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

APORTES COLABORATIVO 3
203092_47

OSCAR ALFONSO CLAVIJO MORALES
CÓDIGO: 13958937

TUTOR:
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PROGRAMA DE INGENIERÍA ELECTRÓNICA
2018

INTRODUCCIÓN

El contenido de este documento tiene como fin desarrollar los ejercicios prácticos de la actividad colaborativa 3 del Diplomado de Profundización Cisco respecto a la guía de actividades entregada por la UNAD en el entorno colaborativo aplicando los conceptos aprendidos en el curso en línea

El desarrollo de los diferentes ejercicios nos ayudara a mejorar las competencias mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces.

Adicional a esto se desarrollaron simulaciones de cada uno de los ejercicios propuestos en el simulador PACKET TRACER.

La solución de estos ejercicios nos brindara un conocimiento en el uso de comandos de configuración ya que con las simulaciones aprendemos a usarlos correctamente, así como los niveles de seguridad que se pueden configurar para diseñar soluciones tecnológicas innovadoras para satisfacer las necesidades de las compañías.

OBJETIVOS

Objetivo general

Comprender de manera práctica los conceptos aprendidos en los diferentes capítulos de la plataforma virtual de CISCO.

Objetivos específicos

- Comprender mediante simulaciones el uso de los diferentes comandos de configuración.
- Realizar las practicas propuestas mediante el simulador PACKET TRACER.

6.4.2.5 Lab - Calculating Summary Routes with IPv4 and IPv6

Topología

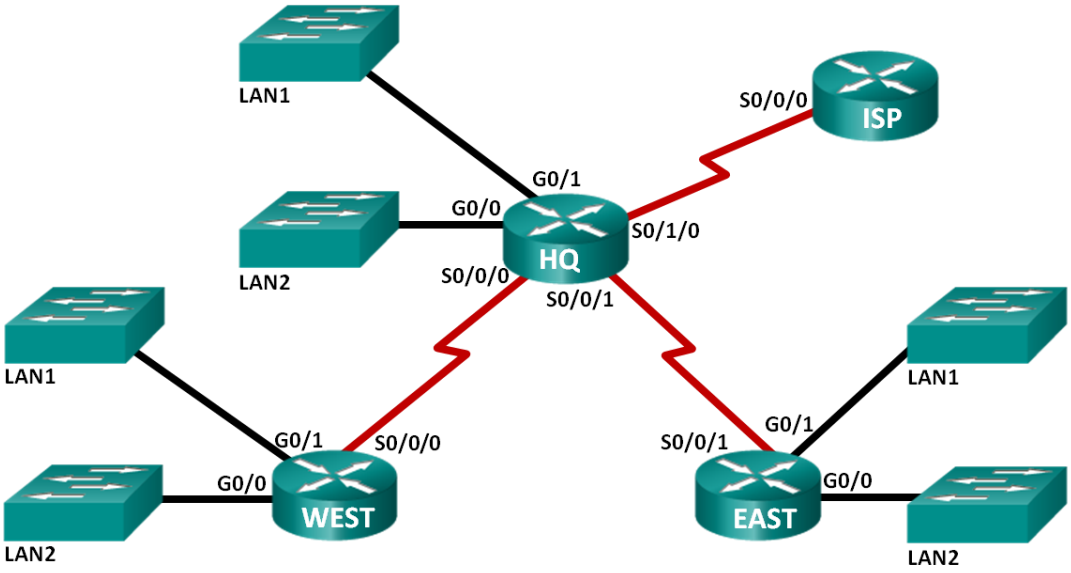


Tabla de direccionamiento

Subred	Dirección IPv4	Dirección IPv6
LAN1 de HQ	192.168.64.0/23	2001:DB8:ACAD:E::/64
LAN2 de HQ	192.168.66.0/23	2001:DB8:ACAD:F::/64
LAN1 de EAST	192.168.68.0/24	2001:DB8:ACAD:1::/64
LAN2 de EAST	192.168.69.0/24	2001:DB8:ACAD:2::/64
LAN1 de WEST	192.168.70.0/25	2001:DB8:ACAD:9::/64
LAN2 de WEST	192.168.70.128/25	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	192.168.71.4/30	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	192.168.71.0/30	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	209.165.201.0/30	2001:DB8:CC1E:1::/64

Objetivos

Parte 1: calcular rutas resumidas IPv4

- Determinar la ruta resumida para las LAN de HQ.
- Determinar la ruta resumida para las LAN ESTE.
- Determinar la ruta resumida para las LAN OESTE.
- Determinar la ruta resumida para las LAN de HQ, ESTE y OESTE.

Parte 2: calcular rutas resumidas IPv6

- Determinar la ruta resumida para las LAN de HQ.
- Determinar la ruta resumida para las LAN ESTE.
- Determinar la ruta resumida para las LAN OESTE.
- Determinar la ruta resumida para las LAN de HQ, ESTE y OESTE.

Información básica/situación

Las rutas resumidas reducen el número de entradas en las tablas de routing y hacen que el proceso de búsqueda en dichas tablas sea más eficaz. Este proceso también disminuye los requisitos de memoria del router. Se puede usar una sola ruta estática para representar unas pocas rutas o miles de rutas.

En esta práctica de laboratorio, determinará las rutas resumidas de diferentes subredes de una red. Después determinará la ruta resumida de toda la red. Determinará rutas resumidas para direcciones IPv4 e IPv6. Debido a que IPv6 usa valores hexadecimales, tendrá que convertir el valor hexadecimal en valor binario.

Recursos necesarios

- 1 computadora (Windows 7, Vista o XP, con acceso a Internet)
- Optativo: calculadora para convertir los valores hexadecimales y decimales en valores binarios

Parte 1. calcular rutas resumidas IPv4

En la parte 1, determinará las rutas resumidas que se pueden utilizar para reducir el tamaño de las tablas de routing. Después de cada conjunto de pasos, complete las tablas con la información apropiada de direccionamiento IPv4.

Paso 1. Indique la máscara de subred de la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato decimal.

Paso 2. Indique la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato binario.

Paso 3. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? **22**

b. Indique la máscara de subred para la ruta resumida en formato decimal.

Paso 4. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 de HQ y la LAN2 de HQ.

b. Agregue ceros para conformar el resto de la dirección de red en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de HQ	192.168.64.0	255.255.254.0	11000000.10101000.01000000.00000000
LAN2 de HQ	192.168.66.0	255.255.254.0	11000000.10101000.01000010.00000000
Dirección de resumen de las LAN de HQ	192.168.64.0	255.255.252.0	11000000.10101000.01000000.00000000

Paso 5. indicar la máscara de subred de la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato decimal.

Paso 6. indicar la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato binario.

Paso 7. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? **23**

b. Indique la máscara de subred para la ruta resumida en formato decimal.

Paso 8. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 ESTE y la LAN2 ESTE.

b. Agregue ceros para conformar el resto de la dirección de red en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección de subred en formato binario
LAN1 de EAST	192.168.68.0	255.255.255.0	11000000.10101000.01000100.00000000
LAN2 de EAST	192.168.69.0	255.255.255.0	11000000.10101000.01000101.00000000
Dirección de resumen de las LAN ESTE	192.168.68.0	255.255.254.0	11000000.10101000.01000100.00000000

Paso 9. indicar la máscara de subred de la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato decimal.

Paso 10. indicar la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato binario.

Paso 11. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? **24**

b. Indique la máscara de subred para la ruta resumida en formato decimal.

Paso 12. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 OESTE y la LAN2 OESTE.

b. Agregue ceros para conformar el resto de la dirección de red en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de WEST	192.168.70.0	255.255.255.128	11000000.10101000.01000110.00000000
LAN2 de WEST	192.168.70.128	255.255.255.128	11000000.10101000.01000110.00000000
Dirección de resumen de las LAN OESTE	192.168.70.0	255.255.255.0	11000000.10101000.01000110.00000000

Paso 13. indicar la dirección IP y la máscara de subred de la ruta resumida de HQ, ESTE y OESTE en formato decimal.

Paso 14. indicar la dirección IP de la ruta resumida de HQ, ESTE y OESTE en formato binario.

Paso 15. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres redes?

_____

b. Indique la máscara de subred para la ruta resumida en formato decimal.

Paso 16. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de HQ, ESTE y OESTE.

b. Agregue ceros para conformar el resto de la dirección de red en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
HQ	192.168.64.0	255.255.252.0	11000000.10101000.01000000.00000000
EAST	192.168.68.0	255.255.254.0	11000000.10101000.01000100.00000000
WEST	192.168.70.0	255.255.255.0	11000000.10101000.01000110.00000000
Ruta resumida de la dirección de red	192.168.64.0	255.255.248.0	11000000.10101000.01000000.00000000

Parte 2. calcular rutas resumidas IPv6

En la parte 2, determinará las rutas resumidas que se pueden utilizar para reducir el tamaño de las tablas de routing. Después de cada conjunto de pasos, complete las tablas con la información apropiada de direccionamiento IPv6.

Topología

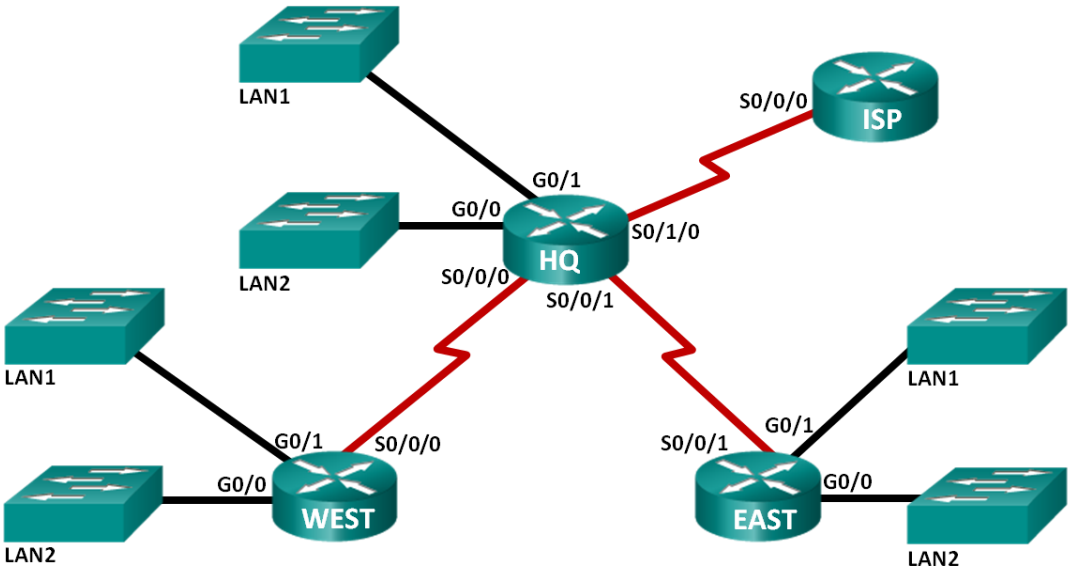


Tabla de direccionamiento

Subred	Dirección IPv6
LAN1 de HQ	2001:DB8:ACAD:E::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64
LAN1 de EAST	2001:DB8:ACAD:1::/64
LAN2 de EAST	2001:DB8:ACAD:2::/64
LAN1 de WEST	2001:DB8:ACAD:9::/64
LAN2 de WEST	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	2001:DB8:CC1E:1::/64

Paso 1. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato hexadecimal.

Paso 2. indicar la ID de subred (bits 48 a 64) de la LAN1 de HQ y la LAN2 de HQ en formato binario.

Paso 3. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? **63**

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

Paso 4. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios de la ID de subred coincidentes para las subredes LAN1 de HQ y LAN2 de HQ.

b. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de HQ	2001:DB8:ACAD:E::/64	FFFF:FFFF:FFFF:FFFF	0000000000001110
LAN2 de HQ	2001:DB8:ACAD:F::/64	FFFF:FFFF:FFFF:FFFF	0000000000001111
Dirección de resumen de las LAN de HQ	2001:DB8:ACAD:E::/63	FFFF:FFFF:FFFF:FFFE	0000000000001110

Paso 5. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato hexadecimal.

Paso 6. indicar la ID de subred (bits 48 a 64) de la LAN1 ESTE y la LAN2 ESTE en formato binario.

Paso 7. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? **62**

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

Paso 8. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 ESTE y la LAN2 ESTE.

b. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de EAST	2001:DB8:ACAD:1::/64	FFFF:FFFF:FFFF:FFFF	0000000000000001
LAN2 de EAST	2001:DB8:ACAD:2::/64	FFFF:FFFF:FFFF:FFFF	0000000000000010
Dirección de resumen de las LAN ESTE	2001:DB8:ACAD::/62	FFFF:FFFF:FFFF:FFFC	0000000000000000

Paso 9. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato decimal.

Paso 10. indicar la ID de subred (bits 48 a 64) de la LAN1 OESTE y la LAN2 OESTE en formato binario.

Paso 11. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? **62**

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

Paso 12. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 OESTE y la LAN2 OESTE.

b. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de WEST	2001:DB8:ACAD:9::/64	FFFF:FFFF:FFFFF:FFFF	0000000000001001
LAN2 de WEST	2001:DB8:ACAD:A::/64	FFFF:FFFF:FFFFF:FFFF	0000000000001010
Dirección de resumen de las LAN OESTE	2001:DB8:ACAD:8::/62	FFFF:FFFF:FFFFF:FFFC	0000000000001000

Paso 13. indicar la dirección IP de la ruta resumida y los primeros 64 bits de la máscara de subred de HQ, ESTE y OESTE en formato decimal.

Paso 14. indicar la ID de subred de la ruta resumida de HQ, ESTE y OESTE en formato binario.

Paso 15. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres ID de subred? **60**

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

Paso 16. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de HQ, ESTE y OESTE.

b. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
HQ	2001:DB8:ACAD:E::/63	FFFF:FFFF:FFFF:FFFE	0000000000001110
EAST	2001:DB8:ACAD::/62	FFFF:FFFF:FFFF:FFFC	0000000000000000
WEST	2001:DB8:ACAD:8::/62	FFFF:FFFF:FFFF:FFFC	0000000000001000
Ruta resumida de la dirección de red	2001:DB8:ACAD::/60	FFFF:FFFF:FFFF:FFF0	0000000000000000

Reflexión

1. ¿Qué diferencia existe entre determinar la ruta resumida para IPv4 y determinarla para IPv6?

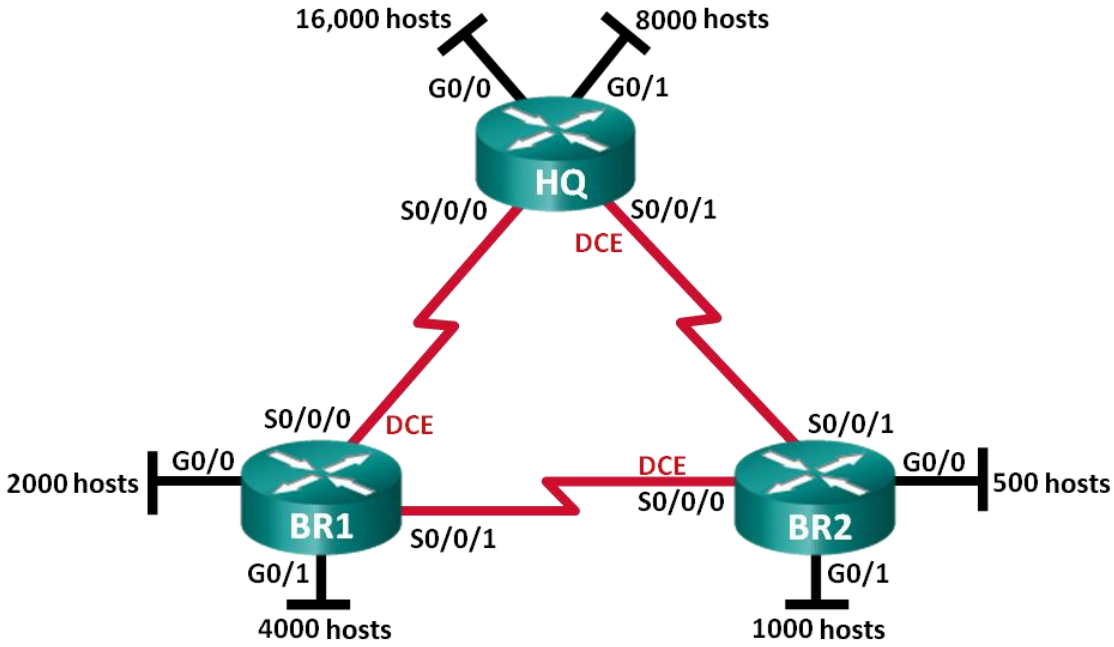
   No hay mayor diferencia excepto porque ipv4 tiene 32 bits y ipv6 tiene 128 bits, también ipv4 es convertir decimal a binario y ipv6 es convertir de hexadecimal a binario.

2. ¿Por qué las rutas resumidas son beneficiosas para una red?

   Hace que la tabla de ruteo vea un proceso más eficiente y reduce los requerimientos de memoria para el router.

6.3.3.7 diseño e implementación de direccionamiento IPv4 con VLSM

Topología



Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direcciones VLSM

Parte 3: realizar el cableado y configurar la red IPv4

Información básica/situación

La máscara de subred de longitud variable (VLSM) se diseñó para conservar direcciones IP. Con VLSM, una red se divide en subredes, que luego se subdividen nuevamente. Este proceso se puede repetir varias veces para crear subredes de distintos tamaños, según el número de hosts requerido en cada subred. El uso eficaz de VLSM requiere la planificación de direcciones.

En esta práctica de laboratorio, se le asigna la dirección de red 172.16.128.0/17 para que desarrolle un esquema de direcciones para la red que se muestra en el diagrama de la topología. Se usará VLSM para que se pueda cumplir con los requisitos de direccionamiento. Después de diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información de dirección IP adecuada.

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)
- 1 computadora (con un programa de emulación de terminal, como Tera Term, para configurar los routers)
- Cable de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet (optativo) y seriales, como se muestra en la topología
- Calculadora de Windows (optativo)

Parte 1: examinar los requisitos de la red

En la parte 1, examinará los requisitos de la red y utilizará la dirección de red 172.16.128.0/17 para desarrollar un esquema de direcciones VLSM para la red que se muestra en el diagrama de la topología.

Nota: puede utilizar la aplicación Calculadora de Windows y la calculadora de subredes IP de www.ipcalc.org como ayuda para sus cálculos.

Paso 1. determinar la cantidad de direcciones host disponibles y la cantidad de subredes que se necesitan.

¿Cuántas direcciones host se encuentran disponibles en una red /17? 32.766

¿Cuál es la cantidad total de direcciones host que se necesitan en el diagrama de la topología? ? 31506

¿Cuántas subredes se necesitan en la topología de la red? 9

Paso 2. determinar la subred más grande que se necesita.

Descripción de la subred (p. ej., enlace BR1 G0/1 LAN o BR1-HQ WAN)) HQ G0/0 LAN

¿Cuántas direcciones IP se necesitan en la subred más grande? 1600

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones? 18 o 255.255.192.

¿Cuántas direcciones host admite esa subred? 16382

¿Se puede dividir la red 172.16.128.0/17 en subredes para admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.128.0/18

172.16.192.0/18

Utilice la primera dirección de red para esta subred.

Paso 3. determinar la segunda subred más grande que se necesita.

Descripción de la subred HQ GO/1 LAN

¿Cuántas direcciones IP se necesitan para la segunda subred más grande? 8000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts? /19 o 255.255.224.0

¿Cuántas direcciones host admite esa subred? 8190

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.192.0/19 , 172.16.224.0/19

Utilice la primera dirección de red para esta subred.

Paso 4. determinar la siguiente subred más grande que se necesita.

Descripción de la subred BR1 G0/1 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 400

¿Cuál es la subred más pequeña que admite esa cantidad de hosts? 20 o 255.255.240.0

¿Cuántas direcciones host admite esa subred? 4094

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.224.0/20

172.16.240.0/20

Utilice la primera dirección de red para esta subred.

Paso 5. determinar la siguiente subred más grande que se necesita.

Descripción de la subred BR1 G0/0 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 200

¿Cuál es la subred más pequeña que admite esa cantidad de hosts? /21 o 255.255.248.0

¿Cuántas direcciones host admite esa subred? 2046

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.240.0/21

172.16.248.0/21

Utilice la primera dirección de red para esta subred.

Paso 6. determinar la siguiente subred más grande que se necesita.

Descripción de la subred BR2 G0/1 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 1000

¿Cuál es la subred más pequeña que admite esa cantidad de hosts? /22 0 255.255.252.0

¿Cuántas direcciones host admite esa subred? 1022

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.248.0/22

172.16.252.0/22

Utilice la primera dirección de red para esta subred.

Paso 7. determinar la siguiente subred más grande que se necesita.

Descripción de la subred BR2 G0/0 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 500

¿Cuál es la subred más pequeña que admite esa cantidad de hosts? 23 o 255.255.254.0

¿Cuántas direcciones host admite esa subred? 510

¿Se puede volver a dividir la subred restante en subredes sin que deje de admitir esta subred? SI

¿Cuáles son las dos direcciones de red que se obtendrían de esta división en subredes?

172.16.252.0/23

172.16.254.0/23

Utilice la primera dirección de red para esta subred.

Paso 8. determinar las subredes que se necesitan para admitir los enlaces seriales.

¿Cuántas direcciones host se necesitan para cada enlace de subred serial? 2

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones host? /30 o 255.255.255.252

d. Divida la subred restante en subredes y, a continuación, escriba las direcciones de red que se obtienen de esta división.

172.16.254.0/24

172.16.255.0/24

e. Siga dividiendo en subredes la primera subred de cada subred nueva hasta obtener cuatro subredes /30. Escriba las primeras tres direcciones de red de estas subredes /30 a continuación.

172.16.254.0/30

172.16.254.4/30

172.16.254.8/30

f. Introduzca las descripciones de las subredes de estas tres subredes a continuación.

Enlace Serial HQ- BR1, Enlace Serial HQ- BR2 y Enlace Serial BR1- BR2

Parte 2: diseñar el esquema de direcciones VLSM

Paso 1. calcular la información de subred.

Utilice la información que obtuvo en la parte 1 para completar la siguiente tabla.

Utilice la información que obtuvo en la parte 1 para completar la siguiente tabla.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host	Dirección de broadcast
HQ G0/0	16 000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8 000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4 000	172.16.224.0/20	172.16.224.1	172.16.239.255
BR1 G0/0	2 000	172.16.240.0/21	172.16.240.1	172.16.247.255
BR2 G0/1	1.000	172.16.248.0/22	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0/23	172.16.252.1	172.16.253.255
HQ S0/0/0-BR1 S0/0/0	2	172.16.254.0/30	172.16.254.1	172.16.254.3
HQ S0/0/1-BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5	172.16.254.7
BR1 S0/0/1-BR2 S0/0/0	2	172.16.254.4/30	172.16.254.9	172.16.254.11

Paso 2. completar la tabla de direcciones de interfaces de dispositivos.

Asigne la primera dirección host en la subred a las interfaces Ethernet. A HQ se le debería asignar la primera dirección host en los enlaces seriales a BR1 y BR2. A BR1 se le debería asignar la primera dirección host para el enlace serial a BR2.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Interfaz del dispositivo
HQ	G0/0	172.16.128.1	255.255.192.0	LAN de 16 000 hosts
	G0/1	172.16.192.1	255.255.224.0	LAN de 8000 hosts
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	LAN de 2000 hosts
	G0/1	172.16.224.1	255.255.240.0	LAN de 4000 hosts
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0

BR2	G0/0	172.16.252.1	255.255.254.0	LAN de 500 hosts
	G0/1	172.16.248.1	255.255.252.0	LAN de 1000 hosts
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

Parte 3: realizar el cableado y configurar la red IPv4

En la parte 3, realizará el cableado de la topología de la red y configurará los tres routers con el esquema de direcciones VLSM que elaboró en la parte 2.

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

Paso 2. configurar los parámetros básicos en cada router.

a. Asigne el nombre de dispositivo al router.

b. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de consola y habilite el inicio de sesión.

e. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

f. Cifre las contraseñas de texto no cifrado.

g. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

Paso 3. configurar las interfaces en cada router.

a. Asigne una dirección IP y una máscara de subred a cada interfaz utilizando la tabla que completó en la parte 2.

b. Configure una descripción de interfaz para cada interfaz.

c. Establezca la frecuencia de reloj en 128000 en todas las interfaces seriales DCE.

HQ(config-if)# **clock rate 128000**

d. Active las interfaces.

Paso 4. guardar la configuración en todos los dispositivos.

Paso 5. Probar la conectividad

a. Haga ping de HQ a la dirección de la interfaz S0/0/0 de BR1.

b. Haga ping de HQ a la dirección de la interfaz S0/0/1 de BR2.

c. Haga ping de BR1 a la dirección de la interfaz S0/0/0 de BR2.

d. Si los pings no se realizaron correctamente, resuelva los problemas de conectividad.

Nota: los pings a las interfaces GigabitEthernet en otros routers no son correctos. Las LAN definidas para las interfaces GigabitEthernet son simuladas. Debido a que no hay ningún dispositivo conectado a estas LAN, están en estado down/down. Debe haber un protocolo de routing para que otros dispositivos detecten esas subredes. Las interfaces de GigabitEthernet también deben estar en estado up/up para que un protocolo de routing pueda agregar las subredes a la tabla de routing. Estas interfaces permanecen en el estado down/down hasta que se conecta un dispositivo al otro extremo del cable de interfaz Ethernet. Esta práctica de laboratorio se centra en VLSM y en la configuración de interfaces.

Reflexión

¿Puede pensar en un atajo para calcular las direcciones de red de las subredes /30 consecutivas?

Una red /30 tiene cuatro espacios de dirección:

La dirección de red, dos direcciones de host y una dirección de difusión.

Otra técnica para obtener la siguiente dirección de red /30 seria tomar la dirección de la red de la red /30 anterior y agregarle 4 al último octeto.

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.				

6.4.2.5 Lab - Calculating Summary Routes with IPv4 and IPv6

Topología

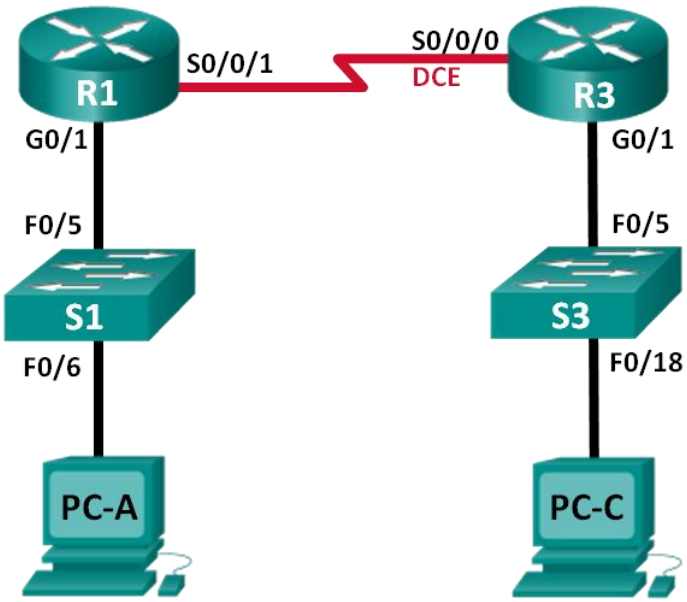


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6/longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::/64 eui-64	N/A
	S0/0/1	FC00::1/64	N/A
R3	G0/1	2001:DB8:ACAD:B::/64 eui-64	N/A
	S0/0/0	FC00::2/64	N/A
PC-A	NIC	SLAAC	SLAAC
PC-C	NIC	SLAAC	SLAAC

Objetivos

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

- Habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.
- Deshabilitar el direccionamiento IPv4 y habilitar SLAAC de IPv6 para las interfaces de red de las computadoras.
- Usar **ipconfig** y **ping** para verificar la conectividad LAN.
- Usar los comandos **show** para verificar la configuración de IPv6.

Parte 2: configurar rutas estáticas y predeterminadas IPv6

- Configurar una ruta estática IPv6 conectada directamente.

- Configurar una ruta estática IPv6 recursiva.
- Configurar una ruta estática predeterminada IPv6.

