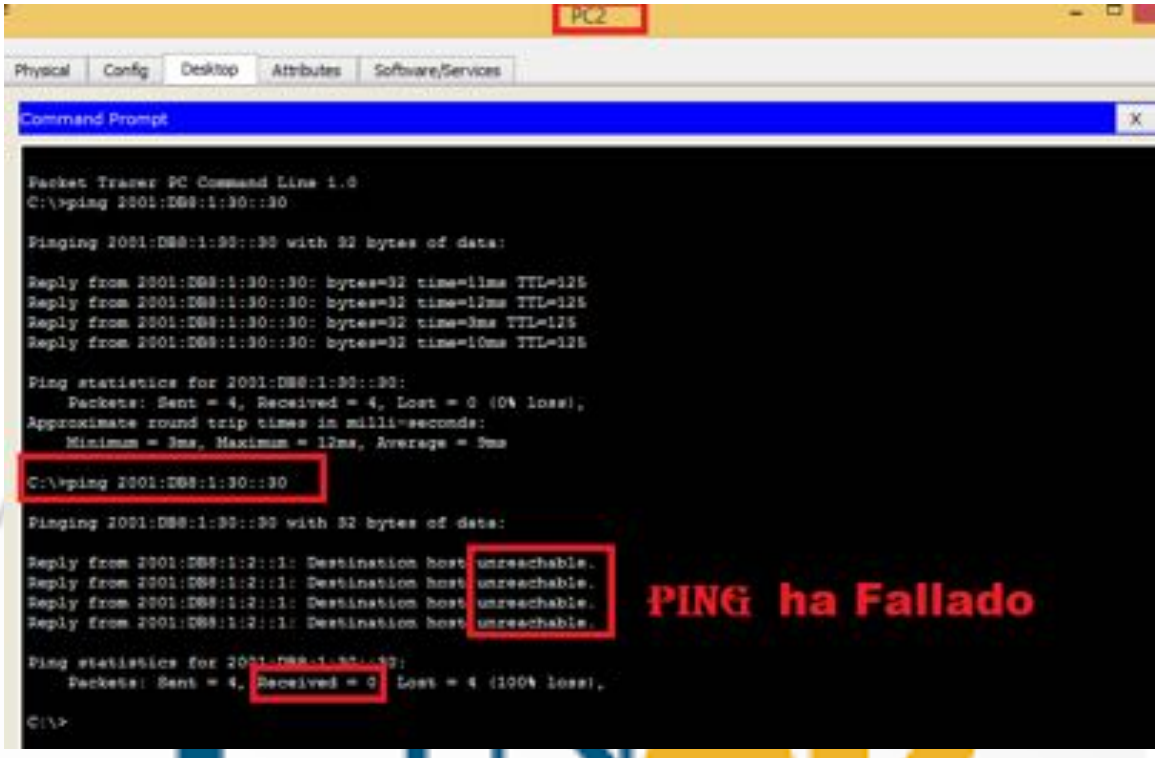
En este caso, el tráfico ICMP puede provenir de cualquier origen. Para asegurar que el tráfico ICMP esté bloqueado, independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL lo más cerca posible del destino.

R3(config)# interface GigabitEthernet0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out

```
R3#enab
R3#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traff
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

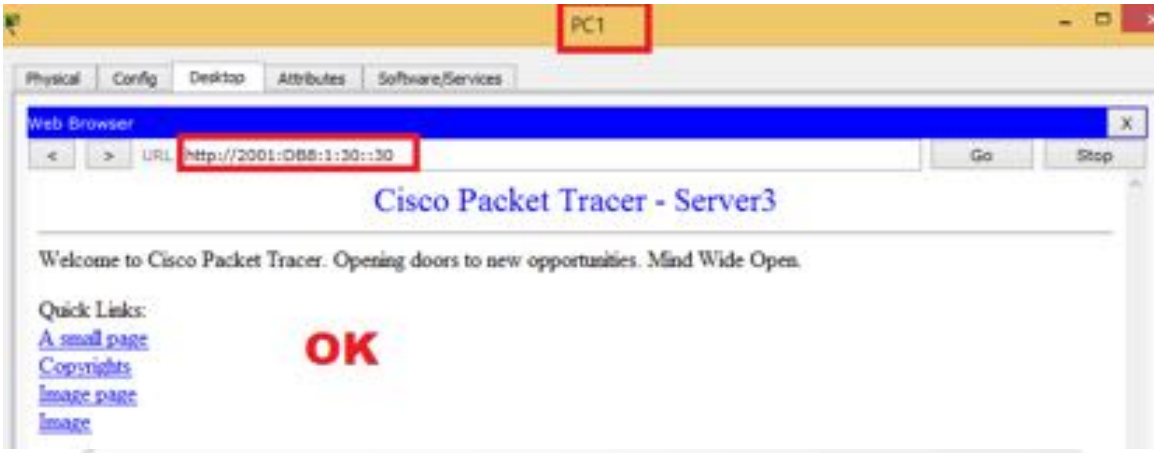
Paso 3: verificar que la lista de acceso adecuada funcione.