Información básica/situación

En esta práctica de laboratorio, configurará toda la red para establecer la comunicación solo con direccionamiento IPv6. Esto incluye la configuración de los routers y las computadoras. Usará la configuración automática de dirección sin estado (SLAAC) para configurar las direcciones IPv6 para los hosts. También configurará rutas estáticas y predeterminadas IPv6 en los routers para habilitar la comunicación con redes remotas que no están conectadas directamente.

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

- 2 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

Parte 3. armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, realizará el cableado de la red y la configurará para que establezca la comunicación utilizando direccionamiento IPv6.

Paso 1. Realice el cableado de red tal como se muestra en el diagrama de topología.

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

Paso 3. habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.

a. Mediante Tera Term, acceda al router etiquetado R1 en el diagrama de la topología mediante el puerto de consola y asígnele el nombre R1.

b. En el modo de configuración global, habilite el routing IPv6 en el R1.

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

c. Configure las interfaces de red en el R1 con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz. La interfaz G0/1 tiene una dirección de unidifusión enrutable globalmente, y se utiliza EUI-64 para crear la porción del identificador de la interfaz de la dirección. La interfaz S0/0/1 tiene una dirección local única y enrutable de forma privada, que se recomienda para las conexiones seriales punto a punto.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:DB8:ACAD:A::/64 eui-64
R1(config-if)# no shutdown
R1(config-if)# interface serial 0/0/1
R1(config-if)# ipv6 address FC00::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

d. Asigne un nombre de dispositivo al router R3.

e. En el modo de configuración global, habilite el routing IPv6 en el R3.

```
R3(config)# ipv6 unicast-routing
```

f. Configure las interfaces de red en el R3 con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz. La interfaz G0/1 tiene una dirección de unidifusión enrutable globalmente, y se utiliza EUI-64 para crear la porción del identificador de la interfaz de la dirección. La interfaz S0/0/0 tiene una dirección local única y enrutable de forma privada, que se recomienda para las conexiones seriales punto a punto. La frecuencia de reloj está establecida, porque es el extremo del DCE del cable serial.

```
R3(config)# interface gigabit 0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64
R3(config-if)# no shutdown
R3(config-if)# interface serial 0/0/0
R3(config-if)# ipv6 address FC00::2/64
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
R3(config-if)# exit
```

Paso 4. deshabilitar el direccionamiento IPv4 y habilitar SLAAC de IPv6 para las interfaces de red de las computadoras.

g. En la PC-A y la PC-C, navegue hasta el menú **Inicio** > **Panel de control**. Haga clic en el enlace **Centro de redes y recursos compartidos** en la vista por íconos. En la ventana Centro de redes y recursos compartidos, haga clic en el enlace **Cambiar configuración del adaptador**, que se encuentra en el lado izquierdo de la ventana, para abrir la ventana Conexiones de red.

h. En la ventana Conexiones de red, verá los íconos de los adaptadores de interfaz de red. Haga doble clic en el ícono de Conexión de área local de la interfaz de red de la computadora que está conectada al switch. Haga clic en **Propiedades** para abrir la ventana de diálogo Propiedades de conexión de área local.

i. Con la ventana Propiedades de conexión de área local abierta, desplácese hacia abajo por los elementos y desactive la casilla de verificación del elemento **Protocolo de Internet versión 4 (TCP/IPv4)** para deshabilitar el protocolo IPv4 en la interfaz de red.

j. Con la ventana Propiedades de conexión de área local todavía abierta, haga clic en la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y luego en **Propiedades**.

k. Con la ventana Propiedades > Protocolo de Internet versión 6 (TCP/IPv6) abierta, verifique que los botones de opción **Obtener una dirección IPv6 automáticamente** y **Obtener la dirección del servidor DNS automáticamente** estén seleccionados. Si no lo están, selecciónelos.

l. Si las computadoras están configuradas para obtener una dirección IPv6 automáticamente, se comunicarán con los routers para obtener la información del gateway y de la subred de la red y configurarán automáticamente la información de la dirección IPv6. En el siguiente paso, verificará la configuración.

Paso 5. usar ipconfig y ping para verificar la conectividad LAN.

m. En la PC-A, abra un símbolo del sistema, escriba **ipconfig /all** y presione Enter. El resultado debe ser similar al que se muestra a continuación. En el resultado, debería ver que la computadora ahora tiene una dirección IPv6 de unidifusión global, una dirección IPv6 link-local y una dirección IPv6 link-local de gateway predeterminado. Es posible que también vea una dirección IPv6 temporal y, en direcciones del servidor DNS, tres direcciones locales de sitio que empiezan con FEC0. Las direcciones locales de sitio son direcciones privadas que tienen compatibilidad retrospectiva con NAT. Sin embargo, no son compatibles con IPv6, y se reemplazaron con direcciones locales únicas.

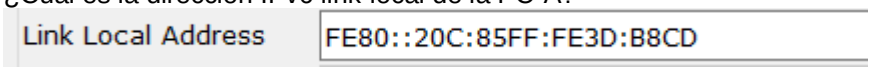
```
C:\Users\User1> ipconfig /all
Windows IP Configuration

<Output Omitted>

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LC Gigabit Network
Connection
   Physical Address. . . . . . . . . : 1C-C1-DE-91-C3-5D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . :
2001:db8:acad:a:7c0c:7493:218d:2f6c(Preferred)
   Temporary IPv6 Address. . . . . . :
2001:db8:acad:a:bc40:133a:54e7:d497(Preferred)
   Link-local IPv6 Address . . . . . :
fe80::7c0c:7493:218d:2f6c%13(Preferred)
   Default Gateway . . . . . . . . . : fe80::6273:5cff:fe0d:1a61%13
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

Sobre la base de la implementación de la red y el resultado del comando **ipconfig /all**, ¿la PC-A recibió información de direccionamiento IPv6 del R1?

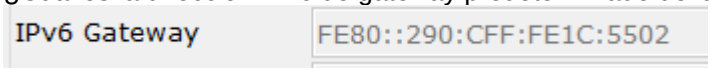
Si, al configurar **ipv6 unicast-routing** se activa la auto configuración en host.

n. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-A?

o. ¿Cuál es la dirección IPv6 link-local de la PC-A?



p. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-A?



q. En la PC-A, use el comando **ping -6** para emitir un ping IPv6 a la dirección link-local de gateway predeterminado. Debería ver respuestas del router R1.

```
C:\Users\User1> ping -6 <default-gateway-address>
```

¿La PC-A recibió respuestas al ping hizo que al R1?

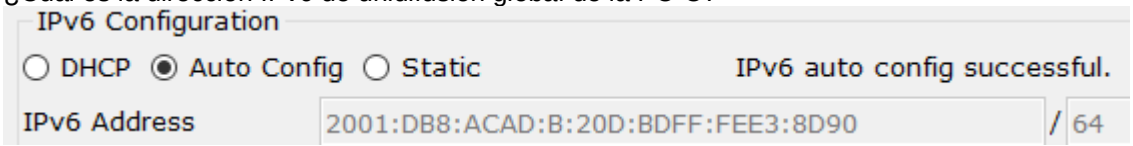
_SI_____

r. Repita el paso 5a en la PC-C.

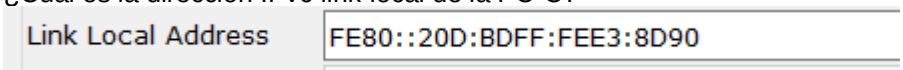
¿La PC-C recibió información de direccionamiento IPv6 del R3?

_SI_____

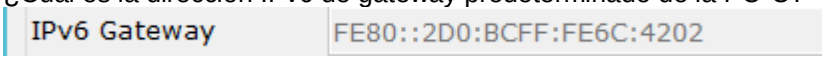
s. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-C?



t. ¿Cuál es la dirección IPv6 link-local de la PC-C?



u. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-C?



v. En la PC-C, use el comando **ping -6** para hacer ping al gateway predeterminado de la PC-C.

¿La PC-C recibió respuestas a los pings que hizo al R3?

__SI_____

w. Intente hacer **ping -6** IPv6 de la PC-A a la dirección IPv6 de la PC-C.

```
C:\Users\User1> ping -6 PC-C-IPv6-address
```

¿El ping se realizó correctamente? ¿Por qué o por qué no?

No, porque R1 conoce únicamente las rutas que están únicamente conectadas y PC-C se encuentra en el siguiente salto.

Paso 6. Use los comandos show para verificar la configuración de IPv6.

x. Revise el estado de las interfaces en el R1 con el comando **show ipv6 interface brief**.

¿Cuáles son las dos direcciones IPv6 de la interfaz G0/1 y qué tipo de direcciones IPv6 son?

GigabitEthernet0/1 [up/up]

FE80::290:CFF:FE1C:5502 Global

2001:DB8:ACAD:A:290:CFF:FE1C:5502 unicast

¿Cuáles son las dos direcciones IPv6 de la interfaz S0/0/1 y qué tipo de direcciones IPv6 son?

Serial0/0/1 [up/up]

FE80::290:CFF:FE1C:5501 global

FC00::1 unicast

y. Para ver información más detallada sobre las interfaces IPv6, escriba el comando **show ipv6 interface** en el R1 y presione Enter.

¿Cuáles son las direcciones del grupo de multidifusión de la interfaz Gigabit Ethernet 0/1?

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF1C:5502

¿Cuáles son las direcciones del grupo de multidifusión de la interfaz S0/0/1?

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

FF02::1:FF1C:5501

¿Para qué se usa la dirección de multidifusión FF02::1?

Comunicación con los nodos de la red.

¿Para qué se usa la dirección de multidifusión FF02::2?

Comunicación entre los segmentos de red.

¿Qué tipo de direcciones de multidifusión son FF02::1:FF00:1 y FF02::1:FF0D:1A60 y para qué se usan?

Resolver las direcciones IP de los dispositivos vecinos y son tipo de multicast solicitadas.

z. Vea la información de la tabla de routing IPv6 del R1 con el comando **show ipv6 route**. La tabla de routing IPv6 debe tener dos rutas conectadas, una para cada interfaz, y tres rutas locales, una para cada interfaz y otra para el tráfico de multidifusión a una interfaz Null0.

¿De qué forma el resultado de la tabla de routing del R1 revela el motivo por el que no pudo hacer ping de la PC-A a la PC-C?

La tabla de routing revela que no hay rutas estáticas para la comunicación de las dos redes.

Parte 4. configurar rutas estáticas y predeterminadas IPv6

En la parte 2, configurará rutas estáticas y predeterminadas IPv6 de tres maneras distintas. Confirmará que las rutas se agreguen a las tablas de routing y verificará que la conectividad entre la PC-A y la PC-C sea correcta.

Configurará tres tipos de rutas estáticas IPv6:

- **Ruta estática IPv6 conectada directamente**: una ruta estática conectada directamente se crea al especificar la interfaz de salida.
- **Ruta estática IPv6 recursiva**: una ruta estática recursiva se crea al especificar la dirección IP del siguiente salto. Este método requiere que el router ejecute una búsqueda recursiva en la tabla de routing para identificar la interfaz de salida.
- **Ruta estática predeterminada IPv6**: similar a una ruta IPv4 de cuádruple cero, una ruta estática predeterminada IPv6 se crea al hacer que el prefijo IPv6 de destino y la longitud de prefijo sean todos ceros, :: /0.

Paso 1. configurar una ruta estática IPv6 conectada directamente.

En una ruta estática IPv6 conectada directamente, la entrada de ruta especifica la interfaz de salida del router. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar una ruta estática IPv6 conectada directamente, utilice el siguiente formato de comando:

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>
```

a. En el router R1, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:B::/64 en el R3 mediante la interfaz de salida S0/0/1 del R1.

```
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)#
```

b. Consulte la tabla de routing IPv6 para verificar la entrada de la ruta estática nueva.

¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta que se agregó recientemente a la tabla de routing?

S 2001:DB8:ACAD:B::/64 [1/0]

via Serial0/0/1, receive

c. Ahora que la ruta estática se configuró en el R1, ¿es posible hacer ping de la PC-A al host PC-C?

No, falta configurar R3.

Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, ese ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 2001:DB8:ACAD:A::/64 en la tabla de routing. Para hacer ping correctamente a través de la red, también debe crear una ruta estática en el R3.

d. En el router R3, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:A::/64, mediante la interfaz de salida S0/0/0 del R3.

```
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)#
```

e. Ahora que ambos routers tienen rutas estáticas, intente hacer **ping -6** de IPv6 desde la PC-A hasta la dirección IPv6 de unidifusión global de la PC-C.

¿El ping se realizó correctamente? ¿Por qué?

Si, por que ya existen las rutas estáticas en los dos routers.

Paso 2. configurar una ruta estática IPv6 recursiva.

En una ruta estática IPv6 recursiva, la entrada de ruta tiene la dirección IPv6 del router del siguiente salto. Para configurar una ruta estática IPv6 recursiva, utilice el siguiente formato de comando:

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <next-hop-ipv6-address>
```

f. En el router R1, elimine la ruta estática conectada directamente y agregue una ruta estática recursiva.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# exit
```

g. En el router R3, elimine la ruta estática conectada directamente y agregue una ruta estática recursiva.

```
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# exit
```

h. Consulte la tabla de routing IPv6 del R1 para verificar la entrada de la ruta estática nueva.

¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta que se agregó recientemente a la tabla de routing?

S 2001:DB8:ACAD:B::/64 [1/0]

via FC00::2, receive

i. Para verificar la conectividad, emita un comando **ping -6** de la PC-A a la PC-C.

¿El ping se realizó correctamente? SI

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

Paso 3. configurar una ruta estática predeterminada IPv6.

En una ruta estática predeterminada, el prefijo IPv6 de destino y la longitud de prefijo son todos ceros.

```
Router(config)# ipv6 route ::/0 <outgoing-interface-type> <outgoing-interface-number> {and/or} <next-hop-ipv6-address>
```

j. En el router R1, elimine la ruta estática recursiva y agregue una ruta estática predeterminada.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# ipv6 route ::/0 serial 0/0/1
R1(config)#
```

k. En el R3, elimine la ruta estática recursiva y agregue una ruta estática predeterminada.

l. Consulte la tabla de routing IPv6 del R1 para verificar la entrada de la ruta estática nueva.

¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta predeterminada que se agregó recientemente a la tabla de routing?
S ::/0 [1/0]

via Serial0/0/1, receive

m. Para verificar la conectividad, emita un comando **ping -6** de la PC-A a la PC-C.

¿El ping se realizó correctamente? _SI_____

Nota: quizás sea necesario inhabilitar el firewall de las computadoras para hacer ping entre estas.

Reflexión

1. Esta práctica de laboratorio se centra en la configuración de rutas estáticas y predeterminadas IPv6. ¿Puede pensar en una situación en la que tendría que configurar rutas estáticas y predeterminadas IPv6 e IPv4 en un router?

   Cuando se esté realizando un proceso de migración de IPv4 a IPv6, por seguridad de funcionamiento de la infraestructura no se deben hacer migraciones tan grandes en una sola etapa, así que es mejor migrar una parte a IPv6 y la otra dejarla en IPv4 hasta el momento ideal de su migración.

2. En la práctica, la configuración de rutas estáticas y predeterminadas IPv6 es muy similar a la configuración de rutas estáticas y predeterminadas IPv4. Independientemente de las diferencias obvias entre el direccionamiento IPv6 e IPv4, ¿cuáles son algunas otras diferencias que se observan al configurar y verificar una ruta estática IPv6 en comparación con una ruta estática IPv4?

   Siempre es necesario especificar que los comandos son para IPv6, ejemplo ipv6 route. Show ipv6 route, mientras que cuando se configuran para IPv6 no es necesario especificar la versión del protocolo.

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.

6.2.2.5 Lab - Configuring IPv4 Static and Default Routes

Topología

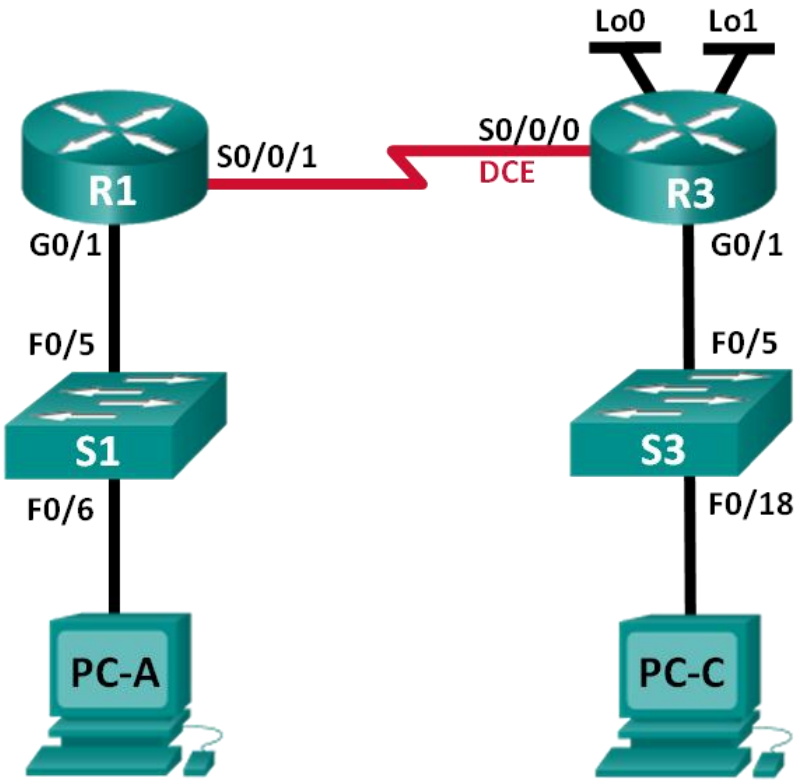


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los parámetros básicos de los dispositivos y verificar la conectividad

Parte 3: configurar rutas estáticas

- Configurar una ruta estática recursiva.
- Configurar una ruta estática conectada directamente.
- Configurar y eliminar rutas estáticas.

Parte 4: configurar y verificar una ruta predeterminada

Información básica/situación

Un router utiliza una tabla de enrutamiento para determinar a dónde enviar los paquetes. La tabla de routing consta de un conjunto de rutas que describen el gateway o la interfaz que el router usa para llegar a una red especificada. Inicialmente, la tabla de routing contiene solo redes conectadas directamente. Para comunicarse con redes distantes, se deben especificar las rutas, que deben agregarse a la tabla de routing.

En esta práctica de laboratorio, configurará manualmente una ruta estática a una red distante especificada sobre la base de una dirección IP del siguiente salto o una interfaz de salida. También configurará una ruta estática predeterminada. Una ruta predeterminada es un tipo de ruta estática que especifica el gateway que se va a utilizar cuando la tabla de routing no incluye una ruta para la red de destino.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. 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

- 2 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

Parte 5. establecer la topología e inicializar los dispositivos

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.

Parte 6. configurar los parámetros básicos de los dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos, como las direcciones IP de interfaz, el acceso a dispositivos y las contraseñas. Verificará la conectividad LAN e identificará las rutas que se indican en las tablas de routing del R1 y el R3.

Paso 1. Configure las interfaces de la PC.

Paso 2. configurar los parámetros básicos en los routers.

a. Configure los nombres de los dispositivos, como se muestra en la topología y en la tabla de direccionamiento.

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

Paso 3. configurar los parámetros IP en los routers.

e. Configure las interfaces del R1 y el R3 con direcciones IP según la tabla de direccionamiento.

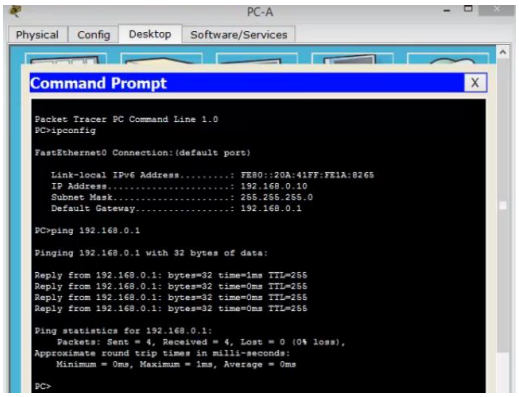
f. La conexión S0/0/0 es la conexión DCE y requiere el comando **clock rate**. A continuación, se muestra la configuración de la interfaz S0/0/0 del R3.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

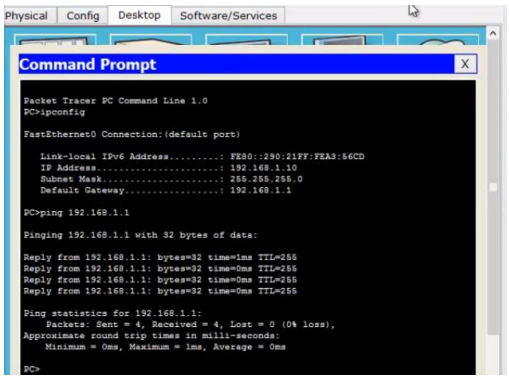
Paso 4. verificar la conectividad de las LAN.

g. Para probar la conectividad, haga ping de cada computadora al gateway predeterminado que se configuró para ese host.

¿Es posible hacer ping de la PC-A al gateway predeterminado? ____SI_____

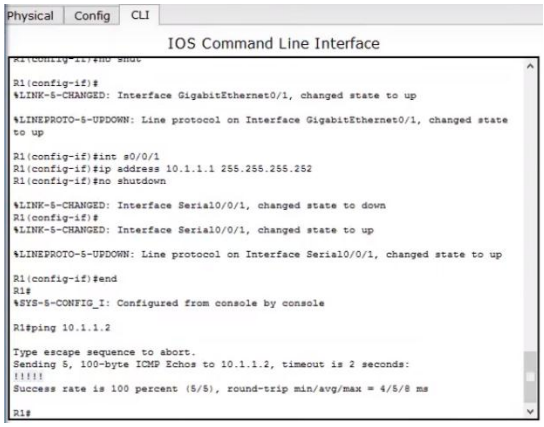


¿Es posible hacer ping de la PC-C al gateway predeterminado? ____SI_____



h. Para probar la conectividad, haga ping entre los routers conectados directamente.

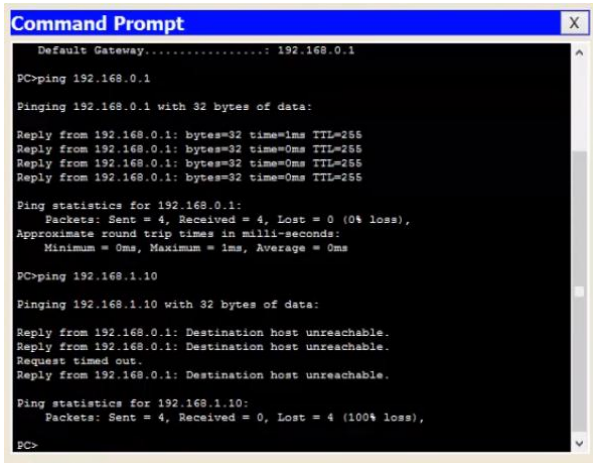
¿Es posible hacer ping del R1 a la interfaz S0/0/0 del R3? ____SI_____



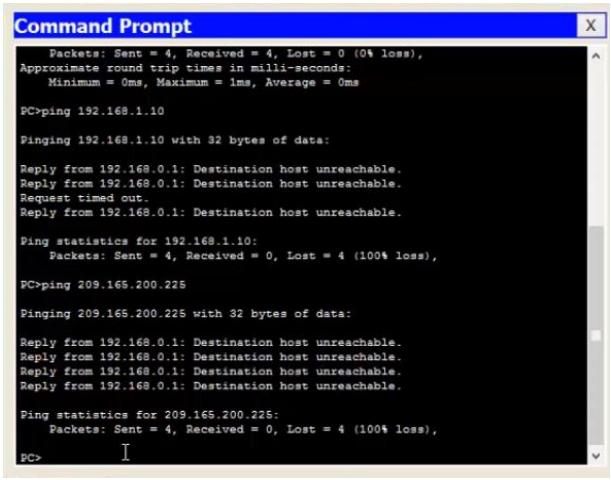
Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.

i. Pruebe la conectividad entre los dispositivos que no están conectados directamente.

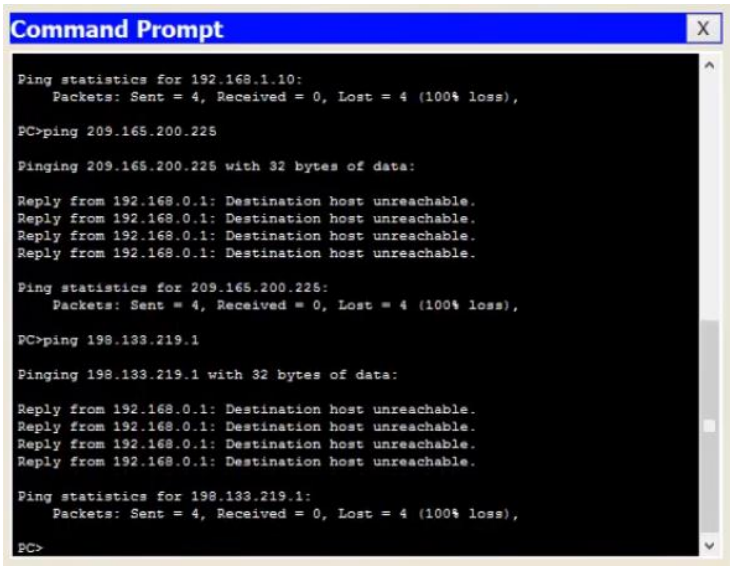
¿Es posible hacer ping de la PC-A a la PC-C? ____NO SE PUEDE_____



¿Es posible hacer ping de la PC-A a la interfaz Lo0? ___ NO SE PUEDE _____



¿Es posible hacer ping de la PC-A a la interfaz Lo1? ___NO_____



¿Los pings eran correctos? ¿Por qué o por qué no?

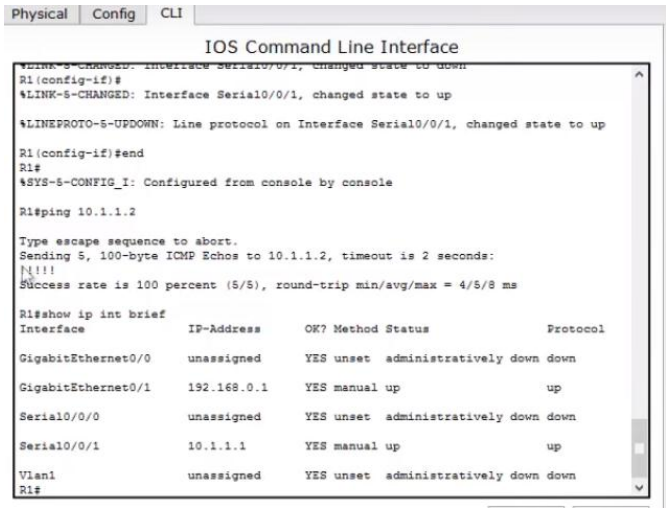
_____NO POR QUE ESTA ESTABLECIDA LA RUTA PARA LLEGAR ALLI_____

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

Paso 5. reunir información.

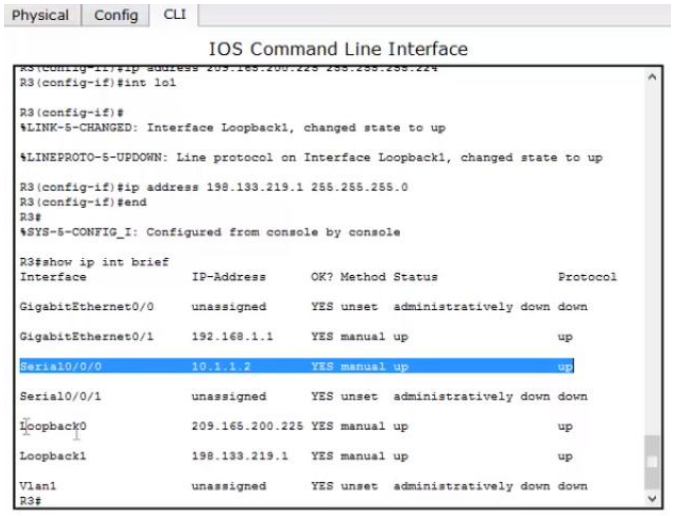
j. Revise el estado de las interfaces en el R1 con el comando **show ip interface brief**.

¿Cuántas interfaces están activadas en el R1? __DOS_____



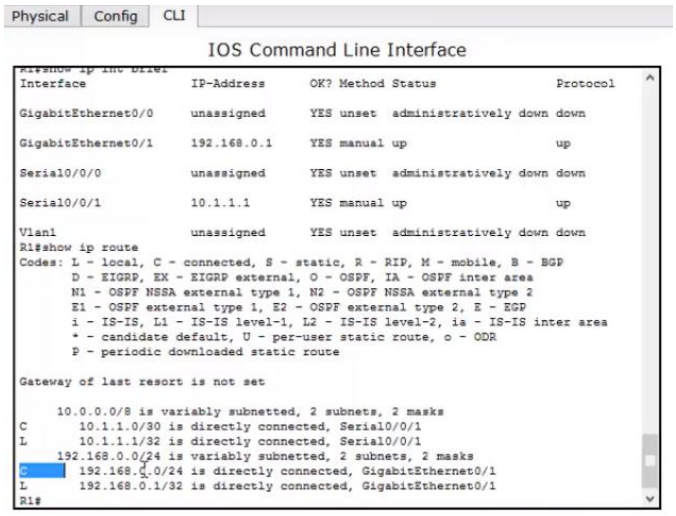
k. Revise el estado de las interfaces en el R3.

¿Cuántas interfaces están activadas en el R3? __CUATRO_____



l. Vea la información de la tabla de routing del R1 con el comando **show ip route**.

¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R1?

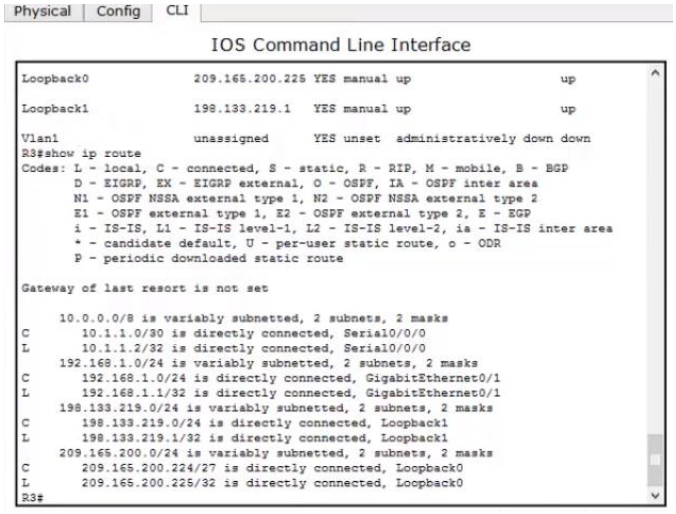


_____TODAS LA QUE NO SON ESTATICA_____

m. Vea la información de la tabla de routing para el R3.

¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R3?

____TODAS LAS DE R1_____



¿Por qué ninguna de las redes está presente en las tablas de enrutamiento para cada uno de los routers?

____POR QUE NO ESTAN VISIBLES _____

_____ _____

Parte 7. Configure las rutas estáticas.

En la parte 3, empleará varias formas de implementar rutas estáticas y predeterminadas, confirmará si las rutas se agregaron a las tablas de routing del R1 y el R3, y verificará la conectividad sobre la base de las rutas introducidas.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. 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.

Paso 1. Configure una ruta estática recursiva.

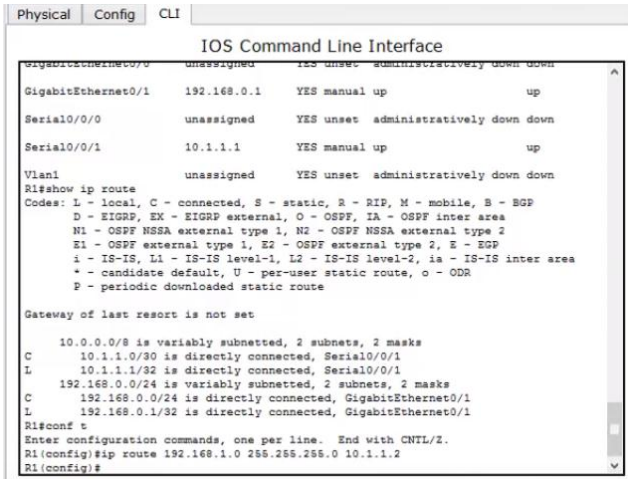
Con una ruta estática recursiva, se especifica la dirección IP del siguiente salto. Debido a que solo se especifica la IP de siguiente salto, el router tiene que hacer varias búsquedas en la tabla de routing antes de reenviar paquetes. Para configurar rutas estáticas recursivas, utilice la siguiente sintaxis:

```
Router(config)# ip route dirección-red máscara-subred dirección-ip
```

a. En el router R1, configure una ruta estática a la red 192.168.1.0 utilizando la dirección IP de la interfaz serial 0/0/0 del R3 como la dirección de siguiente salto. En el espacio proporcionado, escriba el comando que utilizó.

____ **ip route** 192.168.1.0 255.255.255.0 10.1.1.2

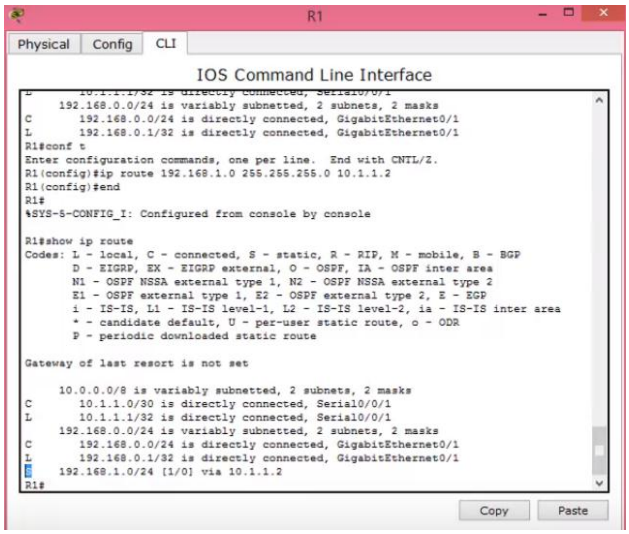
_____



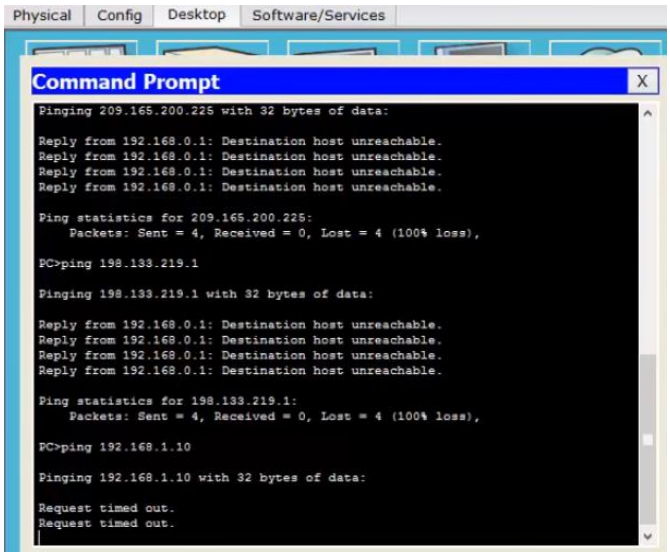
b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?

_____CON
S_____



¿Es posible hacer ping del host PC-A host a al host PC-C? ____NO_____



Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, este ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 192.168.0.0 en la tabla de routing.

Paso 2. configurar una ruta estática conectada directamente.

Con una ruta estática conectada directamente, se especifica el parámetro *interfaz-salida*, que permite que el router resuelva una decisión de reenvío con una sola búsqueda. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar rutas estáticas conectadas directamente con una interfaz de salida especificada, utilice la siguiente sintaxis:

```
Router(config)# ip route dirección-red máscara-subred interfaz-salida
```

c. En el router R3, configure una ruta estática a la red 192.168.0.0 con la interfaz S0/0/0 como la interfaz de salida. En el espacio proporcionado, escriba el comando que utilizó.

___ **ip route** 192.168.0.0 255.255.255.0 s0/0/0

_____

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 192.168.0.0 255.255.255.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R3(config)#
```

Copy Paste

d. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?

_____CON LAS S_____

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

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 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
S    192.168.0.0/24 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C       198.133.219.0/24 is directly connected, Loopback1
L       198.133.219.1/32 is directly connected, Loopback1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R3#
```

e. ¿Es posible hacer ping del host PC-A host a al host PC-C? ___SI_____

```
Command Prompt
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

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

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>
```

Este ping debe tener éxito.

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

Paso 3. configurar una ruta estática.

f. En el router R1, configure una ruta estática a la red 198.133.219.0 utilizando una de las opciones de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

____ **ip route** 198.133.219.0 255.255.255.0 10.1.1.2

_____

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/1
L       10.1.1.1/32 is directly connected, Serial0/0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 198.133.219.0 255.255.255.0 10.1.1.2
R1(config)#
```

g. En el router R1, configure una ruta estática a la red 209.165.200.224 en el R3 utilizando la otra opción de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

_____ **ip route** 209.165.200.224 255.255.255.224 s0/0/1

_____

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/1
L       10.1.1.1/32 is directly connected, Serial0/0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 198.133.219.0 255.255.255.0 10.1.1.2
R1(config)#ip route 209.165.200.224 255.255.255.224 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#
```

h. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?

____SI CONLA
S_____

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/1
L       10.1.1.1/32 is directly connected, Serial0/0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
S    198.133.219.0/24 [1/0] via 10.1.1.2
     209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224/27 is directly connected, Serial0/0/1
R1#
```

i. ¿Es posible hacer ping del host PC-A a la dirección 198.133.219.1 del R1? ___SI_____

j.

```
Command Prompt
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 198.133.219.1

Pinging 198.133.219.1 with 32 bytes of data:

Reply from 198.133.219.1: bytes=32 time=2ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254

Ping statistics for 198.133.219.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
```

Este ping debe tener éxito.

Paso 4. Elimine las rutas estáticas de las direcciones de loopback.

k. En el R1, utilice el comando **no** para eliminar las rutas estáticas de las dos direcciones de loopback de la tabla de routing. En el espacio proporcionad o, escriba los comandos que utilizó.

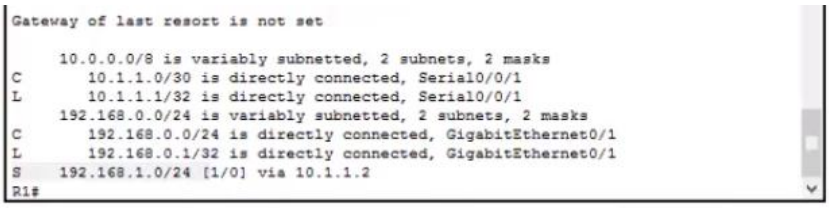
_____ NO IP ROUTE ANTES DE LOS DOS

ip route 198.133.219.0 255.255.255.0 S0/0/1

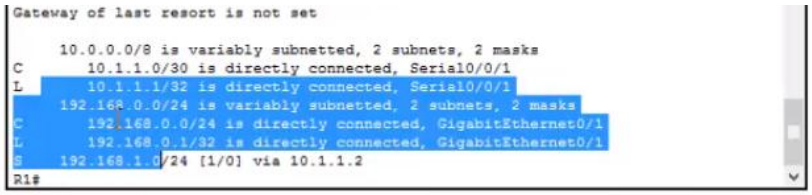
ip route 209.165.200.224 255.255.255.224 S0/0/1 _____

l. Observe la tabla de routing para verificar si se eliminaron las rutas.

¿Cuántas rutas de red se indican en la tabla de routing del R1? __TRES_____



¿El gateway de último recurso está establecido? ___NO_____



Parte 8. configurar y verificar una ruta predeterminada

En la parte 4, implementará una ruta predeterminada, confirmará si la ruta se agregó a la tabla de routing y verificará la conectividad sobre la base de la ruta introducida.

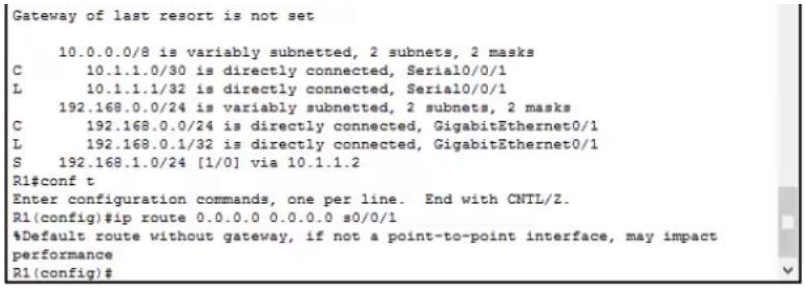
Una ruta predeterminada identifica el gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática predeterminada es una ruta estática con 0.0.0.0 como dirección IP y máscara de subred de destino. Comúnmente, esta ruta se denomina “ruta de cuádruple cero”.

En una ruta predeterminada, se puede especificar la dirección IP del siguiente salto o la interfaz de salida. Para configurar una ruta estática predeterminada, utilice la siguiente sintaxis:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

a. Configure el router R1 con una ruta predeterminada que utilice la interfaz de salida S0/0/1. En el espacio proporcionado, escriba el comando que utilizó.

__ SOLO SE PONE AL FINAL 10.1.1.2 LOS DEMAS SON 0_____



b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?

_____ES UN S*_____

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

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/1
L       10.1.1.1/32 is directly connected, Serial0/0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
S*   0.0.0.0/0 is directly connected, Serial0/0/1
R1#
```

¿Cuál es el gateway de último recurso?

_____ 10.1.1.2

_____

c. ¿Es posible hacer ping del host PC-A a 209.165.200.225? ___SI_____

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>
```

d. ¿Es posible hacer ping del host PC-A a 198.133.219.1? ____SI_____

```
PC>ping 198.133.219.1

Pinging 198.133.219.1 with 32 bytes of data:

Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254

Ping statistics for 198.133.219.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>
```

Estos pings deben tener éxito.

Reflexión

1. Una nueva red 192.168.3.0/24 está conectada a la interfaz G0/0 del R1. ¿Qué comandos podrían utilizarse para configurar una ruta estática a esa red desde el R3?

   _____ ip router 192.168.3.0 255.255.255.255 s0/0/0

   _____

   _____

   _____

2. ¿Ofrece alguna ventaja configurar una ruta estática conectada directamente, en vez de una ruta estática?

   _____ SI FUNCIONA MEJOR

   _____

_____
_____

3. ¿Por qué es importante configurar una ruta predeterminada en un router?

   ____ PARA QUE SALGA BIEN EL ENVIO
   _____

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 para las partes 2, 3 y 4

Los comandos que se indican en el apéndice A sirven exclusivamente como referencia. Este apéndice no incluye todos los comandos específicos que se necesitan para completar esta práctica de laboratorio.

Configuración básica de los dispositivos

Configure los parámetros IP en el router.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Configuraciones de rutas estáticas

Configure una ruta estática recursiva.

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

Configure una ruta estática conectada directamente.

```
R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0
```

Elimine las rutas estáticas.

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1
```

o

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
0
R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Configuración de rutas predeterminadas

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

5.1.3.7 Práctica de laboratorio: configuración de routing entre VLAN basado en enlaces troncales 802.1Q

Gustavo mercado cod. 1047422884

Topología

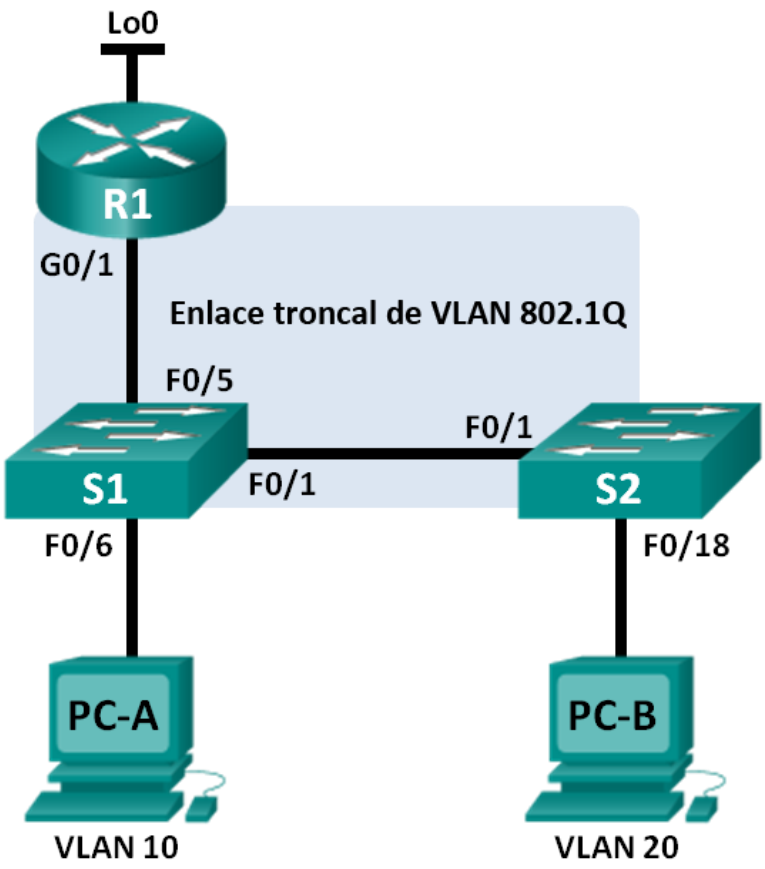


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Especificaciones de la asignación de puertos de switch

Puertos	Asignaciones	Red
S1 F0/1	Enlace troncal de 802.1Q	N/A
S2 F0/1	Enlace troncal de 802.1Q	N/A
S1 F0/5	Enlace troncal de 802.1Q	N/A
S1 F0/6	VLAN 10: Estudiantes	192.168.10.0/24
S2 F0/18	VLAN 20: Cuerpo docente	192.168.20.0/24

Objetivos

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

Parte 2: configurar switches con VLAN y enlaces troncales

Parte 3: configurar routing entre VLAN basado en enlaces troncales

Información básica/situación

Un segundo método para proporcionar routing y conectividad a varias VLAN es mediante el uso de un enlace troncal 802.1Q entre uno o más switches y una única interfaz del router. Este método también se conoce como “routing entre VLAN con router-on-a-stick”. En este método, se divide la interfaz física del router en varias subinterfaces que proporcionan rutas lógicas a todas las VLAN conectadas.

En esta práctica de laboratorio, configurará el routing entre VLAN basado en enlaces troncales y verificará la conectividad a los hosts en diferentes VLAN y con un loopback en el router.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing entre VLAN basado en enlaces troncales. Sin embargo, los comandos requeridos para la configuración 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 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.

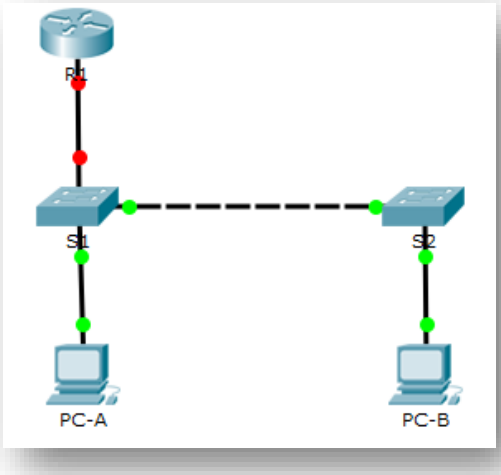
Recursos necesarios

- 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

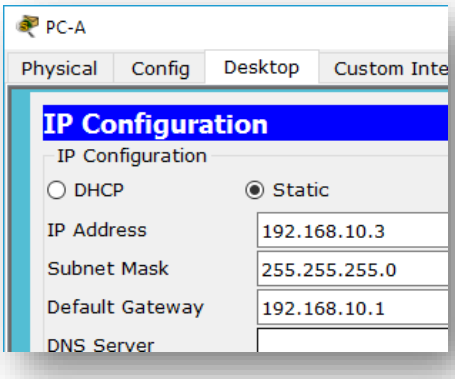
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

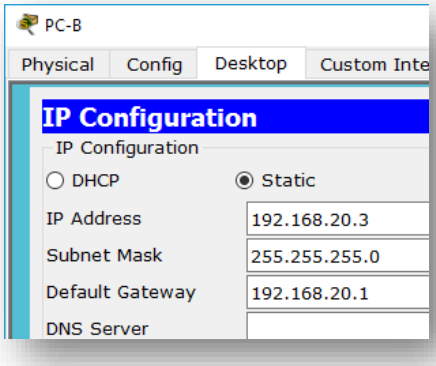
En la parte 1, configurará la topología de la red y configurará los parámetros básicos en los equipos host, los switches y el router.

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



Paso 2. configurar los equipos host.





Paso 3. inicializar y volver a cargar los routers y switches, según sea necesario.

Paso 4. configurar los parámetros básicos para cada switch.

e. Desactive la búsqueda del DNS.

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

g. Asigne **class** como la contraseña del modo EXEC privilegiado.

h. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

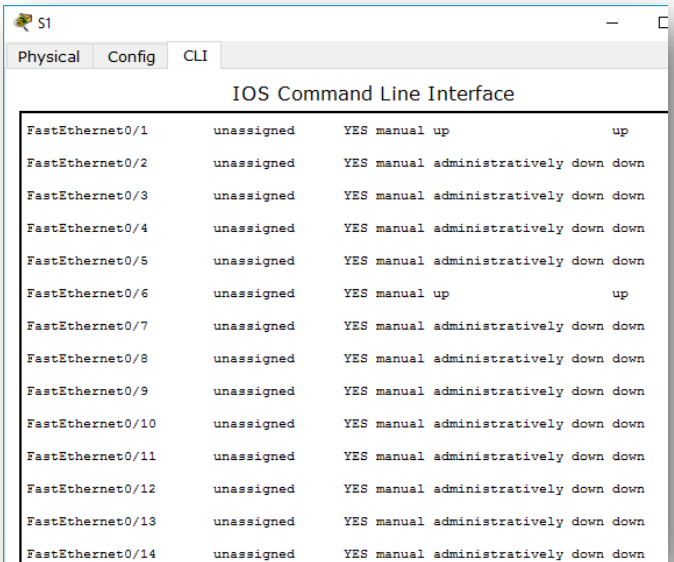
i. Configure **logging synchronous** para la línea de consola.

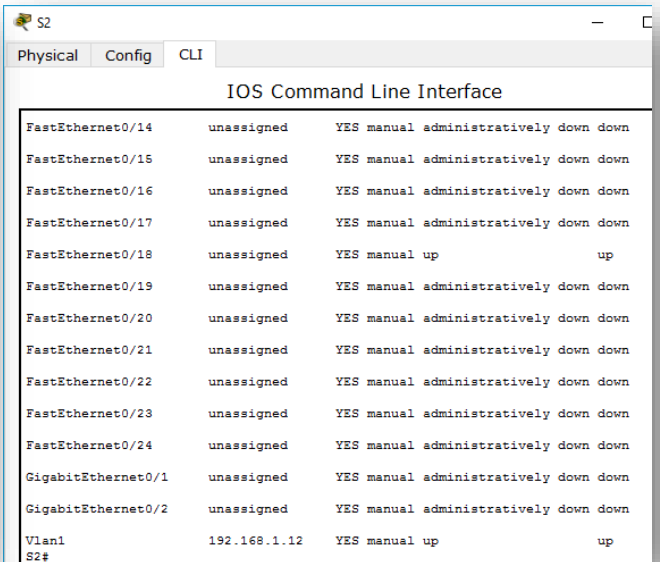
j. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

k. Configure el gateway predeterminado en los dos switches.

l. Desactive administrativamente todos los puertos que no se usen en el switch.

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





Paso 5. configurar los parámetros básicos para el router.

a. Desactive la búsqueda del DNS.

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

c. Configure la dirección IP Lo0, como se muestra en la tabla de direccionamiento. No configure las subinterfaces en esta instancia; esto lo hará en la parte 3.

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

e. Asigne **class** como la contraseña del modo EXEC privilegiado.

f. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

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

Parte 2: configurar los switches con las VLAN y los enlaces troncales

En la parte 2, configurará los switches con las VLAN y los enlaces troncales.

Nota: los comandos requeridos para la parte 2 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar el S1 y el S2 sin consultar el apéndice.

Paso 1. Configurar las VLAN en S1.

a. En el S1, configure las VLAN y los nombres que se indican en la tabla Especificaciones de la asignación de puertos de switch. En el espacio proporcionado, escriba los comandos que utilizó. // Vlan 10 Vlan 20 y name Estudiantes, name Cuerpo_docente

b. En el S1, configure la interfaz conectada al R1 como enlace troncal. También configure la interfaz conectada al S2 como enlace troncal. En el espacio proporcionado, escriba los comandos que utilizó.

// switchport mode trunk

c. En el S1, asigne el puerto de acceso para la PC-A a la VLAN 10. En el espacio proporcionado, escriba los comandos que utilizó. // switchport mode Access switchport access vlan 10

Paso 2. configurar las VLAN en el switch 2.

a. En el S2, configure las VLAN y los nombres que se indican en la tabla Especificaciones de la asignación de puertos de switch.

b. En el S2, verifique que los nombres y números de las VLAN coincidan con los del S1. En el espacio proporcionado, escriba el comando que utilizó. // show vlan brief

c. En el S2, asigne el puerto de acceso para la PC-B a la VLAN 20.

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 20

d. En el S2, configure la interfaz conectada al S1 como enlace troncal.

S1(config)#interface f0/1

S1(config-if)#switchport mode trunk

Parte 3: configurar routing entre VLAN basado en enlaces troncales

En la parte 3, configurará el R1 para enrutar a varias VLAN mediante la creación de subinterfaces para cada VLAN. Este método de routing entre VLAN se denomina “router-on-a-stick”.

Nota: los comandos requeridos para la parte 3 se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar el routing entre VLAN basado en enlaces troncales o con router-on-a-stick sin consultar el apéndice.

Paso 1. configurar una subinterfaz para la VLAN 1.

a. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 1 y use el 1 como ID de la subinterfaz. En el espacio proporcionado, escriba el comando que utilizó.

// R1(config)#interface g0/1.1

R1(config-subif)#

b. Configure la subinterfaz para que opere en la VLAN 1. En el espacio proporcionado, escriba el comando que utilizó.

// R1(config-subif)#encapsulation dot1Q 1

R1(config-subif)#

c. Configure la subinterfaz con la dirección IP de la tabla de direccionamiento. En el espacio proporcionado, escriba el comando que utilizó.

// R1(config-subif)#ip address 192.168.1.1 255.255.255.0

Paso 2. configurar una subinterfaz para la VLAN 10.

a. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 10 y use el 10 como ID de la subinterfaz.

b. Configure la subinterfaz para que opere en la VLAN 10.

c. Configure la subinterfaz con la dirección de la tabla de direccionamiento.

```
// R1(config)#interface g0/1.10
  R1(config-subif)#encapsulation dot1Q 10
  R1(config-subif)#ip address 192.168.10.1 255.255.255.0
```

Paso 3. configurar una subinterfaz para la VLAN 20.

a. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 20 y use el 20 como ID de la subinterfaz.

b. Configure la subinterfaz para que opere en la VLAN 20.

c. Configure la subinterfaz con la dirección de la tabla de direccionamiento.

// R1(config-subif)#int g0/1.20

R1(config-subif)#encapsulation dot1Q 20

R1(config-subif)#ip address 192.168.20.1 255.255.255.0

Paso 4. habilitar la interfaz G0/1.

Habilite la interfaz G0/1. En el espacio proporcionado, escriba los comandos que utilizó. // no shutdown

Paso 5. Verifique la conectividad.

Introduzca el comando para ver la tabla de routing en el R1. ¿Qué redes se enumeran?