a) Haga ping de la PC2 a 2001:DB8:1:30::30. *El ping debe fallar.*

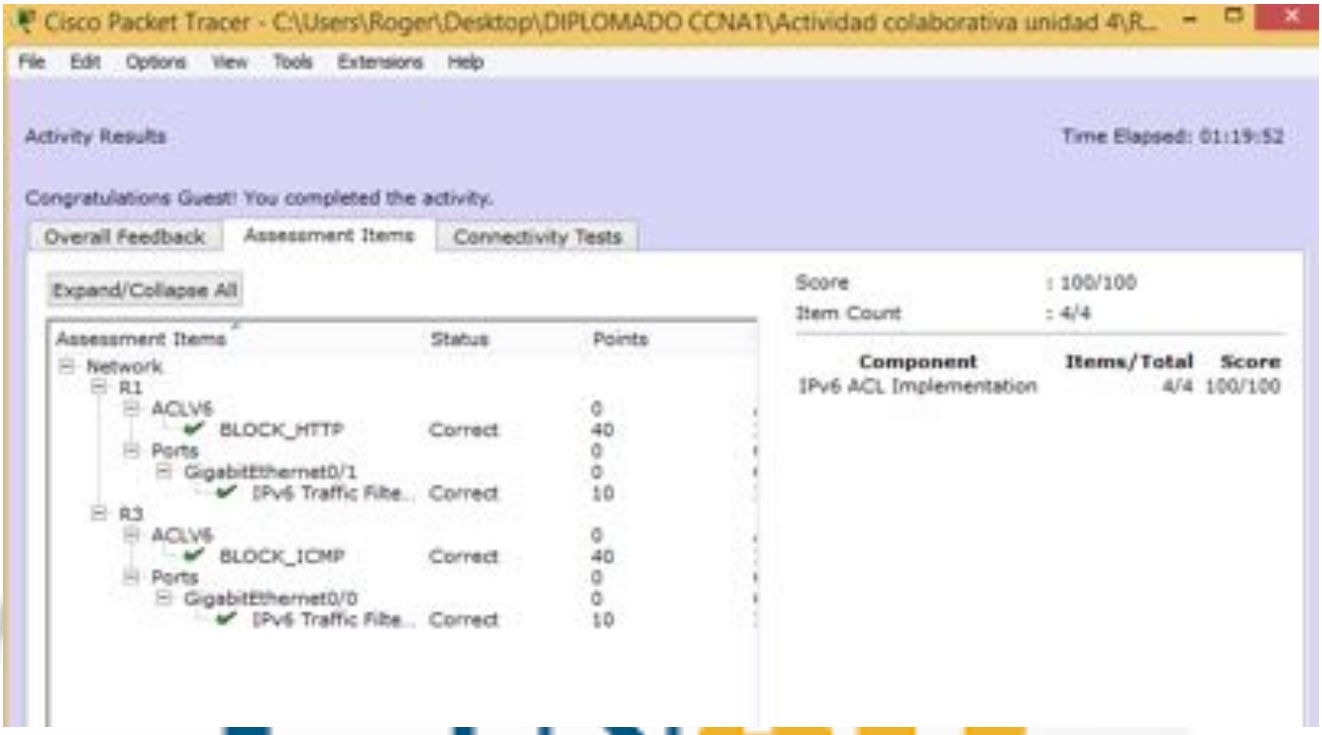


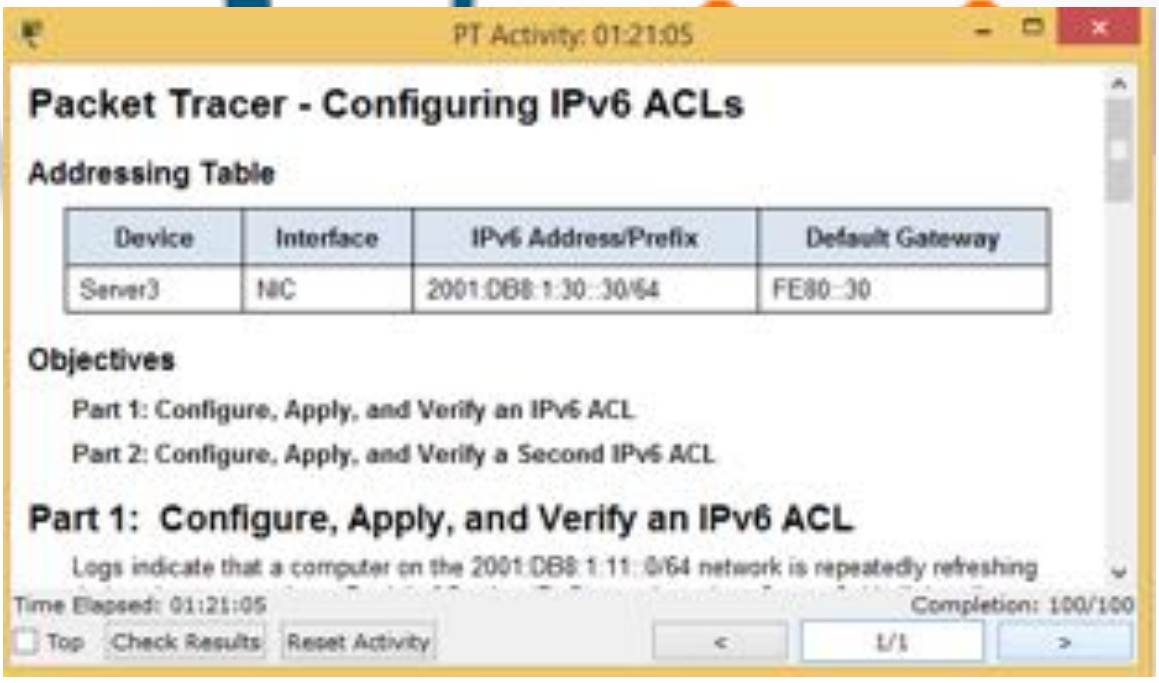
b) Haga ping de la PC1 a 2001:DB8:1:30::30. *El ping debe fallar.*

Abra el navegador web de la PC1 con la dirección http://2001:DB8:1:30::30 o https://2001:DB8:1:30::30. *Debería aparecer el sitio web.*



Universidad Nacional
Abierta y a Distancia


Cisco Packet Tracer - C:\Users\Roger\Desktop\DIPLOMADO CCNA1\Actividad colaborativa unidad 4\R...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:19:52
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Score : 100/100
Item Count : 4/4
Assessment Items
Status
Points
Network
R1
ACLV6 0
BLOCK_HTTP Correct 40
Ports 0
GigabitEthernet0/1 0
IPv6 Traffic Filte... Correct 10
R3
ACLV6 0
BLOCK_ICMP Correct 40
Ports 0
GigabitEthernet0/0 0
IPv6 Traffic Filte... Correct 10
Component
Items/Total
Score
IPv6 ACL Implementation 4/4 100/100


PT Activity: 01:21:05
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
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
Time Elapsed: 01:21:05
Completion: 100/100
Top
Check Results
Reset Activity
<
1/1
>

Conclusiones

Después de haber culminado este último trabajo colaborativo, los integrantes concluimos que las prácticas realizadas en los anteriores trabajos colaborativos fueron base imprescindible para organizar y desarrollar el presente informe de CNNA2, el cual desarrolló en nosotros competencias de carácter analítico, orientadas a la comprensión y formulación de