```
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1.1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1.1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R1#
```

¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 10? // Si

```
Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

```
PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

¿Es posible hacer ping de la PC-A a la interfaz Lo0? //SI

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

¿Es posible hacer ping de la PC-A al S2? //Si

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=254
Reply from 192.168.1.12: bytes=32 time=0ms TTL=254
Reply from 192.168.1.12: bytes=32 time=0ms TTL=254
Reply from 192.168.1.12: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

Reflexión

¿Cuáles son las ventajas del routing entre VLAN basado en enlaces troncales comparado con el routing entre VLAN con router-on-a-stick?

// Un router-on-a-stick con un ruteo entre vlan permite que una sola interface pueda rutear multiples vlans distinto al ruteo entre vlan que require un punto por vlan

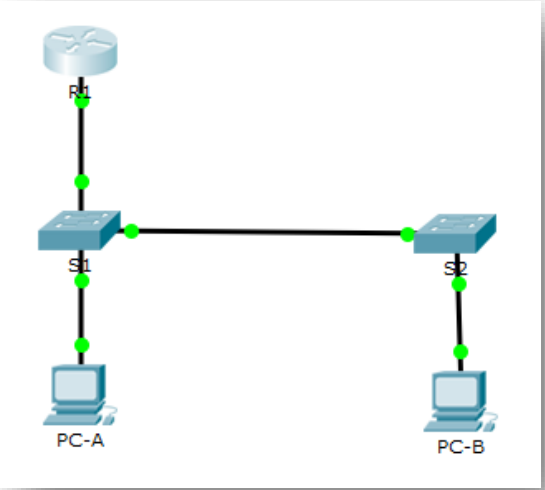


Tabla de resumen de interfaces del router

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

Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
```

Router R1

```
R1(config)# interface g0/1.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

4.1.4.7 configuración de los parámetros básicos del router con CCP

Topología

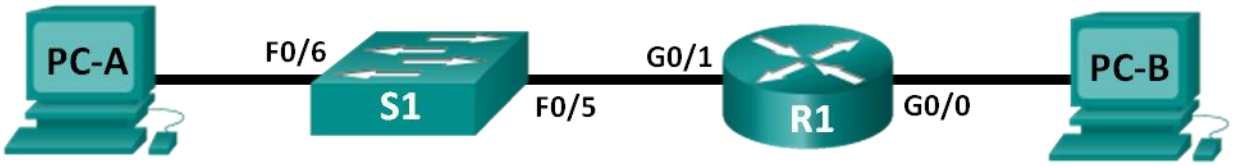


Tabla de direccionamiento

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
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

Parte 3: configurar el router para permitir el acceso de CCP

Parte 4: (optativo) instalar y configurar CCP en la PC-A

Parte 5: configurar los parámetros del R1 con CCP

Parte 6: usar las utilidades de CCP

Información básica/situación

Cisco Configuration Professional (CCP) es una aplicación basada en computadora que proporciona administración de dispositivos basados en GUI para routers de servicios integrados (ISR). Simplifica la configuración del routing, el firewall, la VPN, la WAN, la LAN y otras configuraciones por medio de menús y de asistentes fáciles de utilizar.

En esta práctica de laboratorio, configurará los parámetros del router con la configuración de la práctica de laboratorio anterior en este capítulo. Se debe establecer conectividad de capa 3 entre la PC que ejecuta CCP (PC-A) y el R1 antes de que CCP pueda establecer una conexión. Además, se debe configurar el acceso y la autenticación HTTP en el R1.

Descargará e instalará CCP en la computadora y luego lo utilizará para supervisar el estado de la interfaz del R1, configurará una interfaz, establecerá la fecha y hora, agregará

un usuario a la base de datos local y editará la configuración de vty. También usará algunas de las utilidades incluidas en CCP.

Nota: las configuraciones de router llevadas a cabo con CCP generan los comandos de CLI del IOS. CCP puede ser muy útil para configurar características más complejas del router, ya que no requiere un conocimiento específico de la sintaxis de los comandos de IOS de Cisco.

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.

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)
- 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

Nota: los requisitos del sistema de la computadora para la versión 2.6 de CCP son los siguientes:

- Procesador de 2 GHz o más rápido
- 1 GB de DRAM como mínimo; se recomienda contar con 2 GB
- 400 MB de espacio en disco duro disponible
- Internet Explorer 6.0 o más reciente
- Resolución de pantalla de 1024x768 o superior
- Java Runtime Environment (JRE), versión 1.6.0_11 o más reciente
- Adobe Flash Player, versión 10.0 o más reciente, con la depuración configurada en No

Nota: las interfaces Gigabit Ethernet en los ISR Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 9. Configurar dispositivos y verificar la conectividad

Parte 10. establecer la topología e inicializar los dispositivos

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

a. Conecte los dispositivos que se muestran en el diagrama de la topología y realice el cableado, según sea necesario.

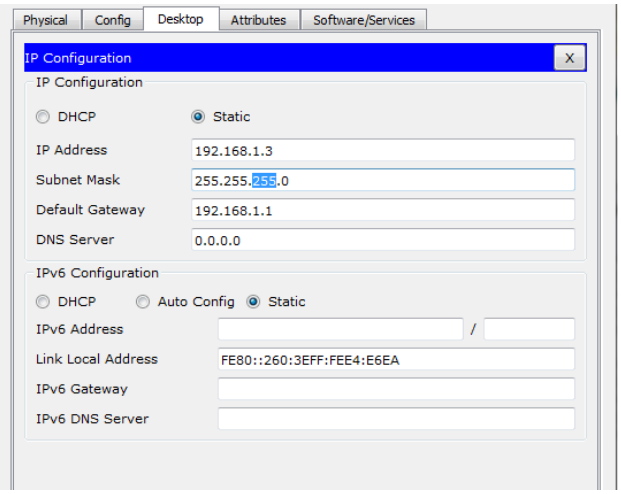
b. Encienda todos los dispositivos de la topología.

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

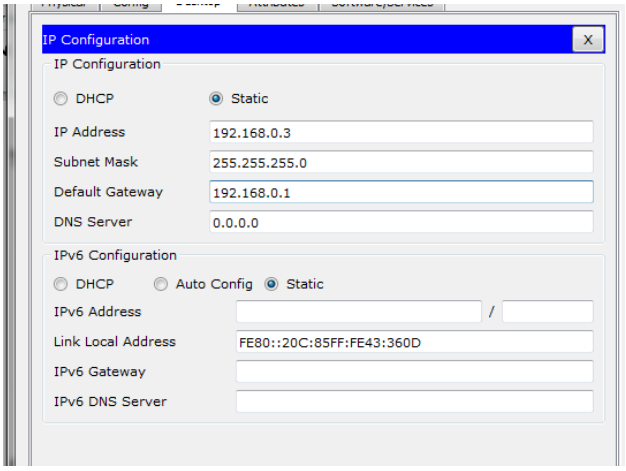
En la parte 2, configurará los parámetros básicos, como las direcciones IP de interfaz (solo G0/1), el acceso seguro a dispositivos y las contraseñas. Consulte la topología y la tabla de direccionamiento para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1. Configure las interfaces de la PC.

c. Configure la dirección IP, la máscara de subred y la configuración del gateway predeterminado en la PC-A.



d. Configure la dirección IP, la máscara de subred y la configuración del gateway predeterminado en la PC-B.



Paso 2. Configurar el router.

Nota: todavía NO configure la interfaz G0/0. Configurará esta interfaz con CCP más adelante en esta práctica de laboratorio.

e. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

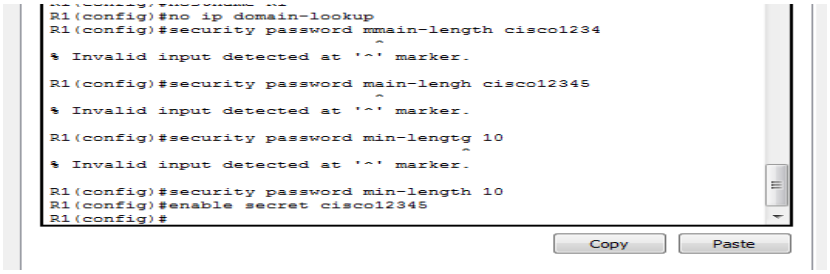
f. Ingrese al modo de configuración global.

g. Desactive la búsqueda del DNS.

h. Asigne un nombre de dispositivo al router.

i. Establezca el requisito de que todas las contraseñas tengan como mínimo 10 caracteres.

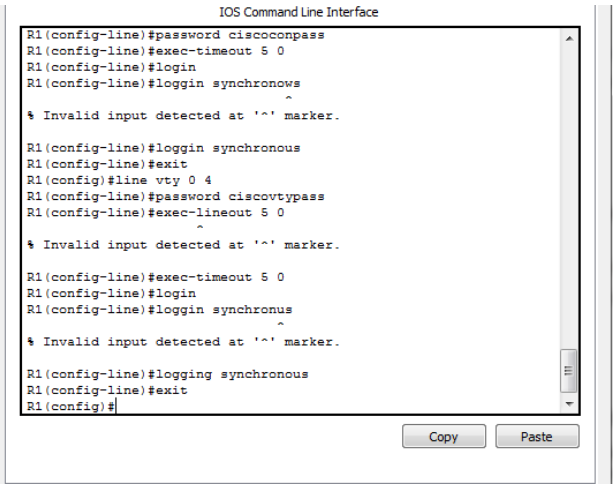
j. Asigne **cisco12345** como la contraseña cifrada del modo EXEC privilegiado.



k. Asigne **ciscoconpass** como la contraseña de consola y habilite el inicio de sesión.

l. Asigne **ciscovtypass** como la contraseña de vty y habilite el inicio de sesión.

m. Configure **logging synchronous** en las líneas de consola y vty.

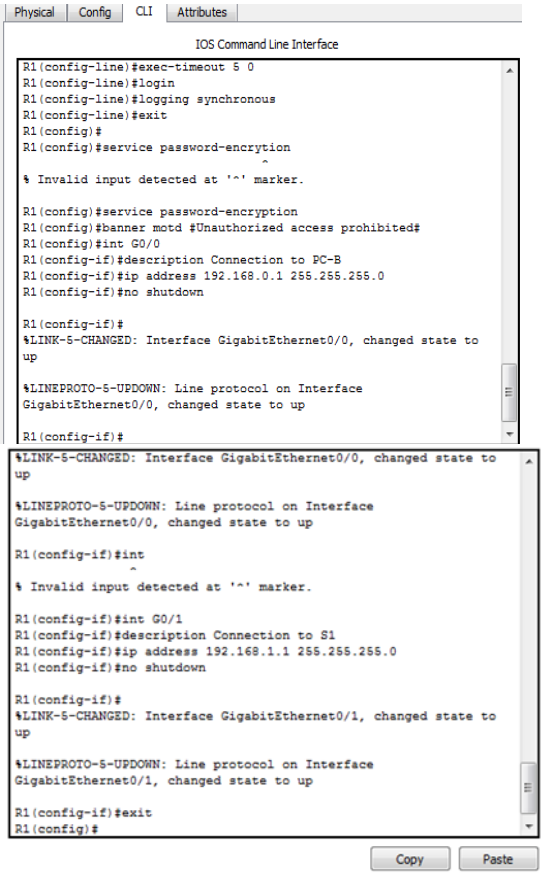


n. Cifre las contraseñas de texto no cifrado.

o. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

p. Configure las direcciones IP y una descripción de la interfaz, y active la interfaz G0/1 en el router.

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



Paso 3. Verificar la conectividad de la red

Verifique que pueda hacer ping a la G0/1 del R1 desde la PC-A.

Parte 11. configurar el router para permitir el acceso de CCP

En la parte 3, configurará el router para permitir el acceso de CCP al habilitar los servicios de servidores HTTP y HTTPS. También habilitará la autenticación HTTP para usar la base de datos local.

Paso 1. habilitar los servicios de servidores HTTP y HTTPS en el router.

R1(config)# **ip http server**
R1(config)# **ip http secure-server**

Paso 2. habilitar la autenticación HTTP para usar la base de datos local en el router.

R1(config)# **ip http authentication local**

Paso 3. configurar el router para el acceso de CCP.

Asigne un usuario en la base de datos local del router para acceder a CCP con el nombre de usuario **admin** y la contraseña **adminpass1**.

R1(config)# **username admin privilege 15 secret adminpass1**

Parte 12. (optativo) instalar y configurar CCP en la PC-A

Paso 1. instalar CCP.

Nota: si CCP ya está instalado en la PC-A, puede omitir este paso.

a. Descargue CCP 2.6 del sitio web de Cisco:

   http://software.cisco.com/download/release.html?mdfid=281795035&softwareid=282159854&release=2.6&rellifecycle=&relind=AVAILABLE&reltype=all

b. Seleccione el archivo **cisco-config-pro-k9-pkg-2_6-en.zip**.

   Nota: verifique si seleccionó el archivo correcto de CCP y no CCP Express. Si hay una versión más actualizada de CCP, puede optar por descargarlo; sin embargo, en esta práctica de laboratorio se usa CCP 2.6.

c. Acepte los términos y condiciones y descargue y guarde el archivo en la ubicación deseada.

d. Abra el archivo ZIP y ejecute el archivo ejecutable de CCP.

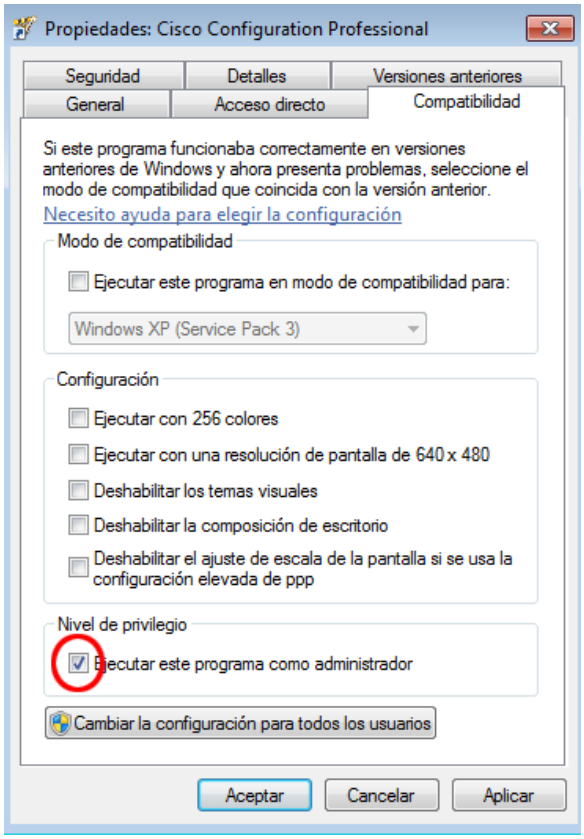
e. Siga las instrucciones en pantalla para instalar CCP 2.6 en la computadora.

Paso 2. cambiar la configuración para ejecutar como administrador.

Si no se ejecuta como administrador, es posible que no pueda iniciar CCP correctamente. Puede cambiar la configuración de inicio para que se ejecute automáticamente en modo administrador.

f. Haga clic con el botón secundario en el ícono del escritorio de **CCP** (o haga clic en el botón **Inicio**) y luego haga clic con el botón secundario en **Cisco Configuration Professional**. En la lista desplegable, seleccione **Propiedades**.

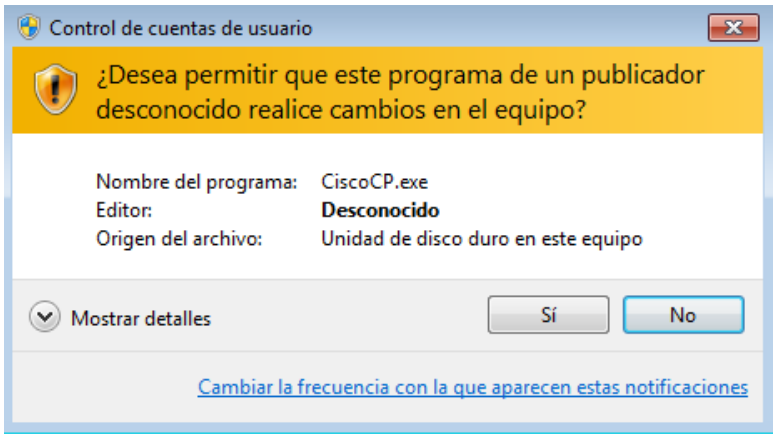
g. En el cuadro de diálogo Properties, seleccione la ficha **Compatibilidad**. En la sección Nivel de privilegio, haga clic en la casilla de verificación **Ejecutar este programa como administrador** y luego haga clic en **Aceptar**.



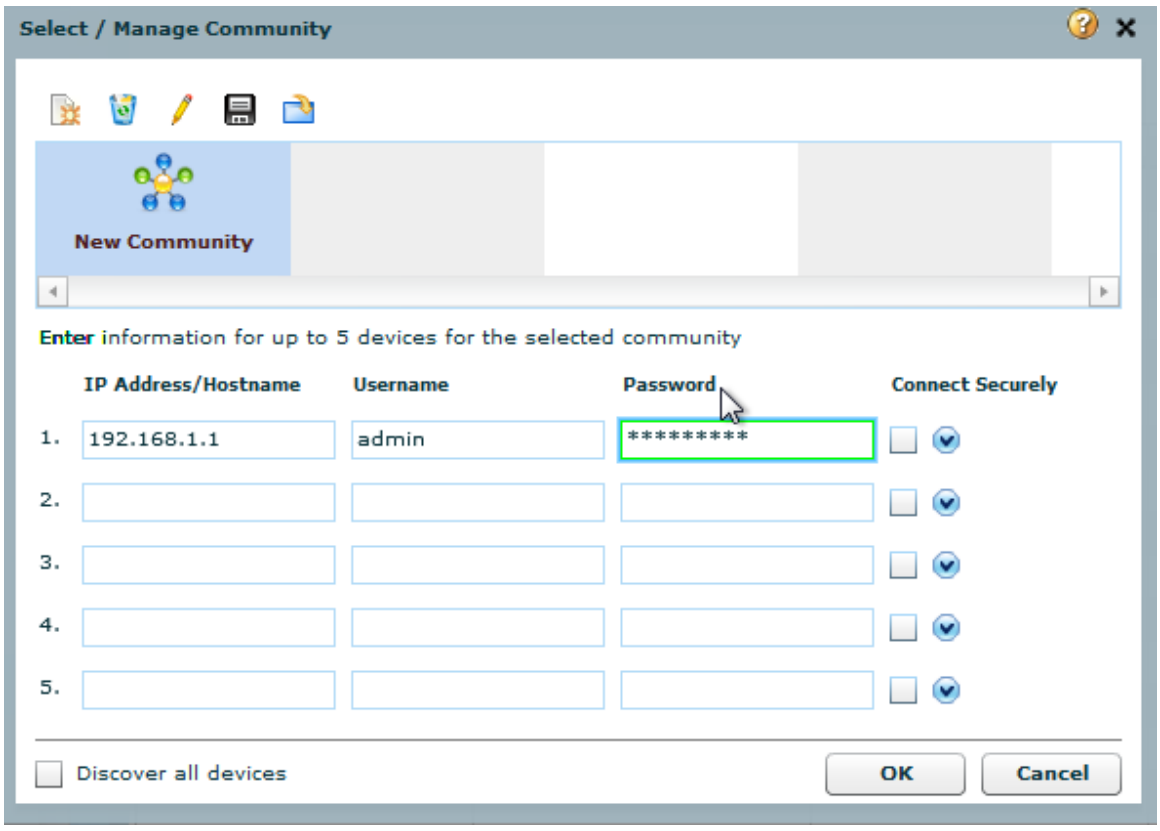
Paso 3. crear o administrar comunidades.

h. En la PC-A, inicie CCP. (Haga doble clic en el ícono del escritorio de CCP o haga clic en **Inicio** > **Cisco Configuration Professional**.

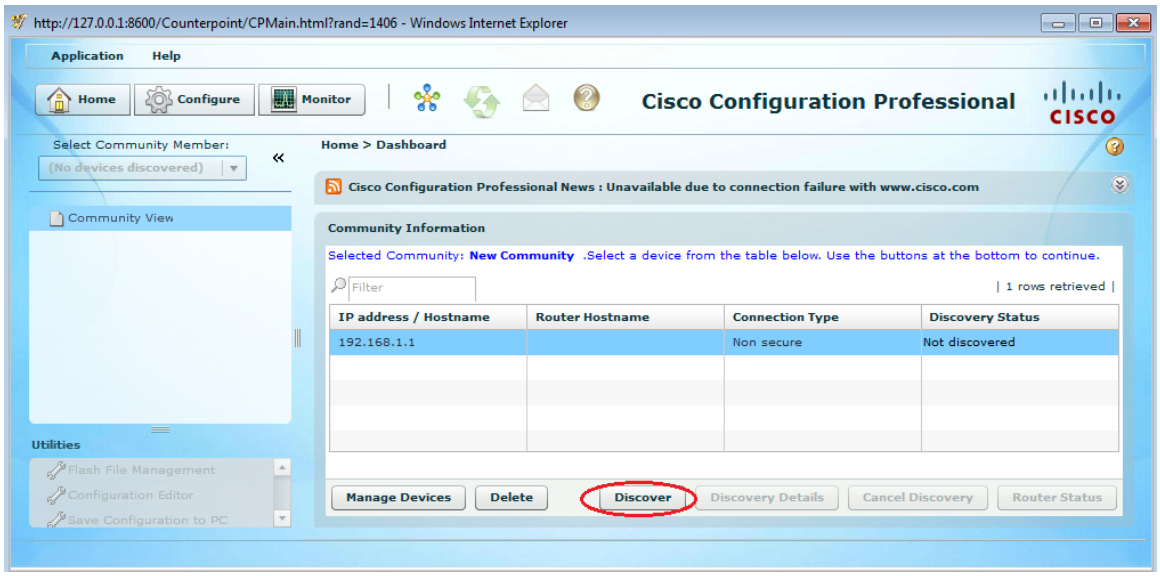
i. Si recibe un mensaje de advertencia de seguridad que le solicita que permita que el programa CiscoCP.exe realice cambios en la computadora, haga clic en **Sí**.



j. Cuando se inicia CCP, aparece el cuadro de diálogo **Select/Manage Community** (Seleccionar/administrar comunidad). Introduzca la dirección IP para la G0/1 del R1, y el nombre de usuario **admin** y la contraseña **adminpass1** que agregó a la base de datos local durante la configuración del router en la parte 2. Haga clic en **Aceptar**.



k. En la venta Community Information (Información de comunidad), haga clic en **Discover** (Detectar).



Si configuró el router correctamente, el Discovery Status (Estado de detección) cambia de **Not discovered** (No detectado) a **Discovered** (Detectado) y el R1 aparece en la columna Router Hostname (Nombre de host del router).

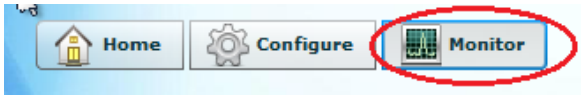
Nota: si hay un problema de configuración, verá el estado Discovery failed (Error de detección). Haga clic en **Discovery Details** (Detalles de detección) para determinar el motivo de la falla en el proceso de detección y luego resuelva el problema.

Parte 13. configurar los parámetros del R1 con CCP

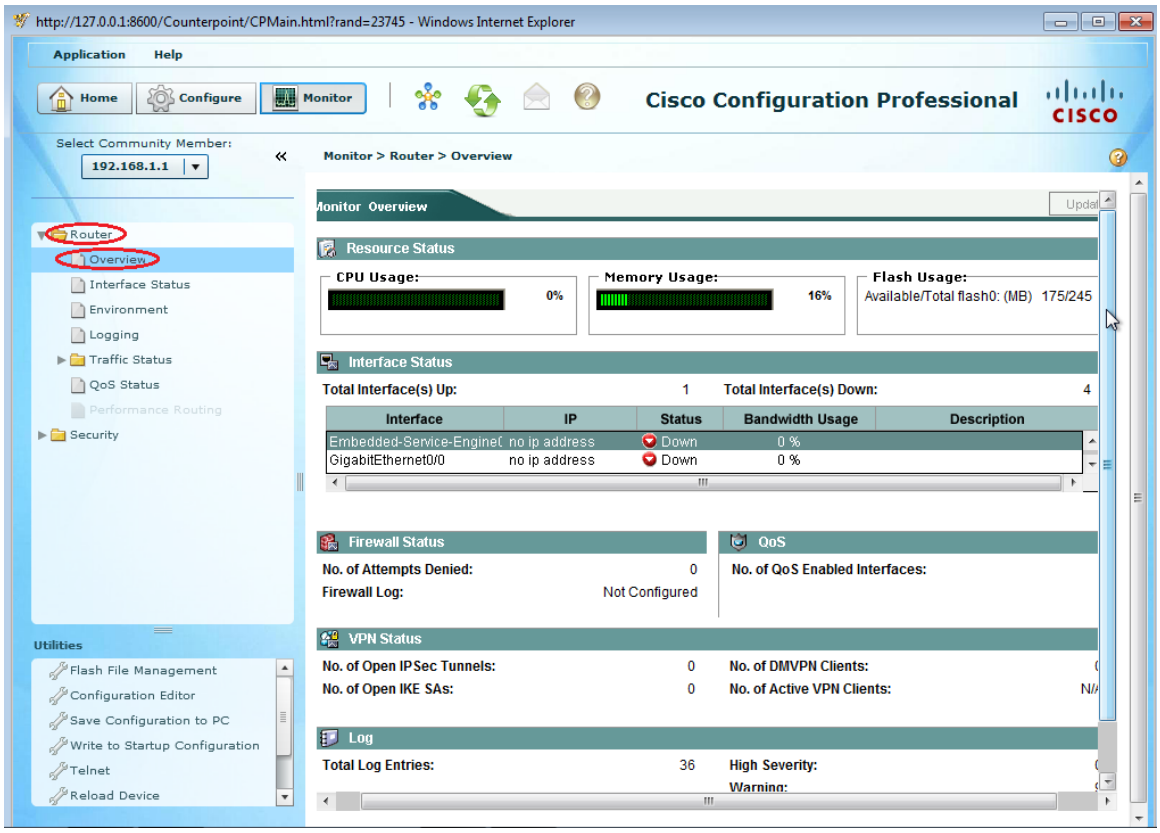
En la parte 5, utilizará CCP para mostrar información sobre el R1, configurará la interfaz G0/0, establecerá la fecha y hora, agregará un usuario a la base de datos local y cambiará la configuración de vty.

Paso 1. ver el estado de las interfaces en el R1.

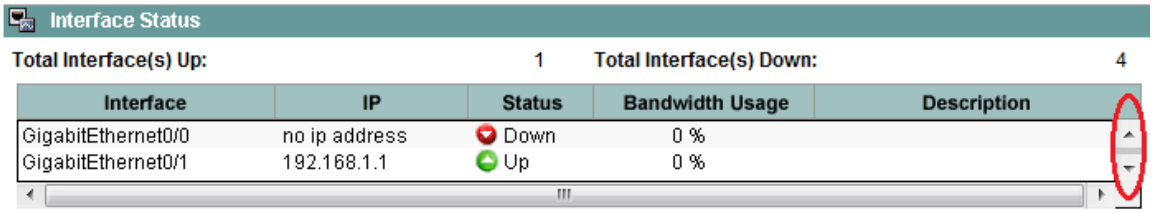
a. En la barra de herramientas de CCP, haga clic en **Monitor**.



b. En el panel de navegación izquierdo, haga clic en **Router** > **Overview** (Router > Descripción general) para visualizar la pantalla Monitor Overview (Descripción general del monitor) en el panel de contenido derecho.

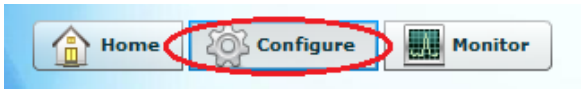


c. Utilice las flechas arriba y abajo en el lado derecho de la lista de interfaces para desplazarse por la lista de interfaces del router.

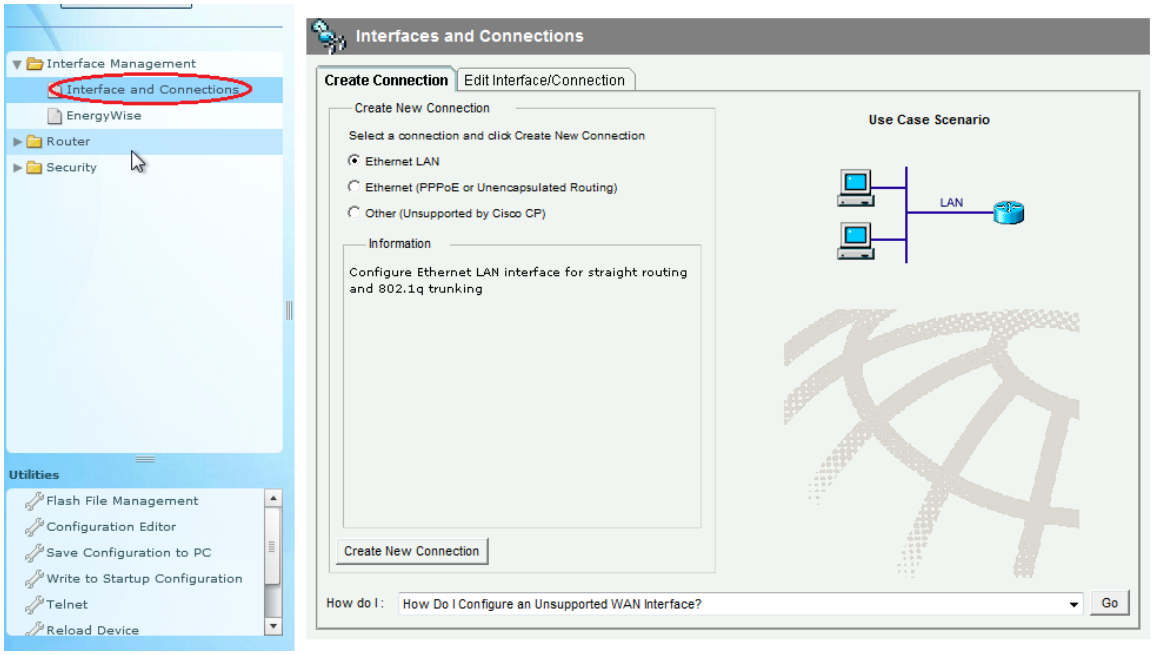


Paso 2. usar el asistente de LAN Ethernet para configurar la interfaz G0/0.

d. En la barra de herramientas de CCP, haga clic en **Configure** (Configurar).



e. En el panel de navegación izquierdo, haga clic en **Interface Management** (Administración de interfaz) > **Interface and Connections** (Interfaz y conexiones) para visualizar la pantalla Interfaces and Connections (Interfaces y conexiones) en el panel de contenido derecho.



f. Haga clic en **Create New Connection** (Crear conexión nueva) para iniciar el asistente de LAN Ethernet.

g. Cuando se le solicite habilitar AAA en el router, haga clic en **No**.

h. Haga clic en **Next** (Siguiente) para avanzar por el proceso de creación de interfaces Ethernet de capa 3.

i. Mantenga seleccionado el botón de opción **Configure this interface for straight routing** (Configurar esta interfaz para routing directo) y haga clic en **Next**.

j. Introduzca **192.168.0.1** en el campo de dirección IP y **255.255.255.0** en el campo de máscara de subred y luego haga clic en **Next**.

k. Mantenga seleccionado el botón de opción **No** en la pantalla del servidor de DHCP y haga clic en **Next**.

l. Revise la pantalla de resumen y haga clic en **Finish** (Finalizar).

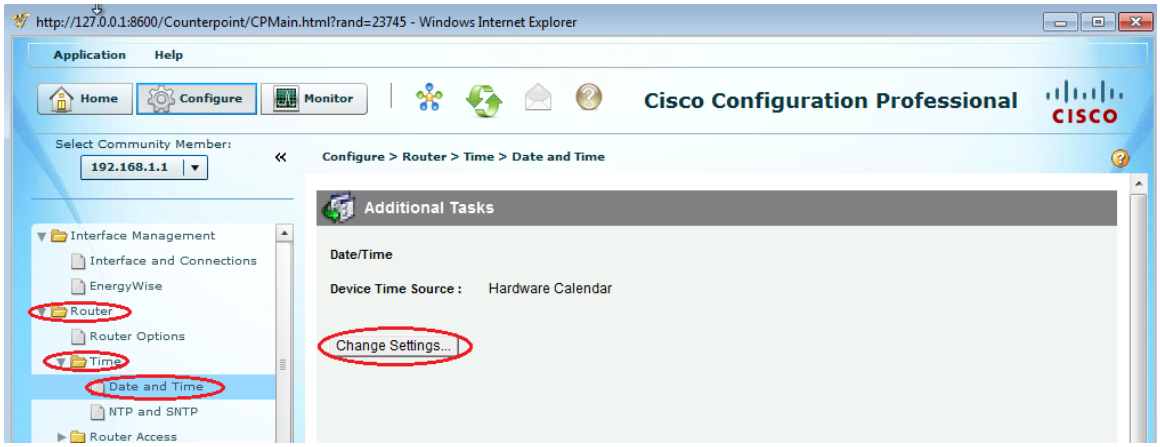
m. Haga clic en la casilla de verificación **Save running config to device's startup config** (Guardar configuración en ejecución en la configuración de inicio del dispositivo) y luego haga clic en **Deliver** (Entregar). Esta acción agrega los comandos que aparecen en la ventana de vista previa a la configuración en ejecución y luego guarda esta última en la configuración de inicio en el router.

n. Aparece la ventana Commands Delivery Status (Estado de entrega de comandos). Haga clic en **OK** para cerrar la ventana. Volverá a la pantalla Interfaces and Connections. G0/0 ahora debería estar de color verde y debería aparecer como Up (Activa) en la columna Status (Estado).

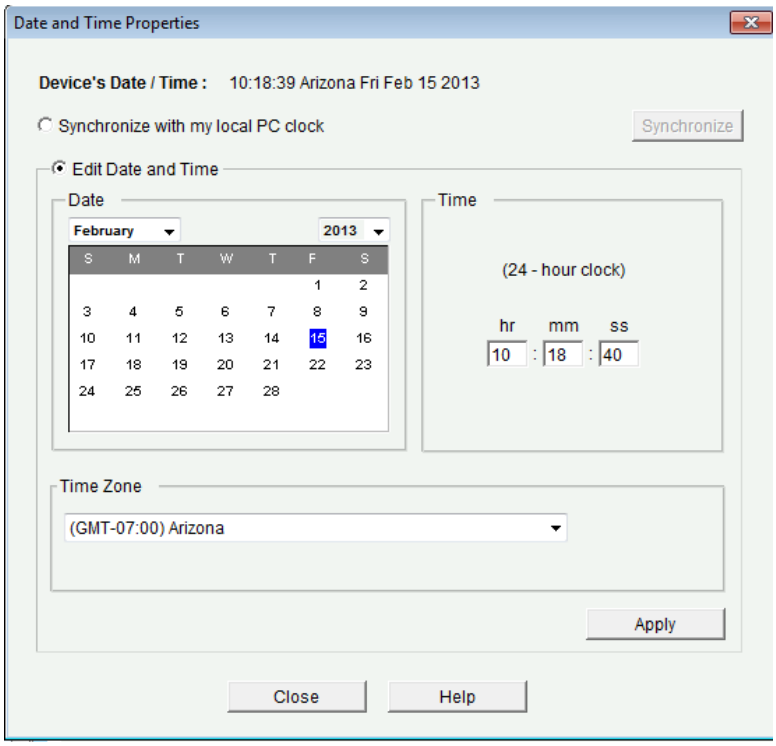
Interface	IP	Type	Slot	Status	Description
Embedded-Service-Engi	no IP address	Embedded-Service-Engine	0	Dow	
GigabitEthernet0/0	192.168.0.1	GigabitEthernet	0	Up	
GigabitEthernet0/1	192.168.1.1	GigabitEthernet	0	Up	Connection to S1 F0/5
Serial0/0/0	no IP address	Serial	0	Dow	
Serial0/0/1	no IP address	Serial	0	Dow	

Paso 3. establecer fecha y hora en el router.

o. En el panel de navegación izquierdo, seleccione **Router** > **Time** > **Date and Time** (Router > Hora > Fecha y hora) para que aparezca la pantalla Additional Tasks > Date/Time (Tareas adicionales > Fecha/hora) en el panel de contenido derecho. Haga clic en **Change Settings...** (Cambiar configuración).



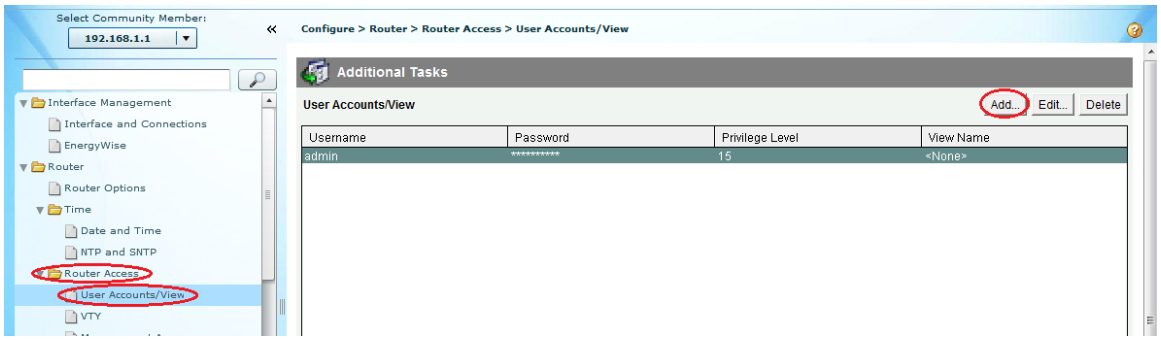
p. En la ventana Date and Time Properties (Propiedades de fecha y hora), edite Date (Fecha), Time (Hora) y Time Zone (Zona horaria). Haga clic en **Apply (Aplicar).**



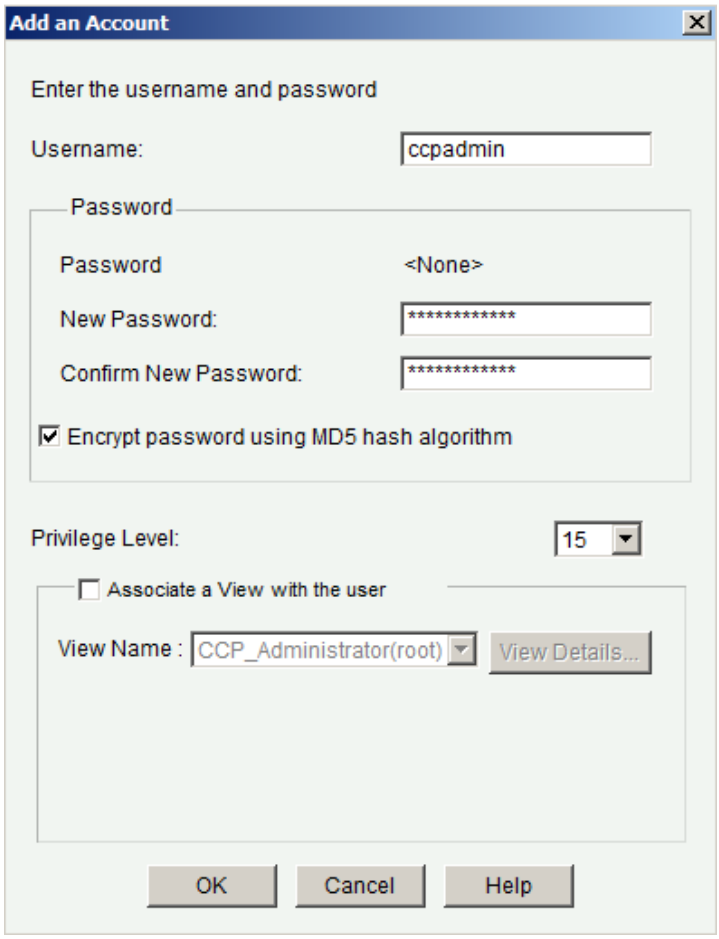
q. En la ventana de configuración del reloj de Router, haga clic en **OK**. En la ventana Date and Time Properties, haga clic en **Close** (Cerrar).

Paso 4. Agregue una cuenta de usuario nueva a la base de datos local.

r. En el panel de navegación izquierdo, seleccione **Router** > **Router Access** > **User Accounts/View** (Router > Acceso al router > Cuentas de usuario/Ver) para visualizar la pantalla Additional Tasks > User Accounts/View en el panel de contenido derecho. Haga clic en el botón **Add…** (Agregar).

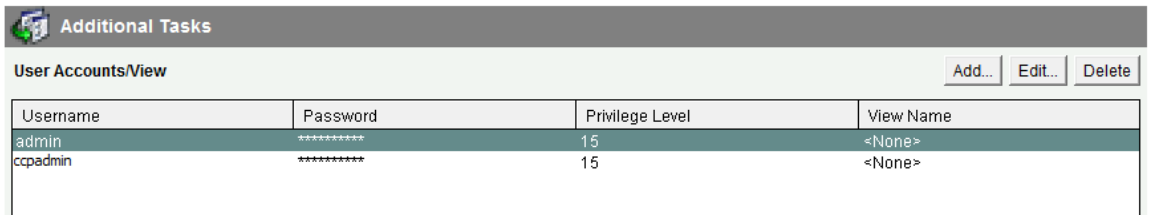


s. Introduzca **ccpadmin** en el campo Username: (Nombre de usuario:). Introduzca **ciscoccppass** en los campos New Password: (Contraseña nueva:) y Confirm New Password: (Confirmar contraseña nueva:). Seleccione **15** en la lista desplegable Privilege Level: (Nivel de privilegio). Haga clic en **OK** para agregar este usuario a la base de datos local.



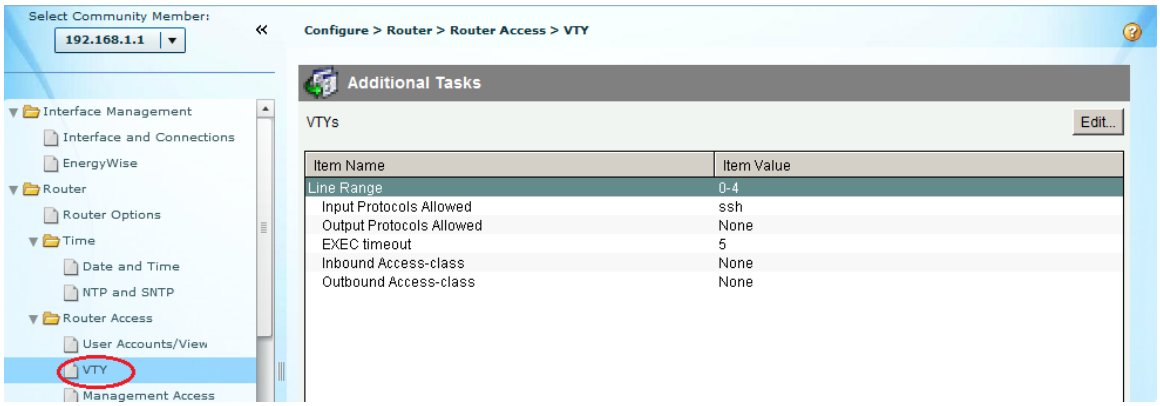
t. En la ventana Deliver Configuration to Device (Entregar configuración al dispositivo), haga clic en la casilla de verificación **Save running config to device's startup config** y luego haga clic en **Deliver**.

u. Revise la información en la ventana Commands Delivery Status y haga clic en **OK**. La cuenta de usuario nueva debería aparecer en el panel de contenido derecho.

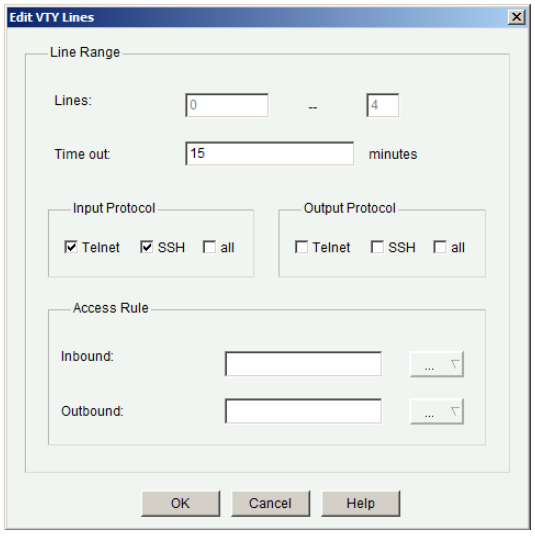


Paso 5. editar la configuración de las líneas vty.

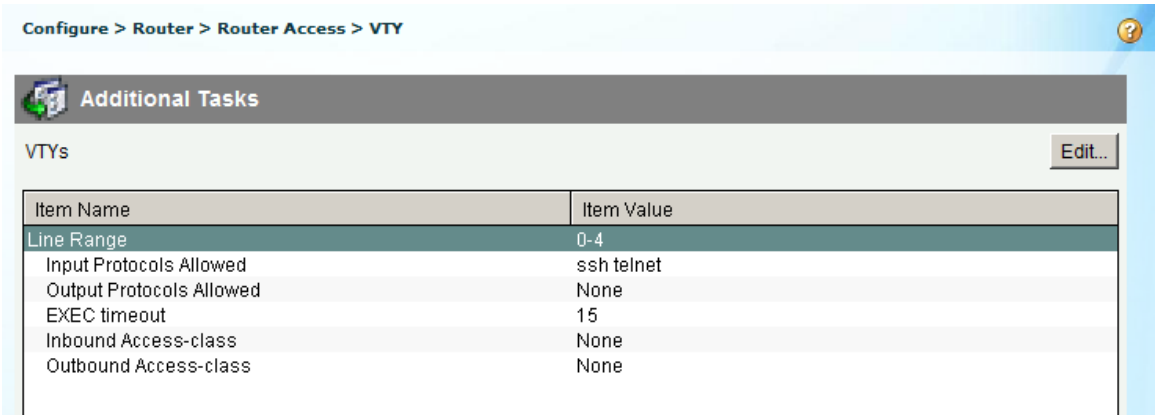
v. En el panel de navegación izquierdo, seleccione **Router Access** > **VTY** (Acceso al router > VTY) para visualizar la ventana Additional Tasks > VTYs (Tareas adicionales > VTY) en el panel de contenido derecho. Haga clic en **Edit…** (Editar).



w. En la ventana Edit VTY Lines (Editar líneas vty), modifique el campo Time out: (Tiempo de espera) y establézcalo en **15** minutos. Haga clic en la casilla de verificación **Input Protocol** > **Telne**t (Protocolo de entrada > Telnet). Revise las otras opciones disponibles. También seleccione la casilla de verificación **SSH**. A continuación, haga clic en **Aceptar**.



x. En la pantalla Deliver Configuration to Device, revise los comandos que se entregarán a la configuración en ejecución y haga clic en **Deliver**. En la ventana Commands Delivery Status, haga clic en **OK**. El panel de contenido derecho debería reflejar los cambios efectuados en el valor de tiempo de espera de ejecución.

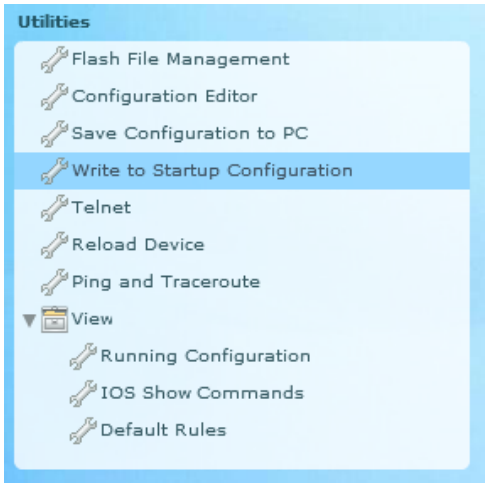


Parte 14. usar utilidades de CCP

En la parte 6, utilizará el panel Utilities (Utilidades) para guardar la configuración en ejecución del router en la configuración de inicio. Usará la utilidad Ping para probar la conectividad de red y la utilidad View (Ver) para visualizar la configuración en ejecución del router. Por último, cerrará CCP.

Paso 1. guardar la configuración en ejecución del router en la configuración de inicio.

a. En la parte inferior del panel de navegación izquierdo, busque el panel Utilities (Utilidades). Haga clic en **Write to Startup Configuration** (Escribir en la configuración de inicio).

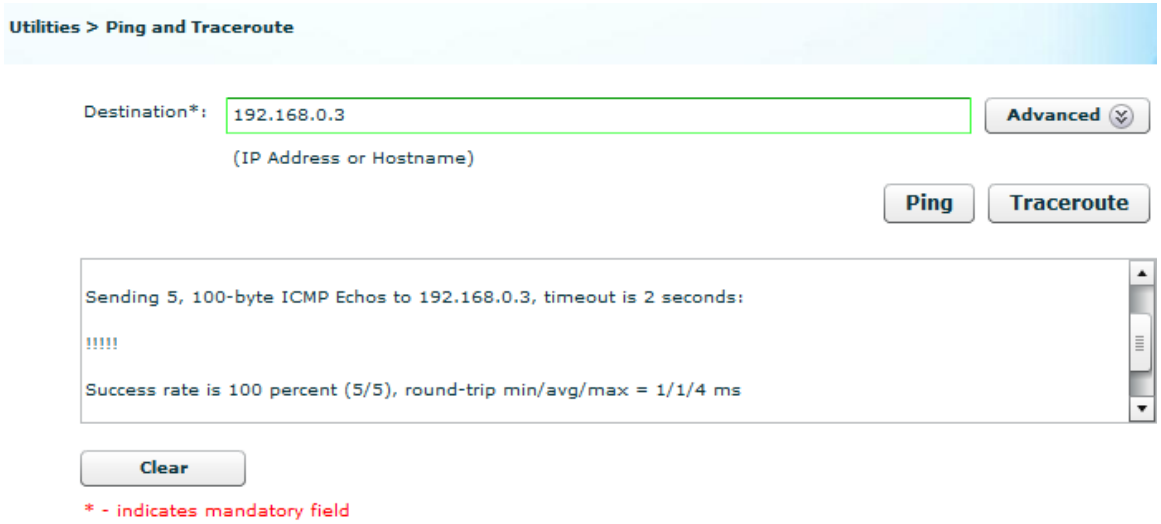


b. El panel de contenido muestra una pantalla de confirmación. Haga clic en **Confirmar**. Aparece una ventana que le informa que la configuración se guardó correctamente. Haga clic en **Aceptar**.

Paso 2. usar la utilidad Ping para probar la conectividad a la PC-B.

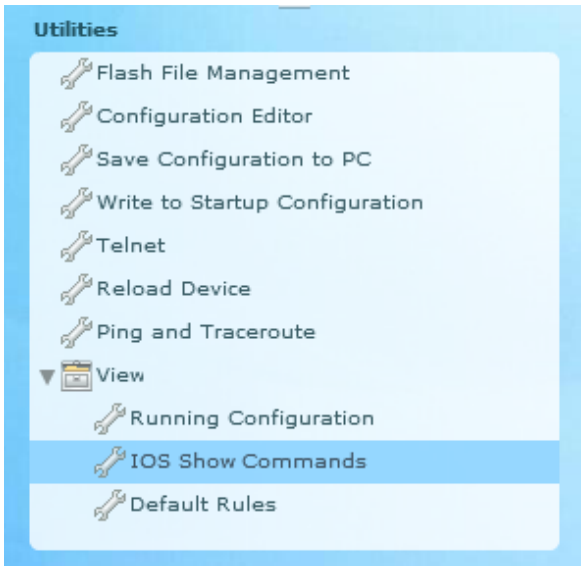
c. En el panel Utilities (Utilidades), haga clic en **Ping and Traceroute** (Ping y traceroute) para mostrar la pantalla Ping and Traceroute en el panel de contenido. Introduzca **192.168.0.3** en el campo Destination*: (Destino*:) y luego haga clic en

Ping. Use la barra de desplazamiento ubicada a la derecha del cuadro de resultados para ver los resultados del ping.

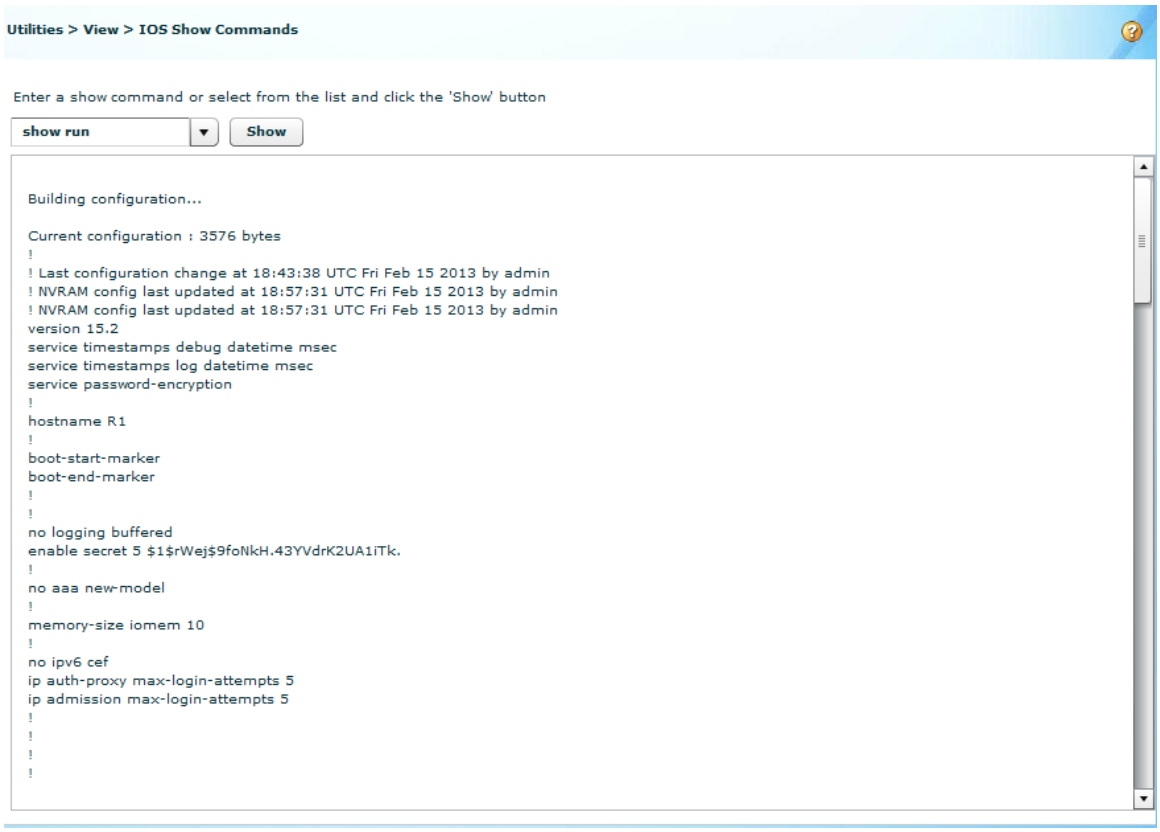


Paso 3. Use la utilidad View para visualizar la configuración en ejecución del router.

d. En el panel Utilities, haga clic en **View** > **IOS Show Commands** (Ver > Comandos show de IOS) para visualizar la pantalla IOS Show Commands en el panel de contenido.

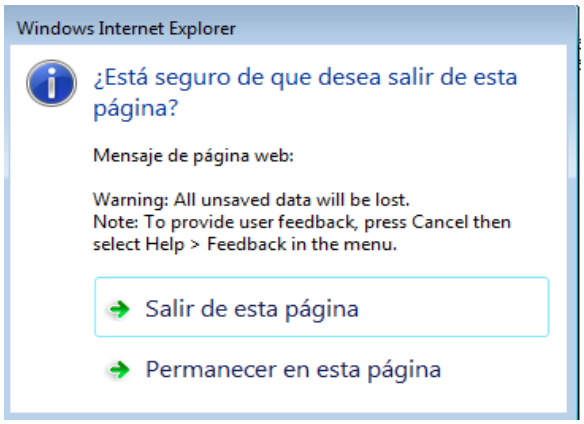


e. Seleccione **show run** en la lista desplegable y haga clic en **Show** (Mostrar). La configuración en ejecución del router se muestra en el panel de contenido.



Paso 4. cerrar CCP.

Cierre la ventana de CCP. Cuando aparezca una ventana de confirmación de Windows Internet Explorer, haga clic en **Salir de esta página**.



Reflexión

1. ¿Qué protocolo de transporte usa CCP para acceder al router, y qué comandos se usan para permitir el acceso?

   CCP utiliza el protocolo HTTP o HTTPS para acceder al router. Para permitir el acceso de CCP, se usan los comandos ip http server o ip http secure-server

2. ¿Qué comando del router le indica a CCP que use la base de datos local para la autenticación?

   ip http authentication local

3. ¿Qué otros comandos **show** se encuentran disponibles en el panel Utilities de CCP?

   Las respuestas pueden variar, pero incluyen: show run, show flash, show startup-config,startup-config, show access-lists, show diag, show interfaces, show version, show tech-support, show environment.

4. ¿Por qué usaría CCP en vez de la CLI del IOS?

   Si tiene que configurar características complejas como una VPN o un firewall, CCP puede facilitar el proceso con menús y asistentes, y no requiere que tenga un conocimiento profundo de los comandos IOS. Además, al introducir comandos de IOS, se pueden cometer errores de pulsación de tecla. CCP genera los comandos de IOS equivalentes.

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.				

2.2.4.11 Lab - Configuring Switch Security Features

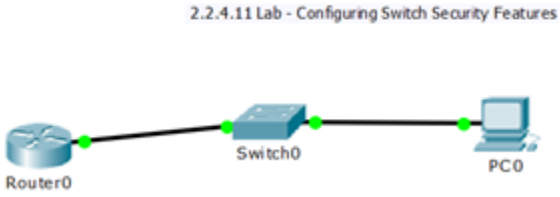
Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

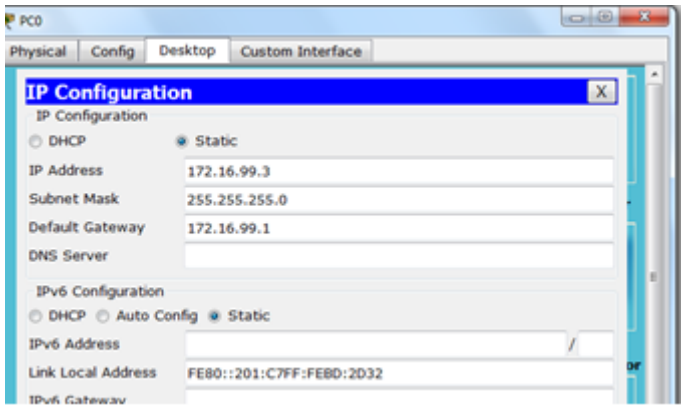
Parte 15. establecer la topología e inicializar los dispositivos

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



Parte 16. Configurar los parámetros básicos de los dispositivos y verificar la conectividad

Paso 1. Configurar una dirección IP en la PC-A.



Paso 2. configurar los parámetros básicos en el R1.

a. Configure el nombre del dispositivo.

b. Desactive la búsqueda del DNS.

c. Configure la dirección IP de interfaz que se muestra en la tabla de direccionamiento.

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

e. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

f. Cifre las contraseñas de texto no cifrado.

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

Paso 3. configurar los parámetros básicos en el S1.

h. Configure el nombre del dispositivo.

i. Desactive la búsqueda del DNS.

j. Asigne **class** como la contraseña del modo EXEC privilegiado**.**

k. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y luego habilite el inicio de sesión.

l. Configure un gateway predeterminado para el S1 con la dirección IP del R1.

m. Cifre las contraseñas de texto no cifrado.

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

o. Cree la VLAN 99 en el switch y asígnele el nombre **Management**.

p. Configure la dirección IP de la interfaz de administración VLAN 99, tal como se muestra en la tabla de direccionamiento, y habilite la interfaz.

q. Emita el comando **show vlan** en el S1. ¿Cuál es el estado de la VLAN 99? **ACTIVA**