hipótesis para la solución de situaciones propias del campo de las redes y las telecomunicaciones, permitiéndonos conocer la aplicabilidad de múltiples comandos, instrucciones y situaciones que sentaran las bases para seguir avanzando en este maravilloso campo.

El desarrollo de competencias cognitivas nos llevaron al establecimiento y reafirmación de nuevos y viejos conceptos frente a los temas objeto de estudio, de gran importancia para la comprensión e interpretación de las situaciones plasmadas en cada uno de los laboratorios del presente informe, los cuales aumentaron nuestros conocimientos sobre los diferentes temas estudiados referente a CNNA2, que a su vez de una u otra forma serán aplicado en un determinado momento de nuestra vida laboral.

- Hacer un uso eficaz del material de apoyo para poder realizar la actividad.
- Realizar configuración de Switches para su correcto funcionamiento.
- Asignar ip y demás configuraciones de manera adecuada utilizando los programas sugeridos en la guía de actividades.
- Trabajar en equipo para para obtener un mayor conocimiento y complementar ideas.
- Se Explicó el funcionamiento de los protocolos de routing dinámico.

- Aprendimos a configurar los parámetros básicos de los dispositivos, configurar y verificar el routing RIPv2, configurar IPv6 en los dispositivos, configurar y verificar el routing RIPng.

- Se analizó la tabla de routing para determinar el origen de la ruta, la distancia administrativa y la métrica de una ruta determinada para incluir IPv4/IPv6.