```
S1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
99   Management                       active
```

Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo para la interfaz de administración VLAN 99?

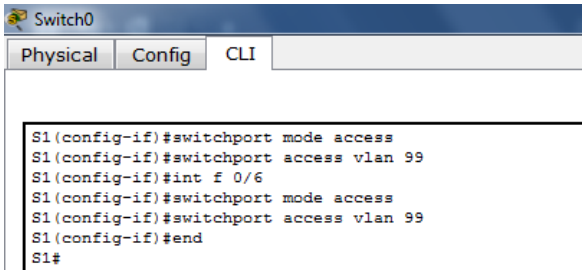
El estado es UP y el protocolo está en DOWN

```
Vlan99                 172.16.99.11    YES manual up                    down
S1#
```

r. ¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando **no shutdown** para la interfaz VLAN 99?

Porque la VLAN 99 no tiene ningún puerto asignado.

s. Asigne los puertos F0/5 y F0/6 a la VLAN 99 en el switch.

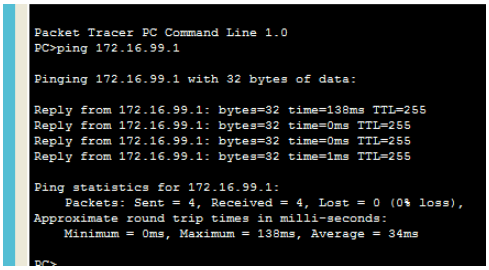


t. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99? **El estado continua en UP pero el protocolo ahora esta en DOWN**

```
Vlan1                  unassigned      YES manual administratively down dow

Vlan99                 172.16.99.11    YES manual up                    up
S1#
```

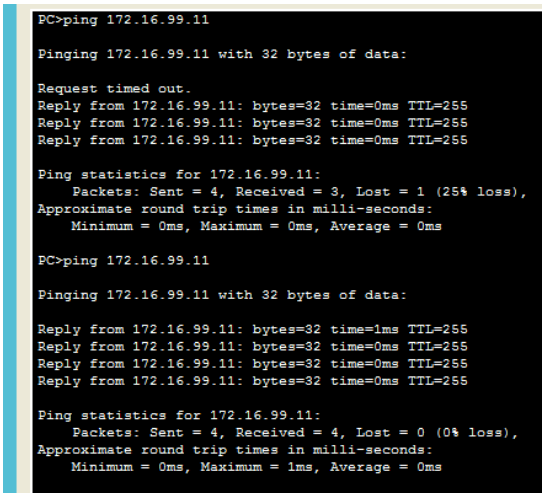
Paso 4. verificar la conectividad entre los dispositivos.

u. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? **SI**



```
Packet Tracer PC Command Line 1.0
PC>ping 172.16.99.1

Pinging 172.16.99.1 with 32 bytes of data:

Reply from 172.16.99.1: bytes=32 time=138ms TTL=255
Reply from 172.16.99.1: bytes=32 time=0ms TTL=255
Reply from 172.16.99.1: bytes=32 time=0ms TTL=255
Reply from 172.16.99.1: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 138ms, Average = 34ms

PC>
```

v. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente? **Inicialmente se pierde un paquete pero al repetir el comando los ping se realizan correctamente**

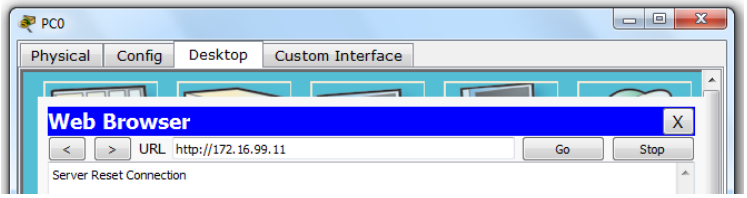


```
PC>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255

Ping statistics for 172.16.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

Reply from 172.16.99.11: bytes=32 time=1ms TTL=255
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255
Reply from 172.16.99.11: bytes=32 time=0ms TTL=255

Ping statistics for 172.16.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

w. En el S1, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? **SI**

```
S1>en
Password:
S1#ping 172.16.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/8/32 ms

S1#ping 172.16.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

x. En la PC-A, abra un navegador web y acceda a http://172.16.99.11. Si le solicita un nombre de usuario y una contraseña, deje el nombre de usuario en blanco y utilice la contraseña **class**. Si le solicita una conexión segura, conteste **No.** ¿Pudo acceder a la interfaz web en el S1? **No hay conexión**



y. Cierre la sesión del explorador en la PC-A.

Parte 17. configurar y verificar el acceso por SSH en el S1

Paso 1. configurar el acceso por SSH en el S1.

a. Habilite SSH en el S1. En el modo de configuración global, cree el nombre de dominio **CCNA-Lab.com**.

b. Cree una entrada de base de datos de usuarios local para que se utilice al conectarse al switch a través de SSH. El usuario debe tener acceso de nivel de administrador.

c. Configure la entrada de transporte para que las líneas vty permitan solo conexiones SSH y utilicen la base de datos local para la autenticación.

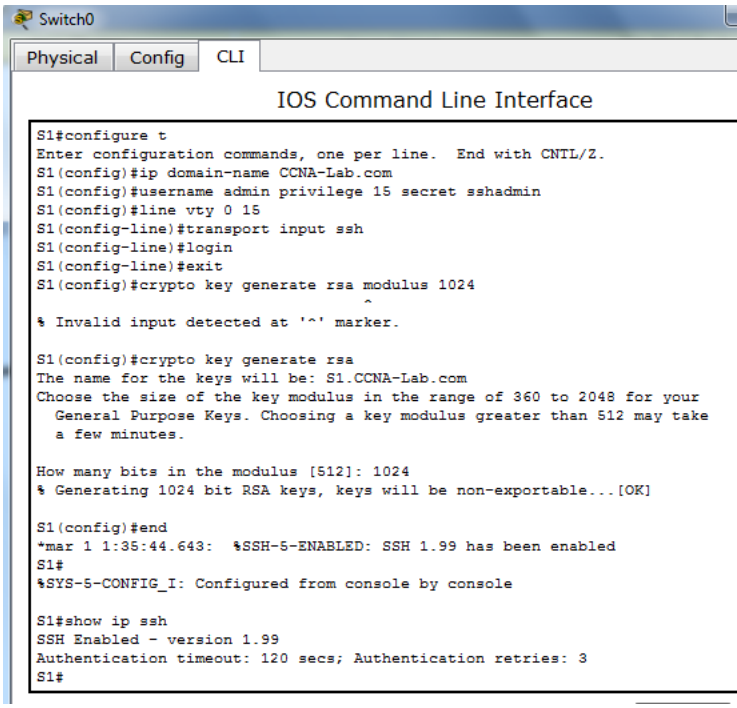
d. Genere una clave criptográfica RSA con un módulo de 1024 bits.

e. Verifique la configuración de SSH y responda las siguientes preguntas.

¿Qué versión de SSH usa el switch? **VERSION 1.99**

¿Cuántos intentos de autenticación permite SSH? **3**

¿Cuál es la configuración predeterminada de tiempo de espera para SSH? **120 SEGUNDOS**



Paso 2. modificar la configuración de SSH en el S1.

Modifique la configuración predeterminada de SSH.

¿Cuántos intentos de autenticación permite SSH? **2**

¿Cuál es la configuración de tiempo de espera para SSH? **75 Segundos**

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip ssh time-out 75
S1(config)#ip ssh aut
S1(config)#ip ssh authentication-retries 2
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Parte 18. configurar y verificar las características de seguridad en el S1

Paso 1. configurar las características de seguridad general en el S1.

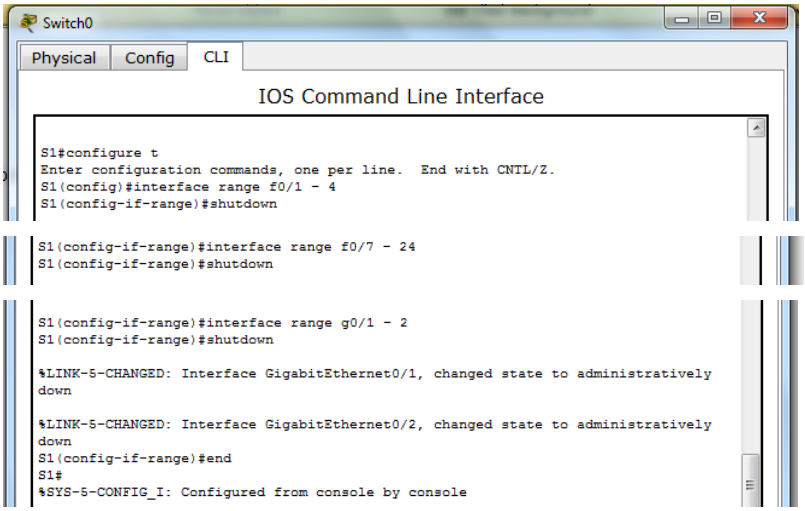
a. Configure un aviso de mensaje del día (MOTD) en el S1 con un mensaje de advertencia de seguridad adecuado.

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd $
Enter TEXT message.  End with the character '$'.
Prohibido el acceso sin ser autorizado$

S1(config)#exit
S1#
```

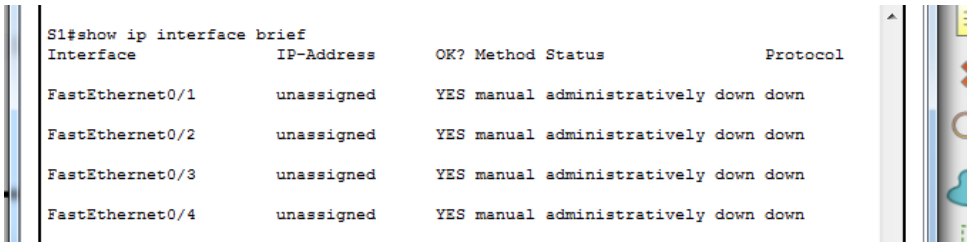
b. Emita un comando **show ip interface brief** en el S1. ¿Qué puertos físicos están activos?

Están activos Todos los puertos

c. Desactive todos los puertos sin utilizar en el switch. Use el comando **interface range**.



d. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado de los puertos F0/1 a F0/4? **ADMINISTRATIVELY DOWN**



e. Emita el comando **show ip http server status**.

EL PACKET TRACER NO PERMITE INGRESAR ESTOS COMANDOS

¿Cuál es el estado del servidor HTTP? _____

¿Qué puerto del servidor utiliza? _____

¿Cuál es el estado del servidor seguro de HTTP? _____

¿Qué puerto del servidor seguro utiliza? _____

f. Las sesiones HTTP envían todo como texto no cifrado. Deshabilite el servicio HTTP que se ejecuta en el S1.

```
S1(config)# no ip http server
```

g. En la PC-A, abra una sesión de navegador web a http://172.16.99.11. ¿Cuál fue el resultado?

_____
_____

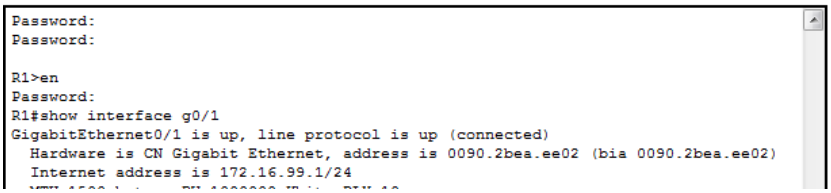
h. En la PC-A, abra una sesión segura de navegador web en https://172.16.99.11. Acepte el certificado. Inicie sesión sin nombre de usuario y con la contraseña **class**. ¿Cuál fue el resultado?

_____
_____

i. Cierre la sesión web en la PC-A.

Paso 2. configurar y verificar la seguridad de puertos en el S1.

j. Registre la dirección MAC de G0/1 del R1. Desde la CLI del R1, use el comando **show interface g0/1** y registre la dirección MAC de la interfaz.

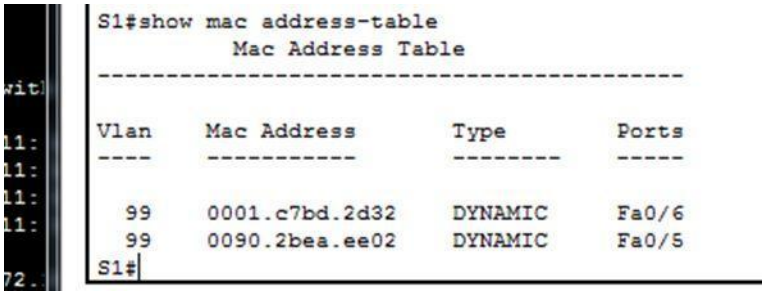


¿Cuál es la dirección MAC de la interfaz G0/1 del R1? **0090.2bea.ee02**

k. Desde la CLI del S1, emita un comando **show mac address-table** en el modo EXEC privilegiado. Busque las entradas dinámicas de los puertos F0/5 y F0/6. Regístrelos a continuación.

Dirección MAC de F0/5: **0090.2bea.ee02**

Dirección MAC de F0/6: **0001.c7bd.2d32**



l. Configure la seguridad básica de los puertos.

1) Desde la CLI del S1, ingrese al modo de configuración de interfaz para el puerto que se conecta al R1.

2) Desactive el puerto.

3) Habilite la seguridad de puertos en F0/5.

4) Configure una entrada estática para la dirección MAC de la interfaz G0/1 del R1 registrada en el paso 2a.

5) Habilite el puerto del switch.

m. Verifique la seguridad de puertos en F0/5 del S1 mediante la emisión de un comando **show port-security interface**.

¿Cuál es el estado del puerto de F0/5? **Seguridad activada**

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/5
S1(config-if)#shut

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to dow

S1(config-if)#switchport port-security
S1(config-if)#switchport port-securitymac-address 0090.2bea.ee02
                                  ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security mac-address 0090.2bea.ee02
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

S1(config-if)#exit
S1(config)#end
S1#
```

```
S1(config-if)#exit
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show port-security interface
% Incomplete command.
S1#show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0090.2BEA.EE02:99
Security Violation Count   : 0
```

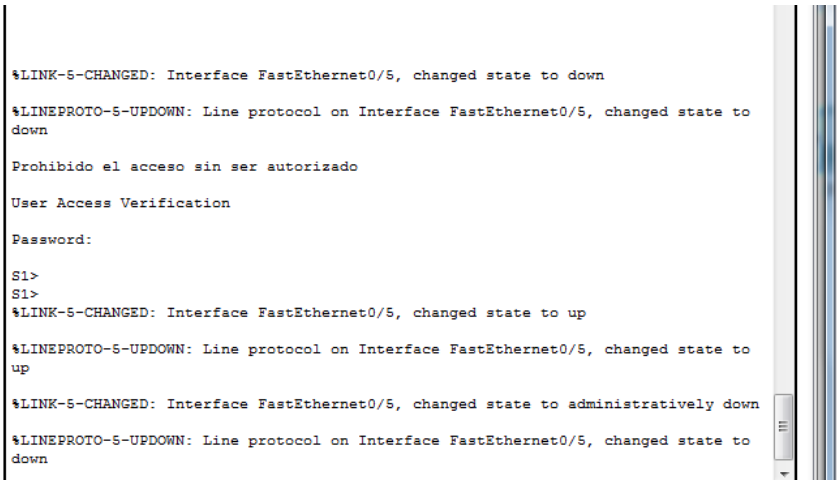
n. En el símbolo del sistema del R1, haga ping a la PC-A para verificar la conectividad.

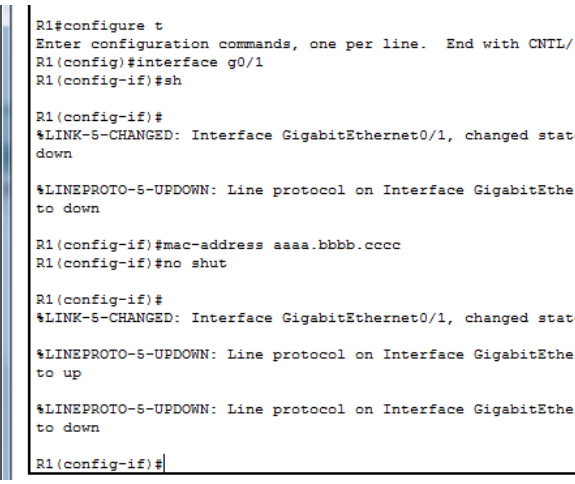
```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#
```

o. Ahora violará la seguridad mediante el cambio de la dirección MAC en la interfaz del router. Ingrese al modo de configuración de interfaz para G0/1 y desactívela.

p. Configure una nueva dirección MAC para la interfaz, con la dirección **aaaa.bbbb.cccc**.

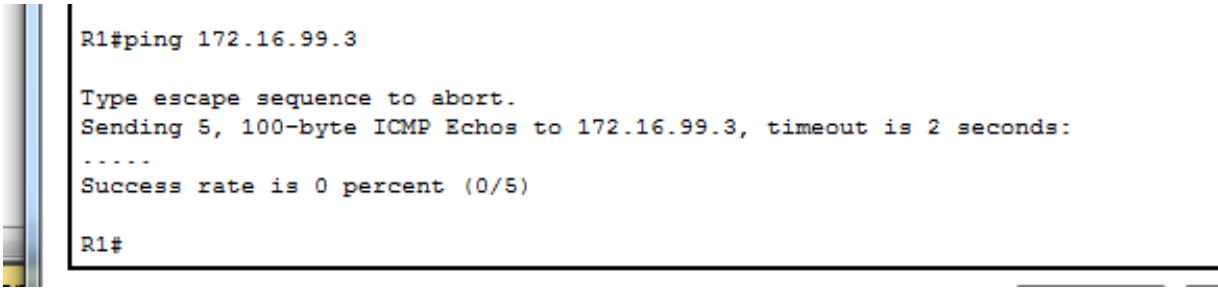
q. De ser posible, tenga una conexión de consola abierta en el S1 al mismo tiempo que realiza este paso. Verá que se muestran varios mensajes en la conexión de consola al S1 que indican una violación de seguridad. Habilite la interfaz G0/1 en R1.





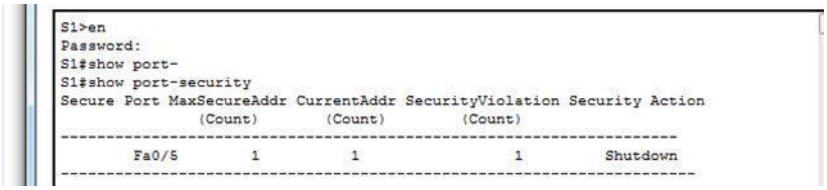
r. En el modo EXEC privilegiado del R1, haga ping a la PC-A. ¿El ping se realizó correctamente? ¿Por qué o por qué no?

No se realizo correctamente por que el puerto de enlace del switch S1 tiene una dirección MAC diferente



s. En el switch, verifique la seguridad de puertos con los comandos que se muestran a continuación.

S1# **show port-security**



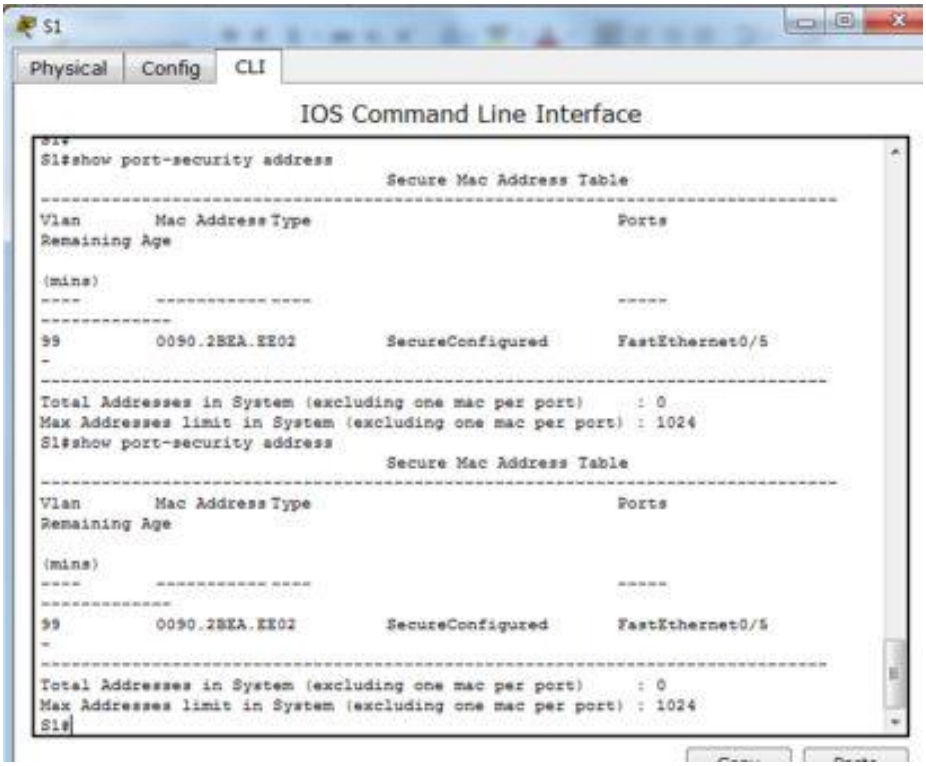
S1# **show port-security interface f0/5**

```
S1#show port-security interface f 0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : AAAA.BBBB.CCCC:99
Security Violation Count   : 1
```

S1# **show interface f0/5**

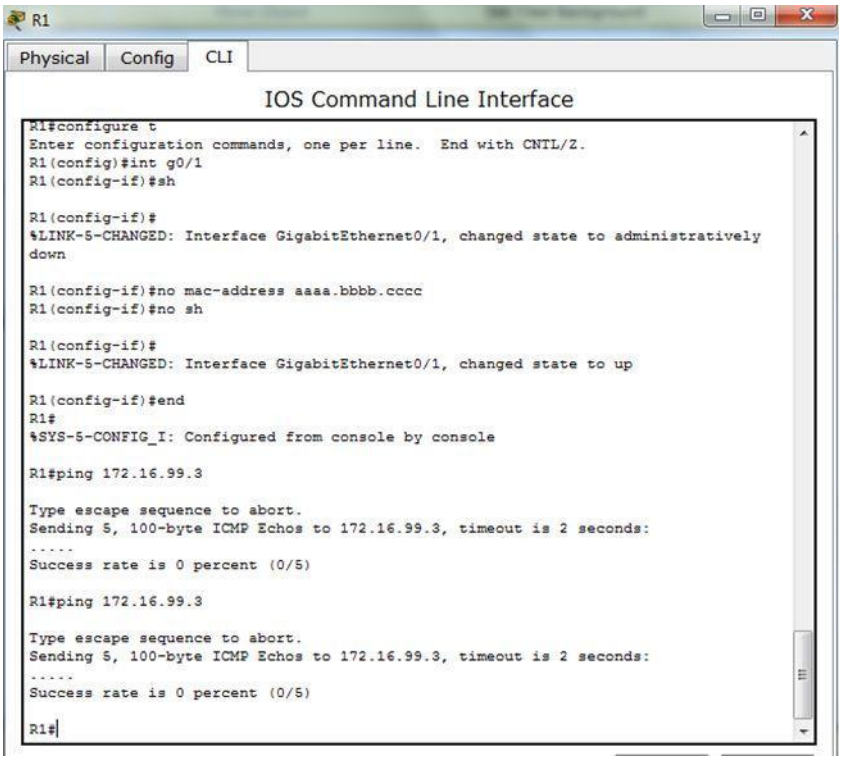
```
S1#show interface f 0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 000b.bec5.8c05 (bia 000b.bec5.8c05)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

S1# **show port-security address**

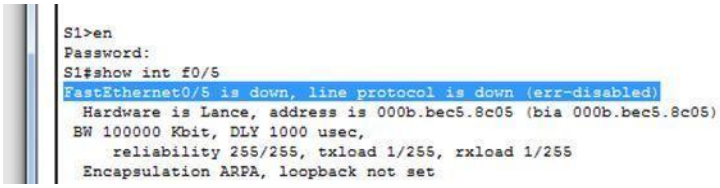


t. En el router, desactive la interfaz G0/1, elimine la dirección MAC codificada de forma rígida del router y vuelva a habilitar la interfaz G0/1.

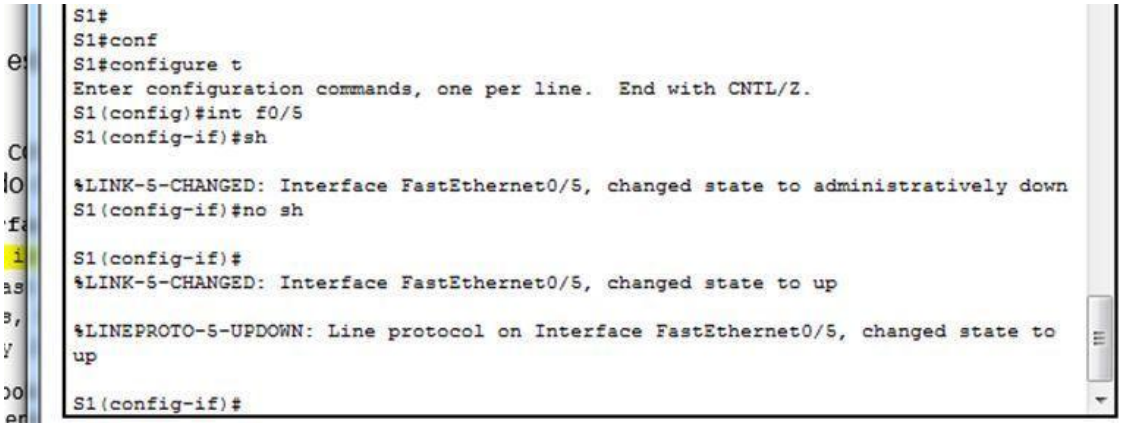
u. Desde el R1, vuelva a hacer ping a la PC-A en 172.16.99.3. ¿El ping se realizó correctamente? **NO**



v. Emita el comando **show interface f0/5** para determinar la causa de la falla del ping. Registre sus conclusiones. **NO se realizo por que el fastethernet y la línea de protocolo están caídas y están deshabilitadas por error.**



w. Borre el estado de inhabilitación por errores de F0/5 en el S1.



x. Emita el comando **show interface f0/5** en el S1 para verificar que F0/5 ya no esté en estado de inhabilitación por errores.

S1# **show interface f0/5**

```
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show int f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Lance, address is 000b.bec5.8c05 (bia 000b.bec5.8c05)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

y. En el símbolo del sistema del R1, vuelva a hacer ping a la PC-A. Debería realizarse correctamente.

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

R1#
```

Reflexión

1. ¿Por qué habilitaría la seguridad de puertos en un switch?

   Para que usuarios no autorizados no puedan ingresar a nuestra red

2. ¿Por qué deben deshabilitarse los puertos no utilizados en un switch?

   Para que no puedan ser conectadas sin autorización otras computadoras u otros dispositivos y mejorar con esto la seguridad.

2.1.1.6 Lab - Configuring Basic Switch Settings

Tabla de direccionamiento

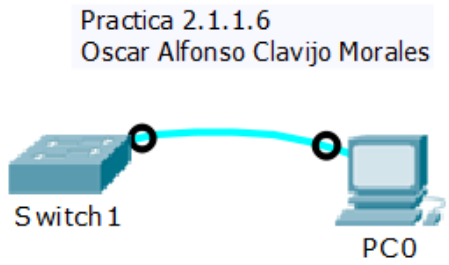
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Parte 19. tender el cableado de red y verificar la configuración predeterminada del switch

En la parte 1, establecerá la topología de la red y verificará la configuración predeterminada del switch.

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

a. Realice el cableado de la conexión de consola tal como se muestra en la topología. En esta instancia, no conecte el cable Ethernet de la PC-A.



b. Con Tera Term u otro programa de emulación de terminal, cree una conexión de consola de la PC-A al switch.

¿Por qué debe usar una conexión de consola para configurar inicialmente el switch? ¿Por qué no es posible conectarse al switch a través de Telnet o SSH?

El switch aún no tiene direcciones IP, asi que no podre accer remotamente con direcciones IP que son Telnet o SSH en cambio con consola si se puede.

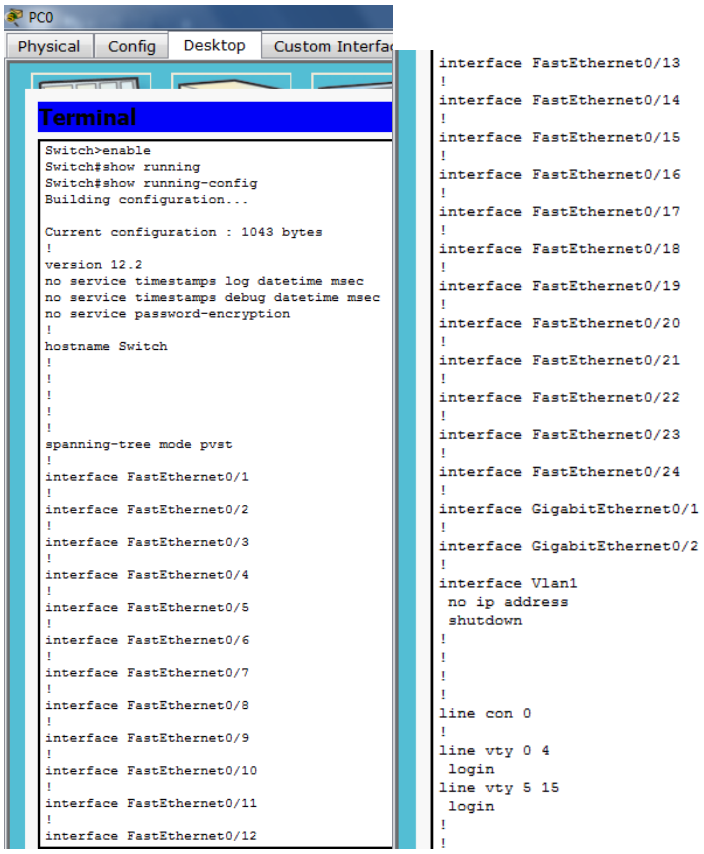
Step 2: Verificar la configuración predeterminada del switch.

a. Use el comando **enable** para ingresar al modo EXEC privilegiado.

```
Switch> enable
Switch#
```

b. Examine el archivo de configuración activa actual.

```
Switch# show running-config
```



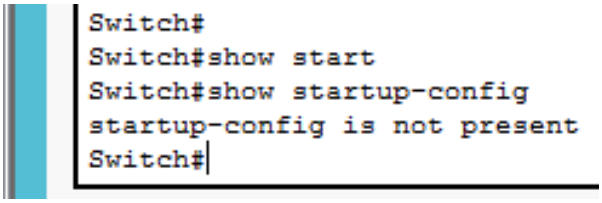
¿Cuántas interfaces FastEthernet tiene un switch 2960? **24**

¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960? **2**

¿Cuál es el rango de valores que se muestra para las líneas vty? **De 0 – 4 y de 5 – 15**

c. Examine el archivo de configuración de inicio en la NVRAM.

```
Switch# show startup-config
startup-config is not present
```



¿Por qué aparece este mensaje? **Esto indica que no hay nada guardado en la memoria no Volatil o NVram**

d. Examine las características de la SVI para la VLAN 1.

```
Switch# show interface vlan1
```

```
Switch#show interf
Switch#show interface vlan 1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0090.2b68.3b03 (bia 0090.2b68.3b03)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, 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
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
Switch#
Switch#
```

¿Hay alguna dirección IP asignada a la VLAN 1? **No hay direcciones IP**

¿Cuál es la dirección MAC de esta SVI? Las respuestas varían. **0090.2b68.3b03**

¿Está activa esta interfaz? **No esta Activada**

e. Examine las propiedades IP de la VLAN 1 SVI.

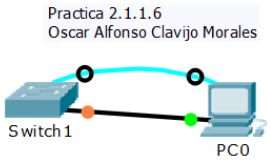
```
Switch# show ip interface vlan1
```

```
Switch#
Switch#show ip interface vlan 1
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
Switch#
```

¿Qué resultado ve? **No esta encendida y no tiene configurada ninguna dirección IP**

f. Conecte el cable Ethernet de la PC-A al puerto 6 en el switch

```
Switch# show ip interface vlan1
```




```
Switch#show ip interface vlan 1
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
Switch#
```

¿Qué resultado ve? **No hay dirección IP configurada**

g. Examine la información de la versión del IOS de Cisco del switch.

```
Switch# show versión
```

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0090.2B68.3B03
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C2960-24TT      12.2                  C2960-LANBASE-M

Configuration register is 0xF

Switch#
```

¿Cuál es la versión del IOS de Cisco que está ejecutando el switch? **Version 12.2**

¿Cuál es el nombre del archivo de imagen del sistema? **C2960-LANBASE-M**

¿Cuál es la dirección MAC base de este switch? **0090.2B68.3B03**

h. Examine las propiedades predeterminadas de la interfaz FastEthernet que usa la PC-A.

```
Switch# show interface f0/6
```

```
Switch#
Switch#show interface f 0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.0c26.be06 (bia 0090.0c26.be06)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (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
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

¿La interfaz está activa o desactivada? **Esta activada**

¿Qué haría que una interfaz se active?

¿Cuál es la dirección MAC de la interfaz? **0090.0c26.be06**

¿Cuál es la configuración de velocidad y de dúplex de la interfaz? **BW 100000 Kbit y Full-duplex, 100Mb/**s

i. Examine la configuración VLAN predeterminada del switch.

Switch# **show vlan**

```
Switch#
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
```

¿Cuál es el nombre predeterminado de la VLAN 1? **1 por Default**

¿Qué puertos hay en esta VLAN? **24 Fa y 2 Gig**

¿La VLAN 1 está activa? **SI**

¿Qué tipo de VLAN es la VLAN predeterminada? **Tipo Enet Ethernet**

j. Examine la memoria flash.

Ejecute uno de los siguientes comandos para examinar el contenido del directorio flash.

```
Switch# show flash
Switch# dir flash:
```

```
Switch#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
Switch#dir flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
Switch#
```

¿Cuál es el nombre de archivo de la imagen de IOS de Cisco? **c2960-lanbase-mz.122-25.FX.bin**

Parte 20. configurar los parámetros básicos de los dispositivos de red

Step 1: configurar los parámetros básicos del switch, incluidos el nombre de host, las contraseñas locales, el mensaje MOTD, la dirección de administración y el acceso por Telnet.

a. Ingrese al modo de configuración global.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

b. Asigne el nombre de host del switch.

```
Switch(config)# hostname S1
S1(config)#
```

c. Configurar la encriptación de contraseñas.

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

d. Asigne **class** como contraseña secreta para el acceso al modo EXEC privilegiado.

```
S1(config)# enable secret class
S1(config)#
```

e. Evite las búsquedas de DNS no deseadas.

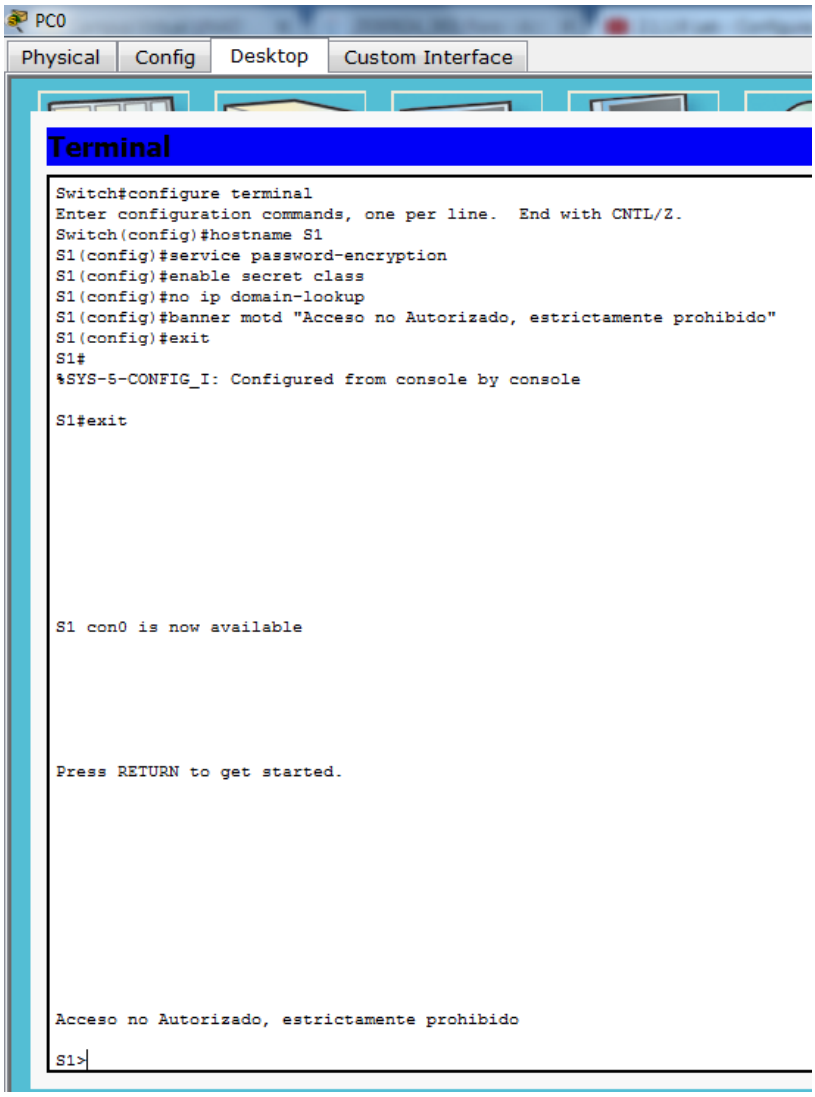
```
S1(config)# no ip domain-lookup
S1(config)#
```

f. Configure un mensaje MOTD.

```
S1(config)# banner motd #
Enter Text message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
```

g. Para verificar la configuración de acceso, alterne entre los modos.

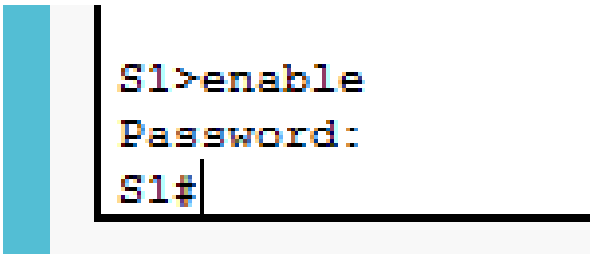
```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available

Press RETURN to get started.
Unauthorized access is strictly prohibited.
S1>
```



¿Qué teclas de método abreviado se usan para ir directamente del modo de configuración global al modo EXEC privilegiado? **enable**

h. Vuelva al modo EXEC privilegiado desde el modo EXEC del usuario. Introduzca la contraseña **class** cuando se le solicite hacerlo.

```
S1> enable
Password:
S1#
```



i. Primero, cree la nueva VLAN 99 en el switch. Luego, establezca la dirección IP del switch en 192.168.1.2 con la máscara de subred 255.255.255.0 en la interfaz virtual interna VLAN 99.

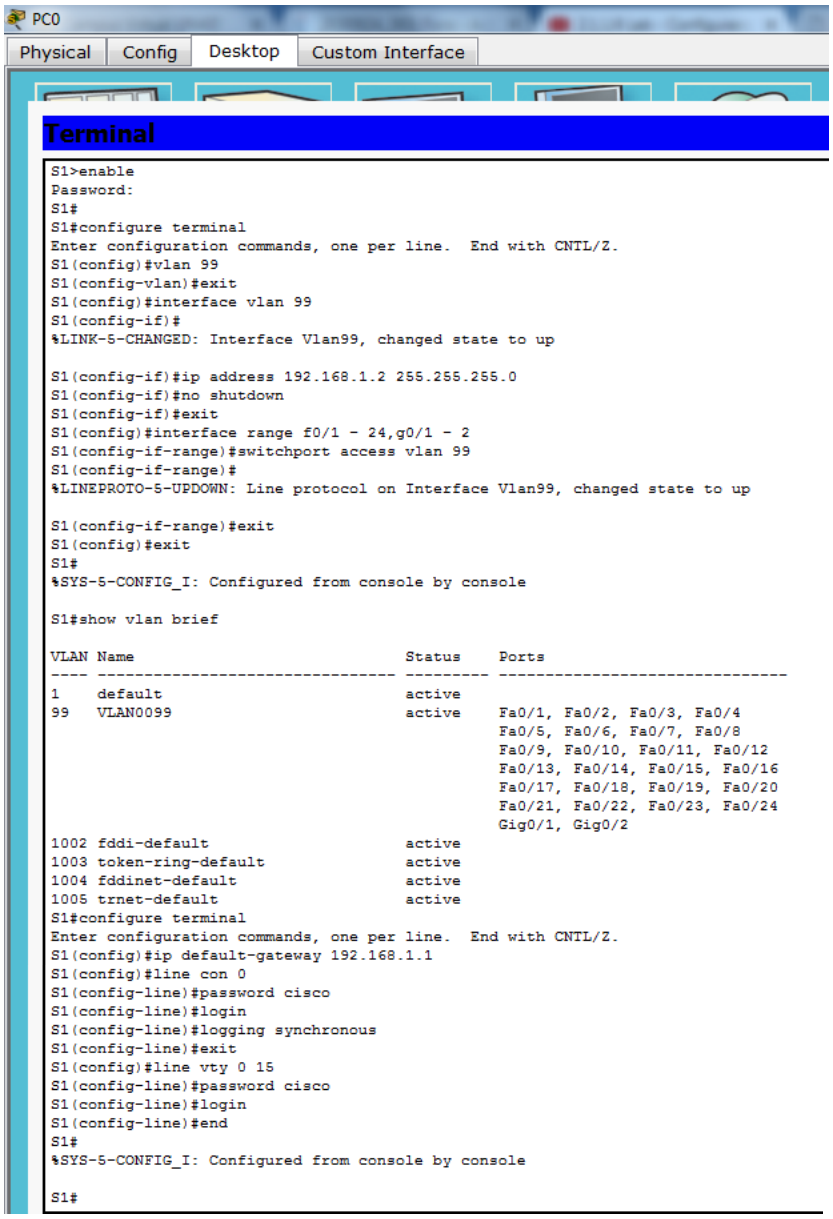
j. Asigne todos los puertos de usuario a VLAN 99.

k. Emita el comando **show vlan brief** para verificar que todos los puertos de usuario estén en la VLAN 99.

l. Configure el gateway IP predeterminado para el S1. Si no se estableció ningún gateway predeterminado, no se puede administrar el switch desde una red remota que esté a más de un router de distancia. Sí responde a los pings de una red remota. Aunque esta actividad no incluye un gateway IP externo, se debe tener en cuenta que finalmente conectará la LAN a un router para tener acceso externo. Suponiendo que la interfaz LAN en el router es 192.168.1.1, establezca el gateway predeterminado para el switch.

m. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción **logging synchronous**.

n. Configure las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no puede acceder al switch mediante telnet.

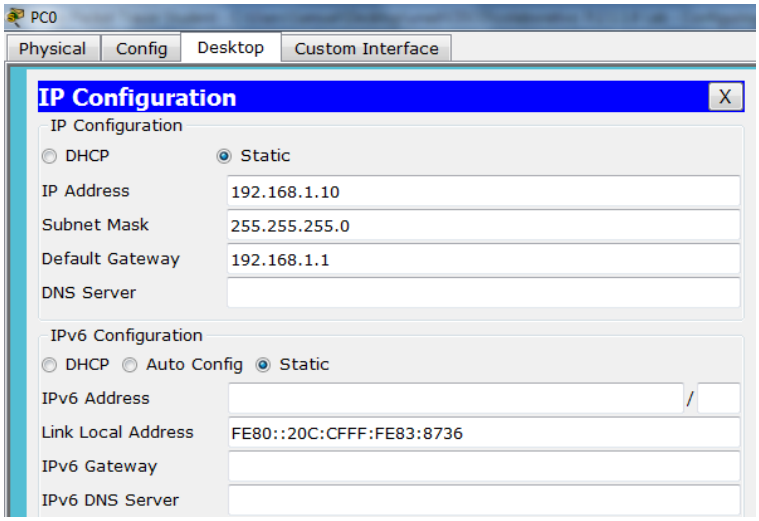


¿Por qué se requiere el comando **login**? **Para que cuando se quiera acceder se solicite un password, de lo contrario no lo haría.**

Step 2: configurar una dirección IP en la PC-A.

Asigne a la computadora la dirección IP y la máscara de subred que se muestran en la tabla de direccionamiento. Aquí se describe una versión abreviada del procedimiento. Para esta topología, no se requiere ningún gateway predeterminado; sin embargo, puede introducir **192.168.1.1** para simular un router conectado al S1.

1) Haga clic en el ícono **Inicio** de Windows > **Panel de control**.
2) Haga clic en **Ver por:** y elija **Íconos pequeños**.
3) Selecciones **Centro de redes y recursos compartidos** > **Cambiar configuración del adaptador**.
4) Seleccione **Conexión de área local**, haga clic con el botón secundario y elija **Propiedades**.
5) Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** > **Propiedades**.
6) Haga clic en el botón de opción **Usar la siguiente dirección IP** e introduzca la dirección IP y la máscara de subred.



Parte 21. verificar y probar la conectividad de red

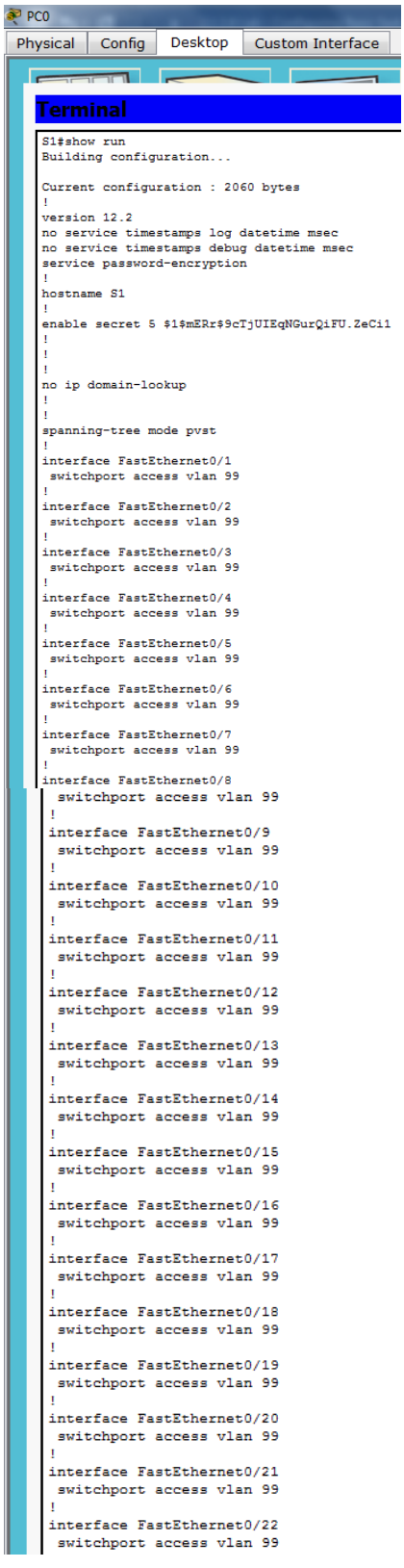
En la parte 3, verificará y registrará la configuración del switch, probará la conectividad de extremo a extremo entre la PC-A y el S1, y probará la capacidad de administración remota del switch.

Step 1: mostrar la configuración del switch.

Desde la conexión de consola en la PC-A, muestre y verifique la configuración del switch. El comando **show run** muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

a. Aquí se muestra un ejemplo de configuración. Los parámetros que configuró están resaltados en amarillo. Las demás son opciones de configuración predeterminadas del IOS.

```
S1# show run
```




```
S1#show run
Building configuration...

Current configuration : 2060 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 99
!
interface FastEthernet0/2
 switchport access vlan 99
!
interface FastEthernet0/3
 switchport access vlan 99
!
interface FastEthernet0/4
 switchport access vlan 99
!
interface FastEthernet0/5
 switchport access vlan 99
!
interface FastEthernet0/6
 switchport access vlan 99
!
interface FastEthernet0/7
 switchport access vlan 99
!
interface FastEthernet0/8
 switchport access vlan 99
!
interface FastEthernet0/9
 switchport access vlan 99
!
interface FastEthernet0/10
 switchport access vlan 99
!
interface FastEthernet0/11
 switchport access vlan 99
!
interface FastEthernet0/12
 switchport access vlan 99
!
interface FastEthernet0/13
 switchport access vlan 99
!
interface FastEthernet0/14
 switchport access vlan 99
!
interface FastEthernet0/15
 switchport access vlan 99
!
interface FastEthernet0/16
 switchport access vlan 99
!
interface FastEthernet0/17
 switchport access vlan 99
!
interface FastEthernet0/18
 switchport access vlan 99
!
interface FastEthernet0/19
 switchport access vlan 99
!
interface FastEthernet0/20
 switchport access vlan 99
!
interface FastEthernet0/21
 switchport access vlan 99
!
interface FastEthernet0/22
 switchport access vlan 99
!
interface FastEthernet0/23
 switchport access vlan 99
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
 switchport access vlan 99
!
interface GigabitEthernet0/2
 switchport access vlan 99
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
!
banner motd ^CAcceso no Autorizado, estrictamente prohibido^C
!
!
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
!
end


S1#
```

b. Verifique la configuración de la VLAN 99 de administración.

S1# **show interface vlan 99**

```
S1#
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0090.2b68.3b03 (bia 0090.2b68.3b03)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, 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
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
S1#
```

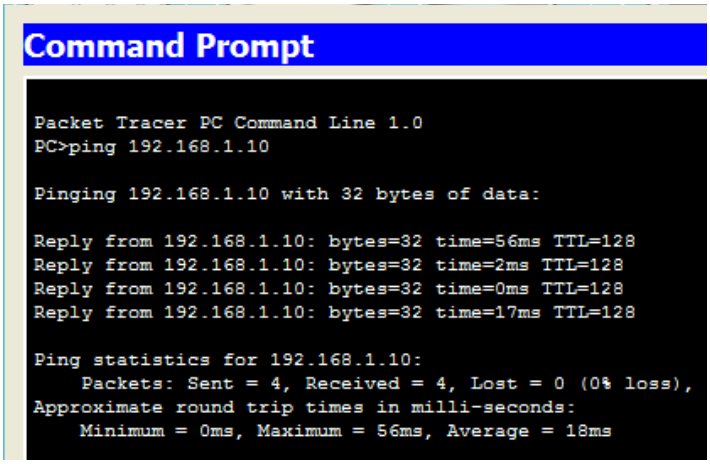
¿Cuál es el ancho de banda en esta interfaz? **BW 100000 Kbit**

¿Cuál es el estado de la VLAN 99? **Vlan99 is up**

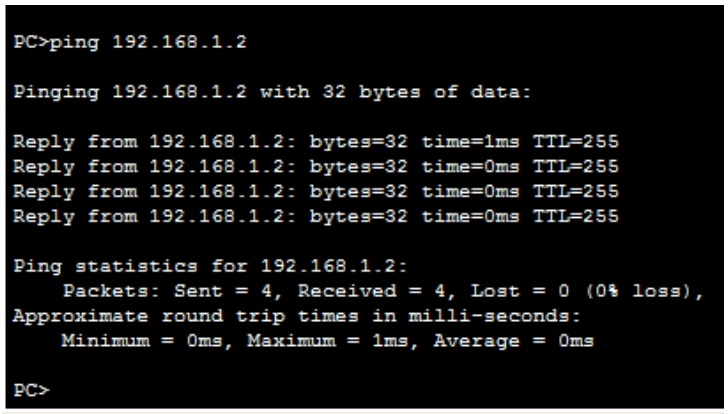
¿Cuál es el estado del protocolo de línea? **line protocol is up**

Step 2: probar la conectividad de extremo a extremo con ping.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de la propia PC-A primero.



b. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración de SVI del S1.



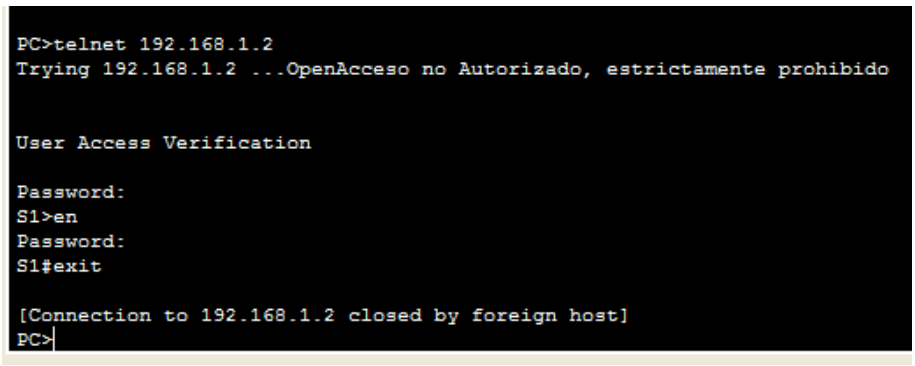
Step 3: probar y verificar la administración remota del S1.

Ahora utilizará Telnet para acceder al switch en forma remota. En esta práctica de laboratorio, la PC-A y el S1 se encuentran uno junto al otro. En una red de producción, el switch podría estar en un armario de cableado en el piso superior, mientras que la computadora de administración podría estar ubicada en la planta baja. En este paso, utilizará Telnet para acceder al switch S1 en forma remota mediante la dirección de administración de SVI. Telnet no es un protocolo seguro; sin embargo, lo usará para probar el acceso remoto. Con Telnet, toda la información, incluidos los comandos y las contraseñas, se envía durante la sesión como texto no cifrado. En las prácticas de laboratorio posteriores, usará SSH para acceder a los dispositivos de red en forma remota.

a. Con la ventana cmd abierta en la PC-A, emita un comando de Telnet para conectarse al S1 a través de la dirección de administración de SVI. La contraseña es **cisco**.