- Aprendimos a armar configurar los parámetros básicos de los dispositivos, configurar y verificar el routing OSPF, cambiar las asignaciones de ID del router, configurar interfaces OSPF pasivas, cambiar las métricas de OSPF.

- Se pudo comprobar cómo las ACLs nos brindan un sin número de herramientas de seguridad para el manejo de nuestras redes y así impedir que personas ajenas a nuestra puedan causarnos daños a la infraestructura de la misma.

- Comprobamos las grandes ventajas que proporciona el poder poner un servidor dhcp en nuestros switches y routers para el momento de generar direcciones IP ya que en un futuro cercano todos nuestros equipos tendrán direcciones IP y hacer esto de manera estática sería un proceso muy largo. Además colocar direccionamiento DHCP en IPv4 e IPv6 es un proceso muy similar.

- Se identificó como NAT es una manera de proteger nuestras redes ya que de alguna manera protege nuestras direcciones IP.

- NAT provee una solución temporal al agotamiento de direcciones IPv4 ya que permite desde una IP publica al momento de acceder a un servidor y/o red, que dicha IP se traduzca en una dirección IP privada y así acceder a todos los servicios como si perteneciera a dicha red sin tener que hacer un enrutamiento largo y pedir permisos de administración.


UNAD
Universidad Nacional
Abierta y a Distancia

Referencias Bibliográficas

- Juan Carlos Vesga F. (2017), Diplomado de Profundización Cisco. Modulo en Línea CCNA1 Introducción a las Redes. Escuela de Ciencias Básicas Tecnologías e Ingenierías. UNAD. Bogotá Colombia.

- Cortez Fernández, R. (2011). Convergencia en el hogar, el futuro nos alcanza. Revista La Razón. Recuperado Mayo del 2017 de http://razon.com.mx/spip.php?article79429

- Natuchita. (2011). Que es Convergencia Tecnológica. Slideshare. Recuperado Mayo del 2017 de http://es.slideshare.net/natuchita/qu-es-convergencia-tecnolgica

- Wikipedia. (2014). Proveedor de servicios de internet. Wikipedia. Recuperado Mayo del 2017 de http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

- Temboury, M. (2008). Que entendemos por convergencia. Nota Enter-IE. Recuperado Mayo del 2017 de https://www.mtc.gob.pe/portal/consultas/cid/Boletines_CID/29_diciembre/ARCHIVO/c onvergencia%20digital.pdf

- Ecured. (2008). IANA. Ecured. Recuperado Mayo del 2017 de http://www.ecured.cu/index.php/IANA

- Wikipedia. (2015). ICANN. Wikipedia. Recuperado Mayo del 2017 de http://es.wikipedia.org/wiki/ICANN

- E-Centro. (2014). Vinton Cerf, Carreras premios y honores. E-Centro. Recuperado Mayo del 2017 de http://centrodeartigos.com/articulosenciclopedicos/article_92769.html

- W3C. (2014). Sobre el W3C. W3C. Recuperado Mayo del 2017 de http://www.w3c.es/Consorcio/about-w3c.html

- Cooper Stephen, B. (2014). Que es un cable RS-232. E-how. Recuperado Mayo del 2017 de http://www.ehowenespanol.com/cable-rs232c-info_206935/

- Chambers John. (2012). Internet of Everything: Fueling an Amazing Future # TomorrowStartsHere. Cisco Blogs. Recuperado Mayo del 2017 de http://blogs.cisco.com/news/internet-of-everything-2

- Chambers John. (2012). Cisco Tomorrow Starts Here. Cisco Blogs. Recuperado Mayo de 2017 de http://www.cisco.com/web/tomorrow-starts-here/index.html

- Ericsson Social Media. (2014). Connected Tree. Ericsson Company. Recuperado Mayo de 2017 de http://www.ericsson.com/article/connected_tree_2045546582_c

- Edic College. (2014). Políticas de uso redes "PEER TO PEER". Edic College. Recuperado Mayo de 2017 de http://www.ediccollege.com/upload/pdf/Politica_de_uso_de_redes_peer_to_peer.pdf

- Baladia Guillerm. (2014). Los programas informáticos P2P y las nuevas perspectivas. Scripta Nova, Revista electrónica de Geografía y ciencias sociales. Recuperado Mayo de 2017 de http://www.ub.edu/geocrit/sn/sn-170-54.htm

- Ruiz Zapatero Guillermo. (2014). Artículos Doctrinales: Derecho Informático. Noticias Jurídicas. Recuperado Mayo de 2017 de http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200705425232565212542125452.html

- En Hacke. (2014). Conexiones 4g multiplican la presencia de Malware. En Hacke. Recuperado Mayo de 2017 de http://www.enhacke.com/tag/virus-informaticos/