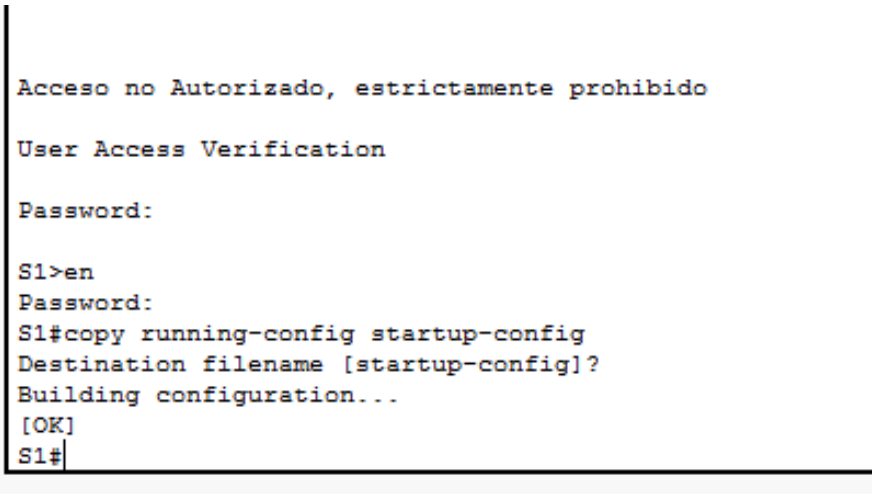
b. Después de introducir la contraseña **cisco**, quedará en la petición de entrada del modo EXEC del usuario. Acceda al modo EXEC privilegiado.

c. Escriba **exit** para finalizar la sesión de Telnet.



Step 4: guardar el archivo de configuración en ejecución del switch.

```
S1# copy running-config startup-config
```



Parte 22. Administrar la tabla de direcciones MAC

En la parte 4, determinará la dirección MAC que detectó el switch, configurará una dirección MAC estática en una interfaz del switch y, a continuación, eliminará la dirección MAC estática de esa interfaz.

Step 1: registrar la dirección MAC del host.

En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** para determinar y registrar las direcciones (físicas) de capa 2 de la NIC de la computadora.

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 000C.CF83.8736
   Link-local IPv6 Address.........: FE80::20C:CFFF:FE83:8736
   IP Address.......................: 192.168.1.10
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.1.1
   DNS Servers......................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID...............: 00-01-00-01-6A-43-37-BB-00-0C-CF-83-87-36


PC>
```

Step 2: Determine las direcciones MAC que el switch ha aprendido.

Muestre las direcciones MAC con el comando **show mac address-table**.

```
S1# show mac address-table
```

```
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    000c.cf83.8736    DYNAMIC     Fa0/6
S1#
```

¿Cuántas direcciones dinámicas hay? **1**

¿Cuántas direcciones MAC hay en total? **1**

¿La dirección MAC dinámica coincide con la dirección MAC de la PC-A? **SI**

Step 3: enumerar las opciones del comando show mac address-table.

a. Muestre las opciones de la tabla de direcciones MAC.

```
S1# show mac address-table ?
```

```
S1#show mac-address-table ?
  dynamic     dynamic entry type
  interfaces  interface entry type
  static      static entry type
  <cr>
S1#show mac-address-table
```

¿Cuántas opciones se encuentran disponibles para el comando **show mac address-table**? **3 opciones**

b. Emita el comando **show mac address-table dynamic** para mostrar solo las direcciones MAC que se detectaron dinámicamente.

```
S1# show mac address-table dynamic
```

¿Cuántas direcciones dinámicas hay? **1**

c. Vea la entrada de la dirección MAC para la PC-A. El formato de dirección MAC para el comando es xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Step 4: Configure una dirección MAC estática.

a. limpie la tabla de direcciones MAC.

Para eliminar las direcciones MAC existentes, use el comando **clear mac address-table** del modo EXEC privilegiado.

```
S1# clear mac address-table dynamic
```

```
S1#CLEAR
S1#clear mac address-table dynamic
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

S1#
```

b. Verifique que la tabla de direcciones MAC se haya eliminado.

```
S1# show mac address-table
```

¿Cuántas direcciones MAC estáticas hay? **NINGUNA**

¿Cuántas direcciones dinámicas hay? **NINGUNA**

c. Examine nuevamente la tabla de direcciones MAC

Es muy probable que una aplicación en ejecución en la computadora ya haya enviado una trama por la NIC hacia el S1. Observe nuevamente la tabla de direcciones MAC en el modo EXEC privilegiado para ver si el S1 volvió a detectar la dirección MAC para la PC-A.

```
S1# show mac address-table
```

¿Cuántas direcciones dinámicas hay? No aparece la dirección

¿Por qué cambió esto desde la última visualización?

Si el S1 aún no volvió a detectar la dirección MAC de la PC-A, haga ping a la dirección IP de la VLAN 99 del switch desde la PC-A y, a continuación, repita el comando **show mac address-table**.

```
S1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    000c.cf83.8736    DYNAMIC     Fa0/6
S1#
```

d. Configure una dirección MAC estática.

Para especificar a qué puertos se puede conectar un host, una opción es crear una asignación estática de la dirección MAC del host a un puerto.

Configure una dirección MAC estática en F0/6 con la dirección que se registró para la PC-A en la parte 4, paso 1.

`S1(config)#` **`mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6`**

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#mac address-table static 000c.cf83.8736 vlan 99 interface fastethernet 0/6
S1(config)#exit
S1#
```

e. Verifique las entradas de la tabla de direcciones MAC.

`S1#` **`show mac address-table`**

```
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    000c.cf83.8736    STATIC      Fa0/6
S1#
```

¿Cuántas direcciones MAC hay en total? **1**

¿Cuántas direcciones estáticas hay? **1**

f. Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99
interface fastethernet 0/6
```

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no mac address-table static 000c.cf83.8736 vlan 99 interface fastethernet 0/6
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

g. Verifique que la dirección MAC estática se haya borrado.

```
S1# show mac address-table
```

```
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

S1#
```

¿Cuántas direcciones MAC estáticas hay en total? **NINGUNA**

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch?

   Por que si no se configura password en las VTY no se podrá hacer Telnet al switch

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?

   Para tener mejor seguridad

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado?

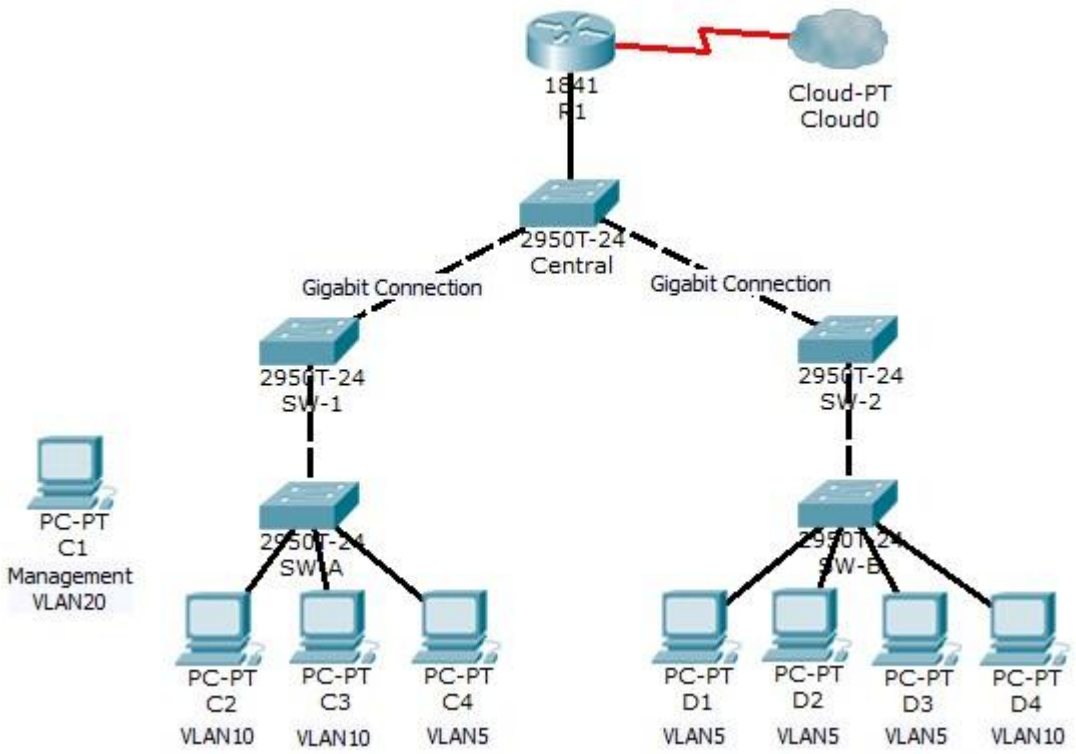
   Con el comando service password-encryption

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?

   Para especificar a que puertos se puede conectar una computadora

6.5.1.3 Packet Tracer - Layer 2 VLAN Security

Topology



Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Background / Scenario

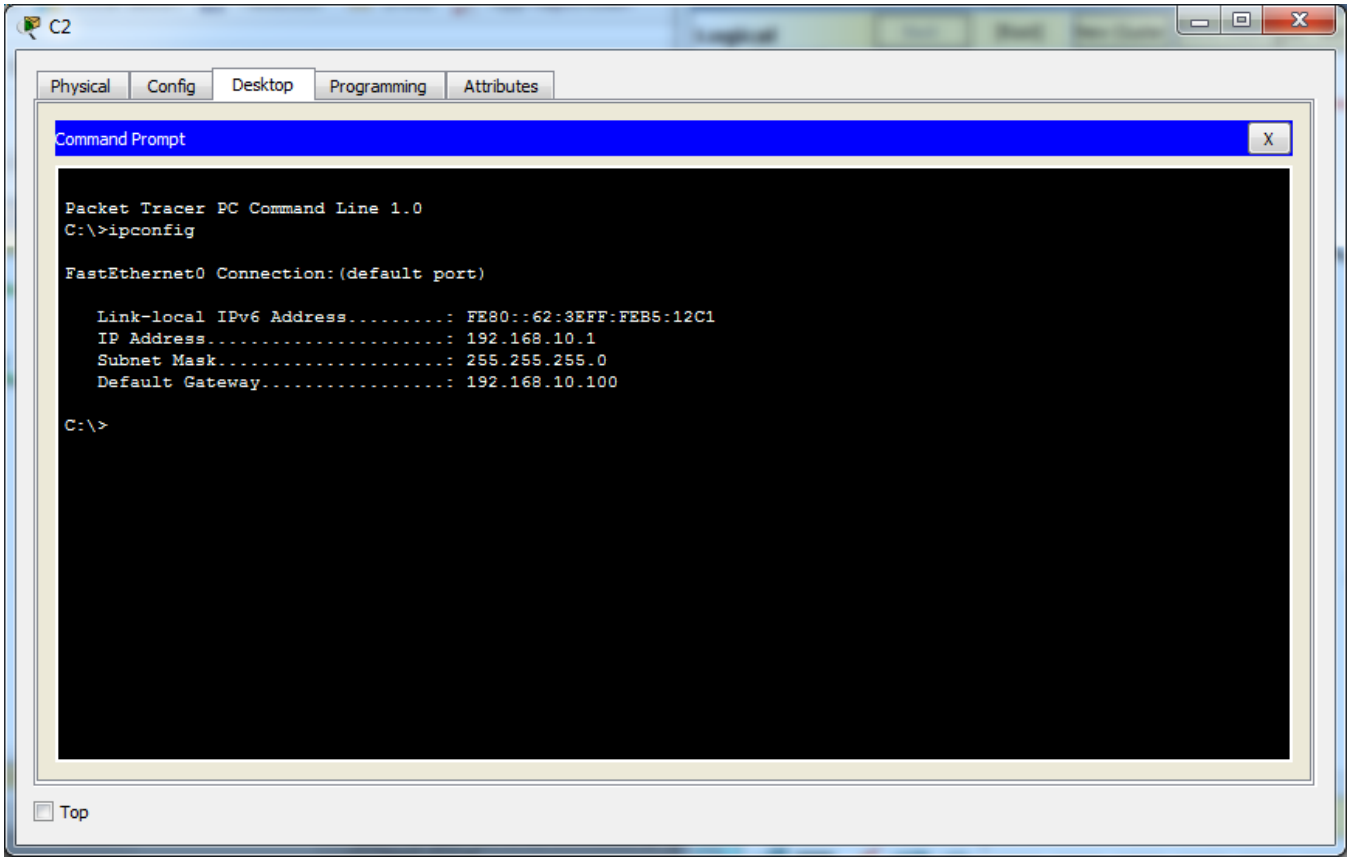
A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

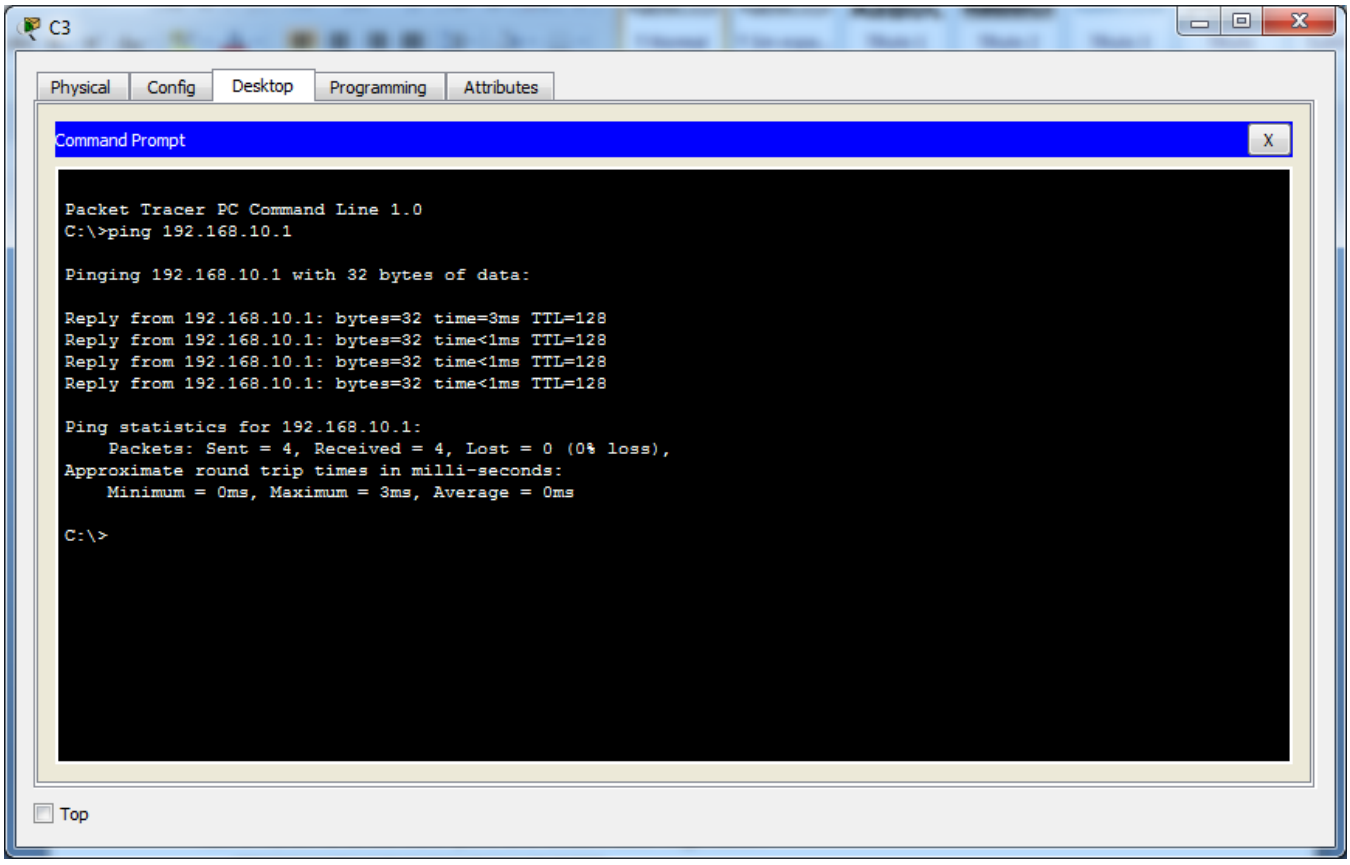
In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to allow the management PC to be able to connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

All devices have been preconfigured with: o Enable secret password: **ciscoenpa55**o Console password: **ciscoconpa55**

o VTY line password: ciscovtypa55Part 1: Verify Connectivity

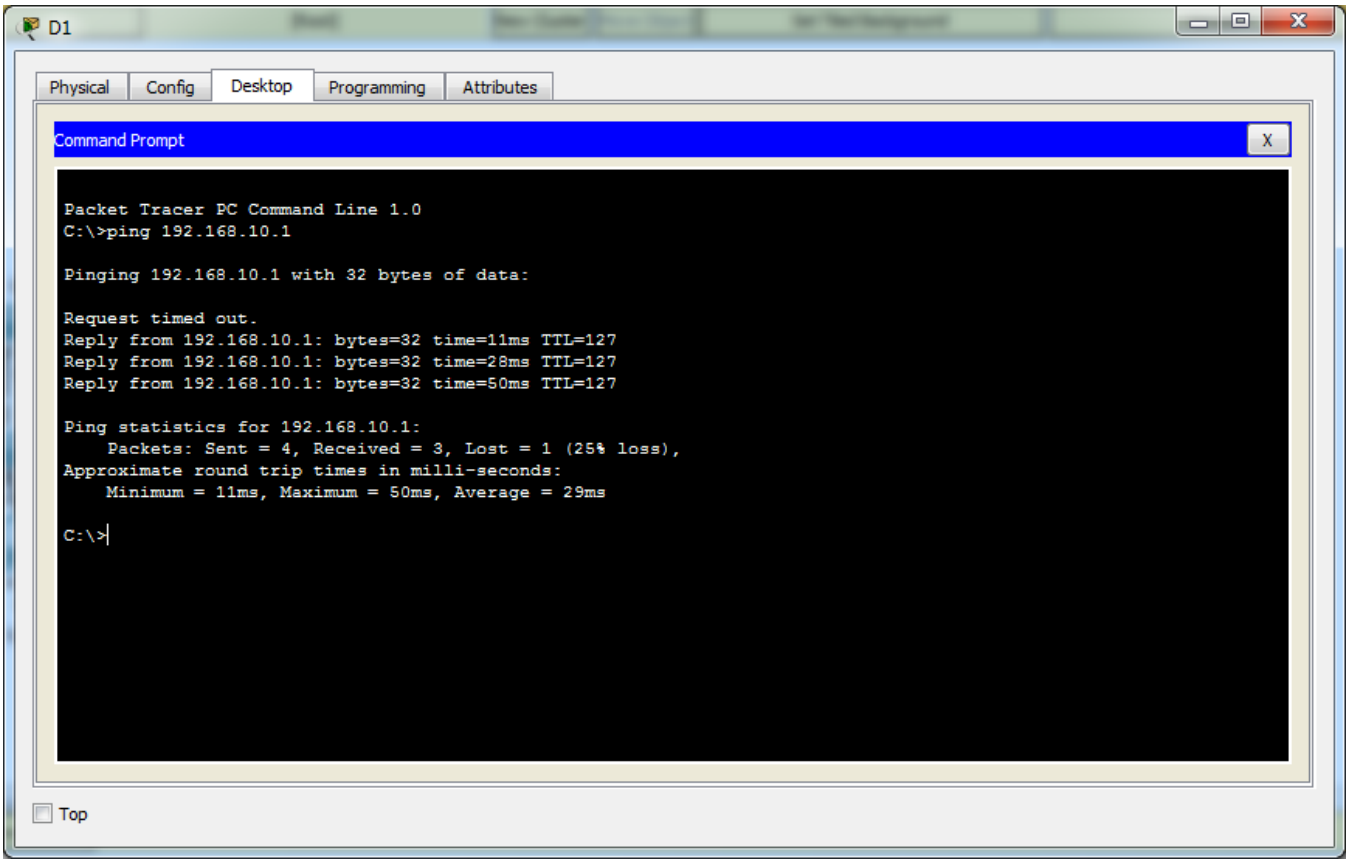
Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).





Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

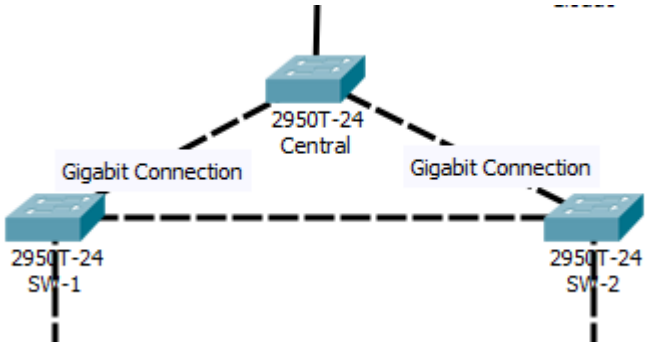
Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.



Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

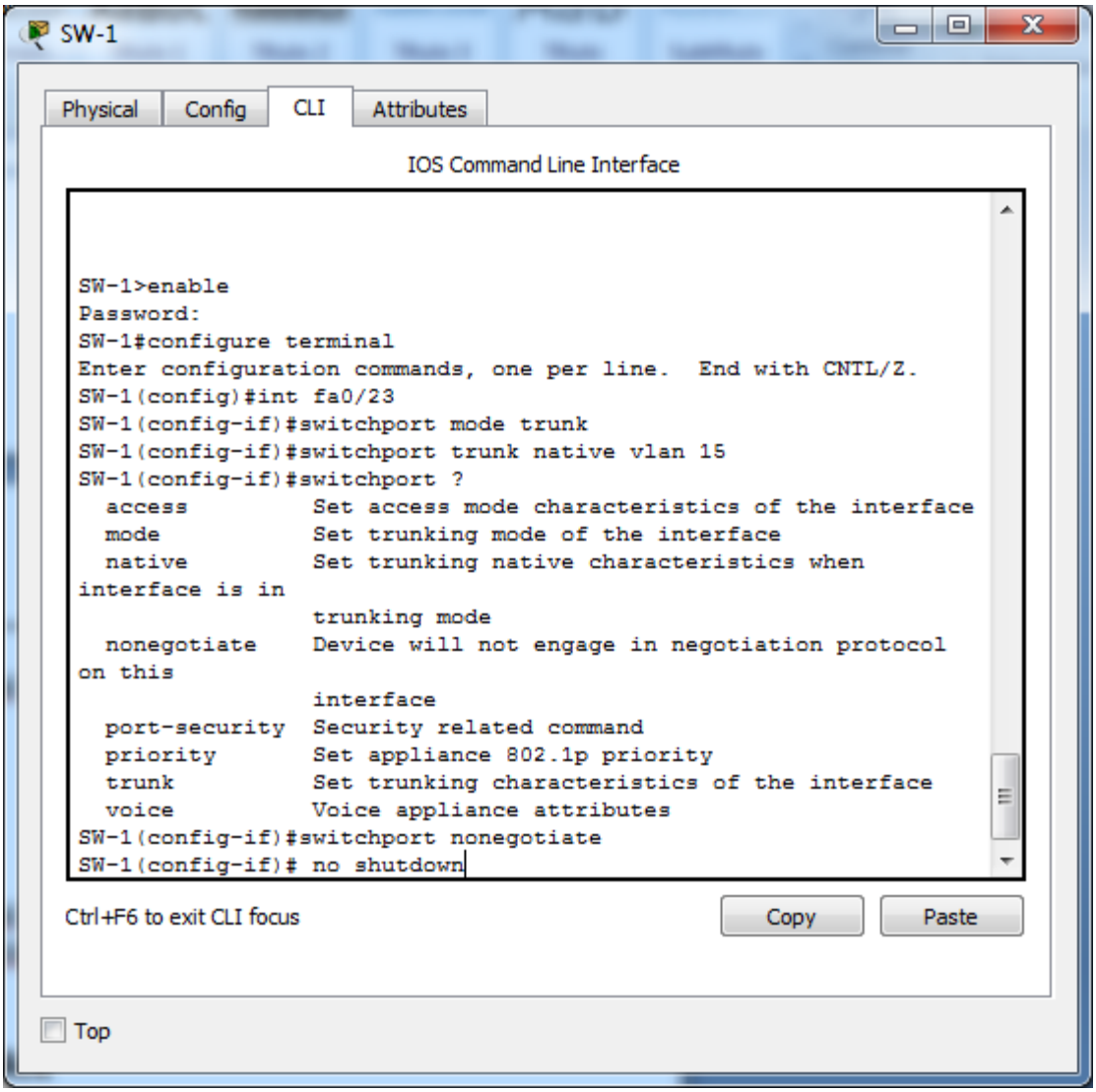
Using a crossover cable, connect port Fa0/23 on **SW-1** to port Fa0/23 on **SW-2**.

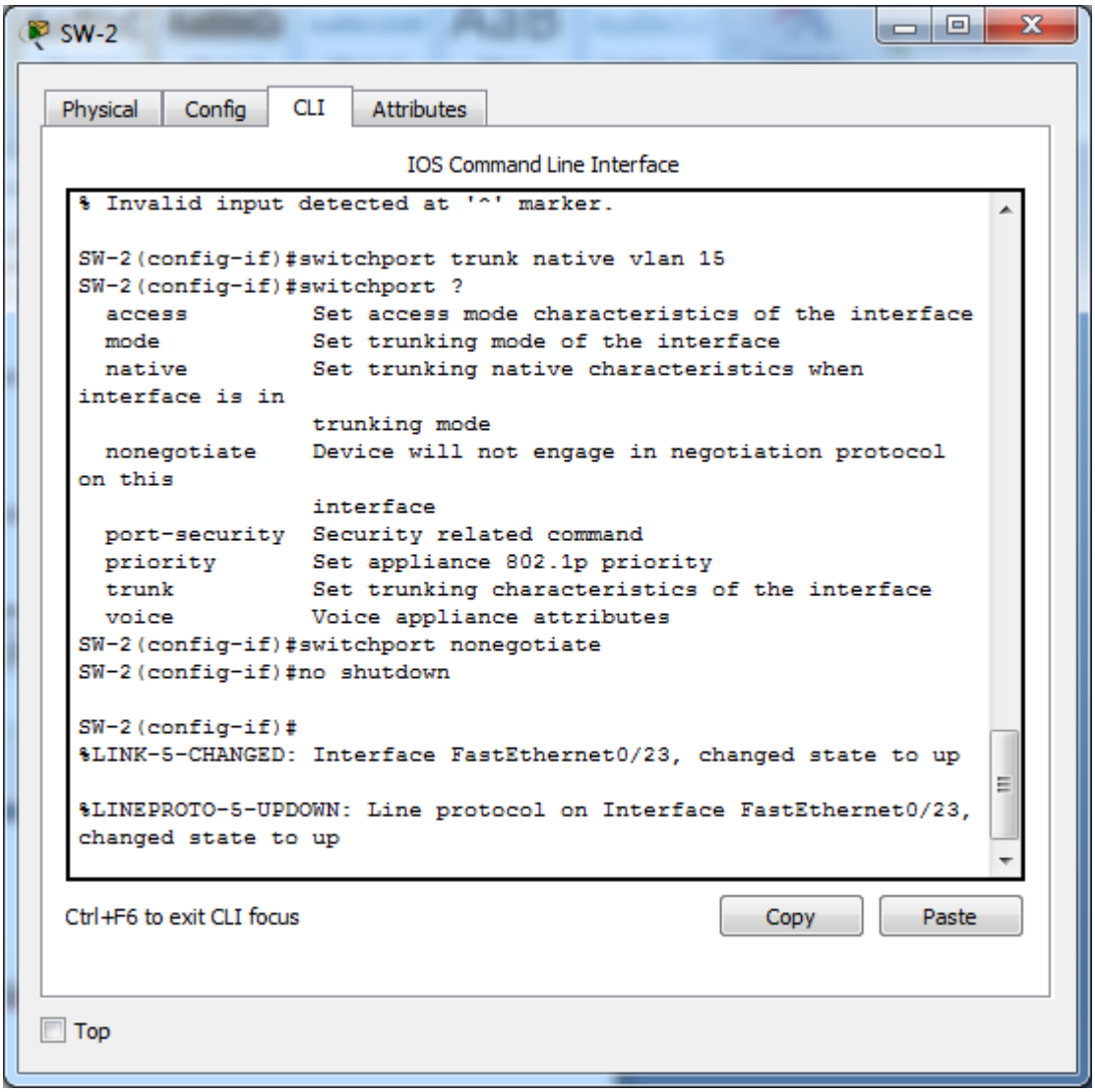


Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

SW-1(config)# interface fa0/23
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk native vlan 15
SW-1(config-if)# switchport nonegotiate
SW-1(config-if)# no shutdown





SW-2(config)# interface fa0/23

SW-2(config-if)# switchport mode trunk

SW-2(config-if)# switchport trunk native vlan 15

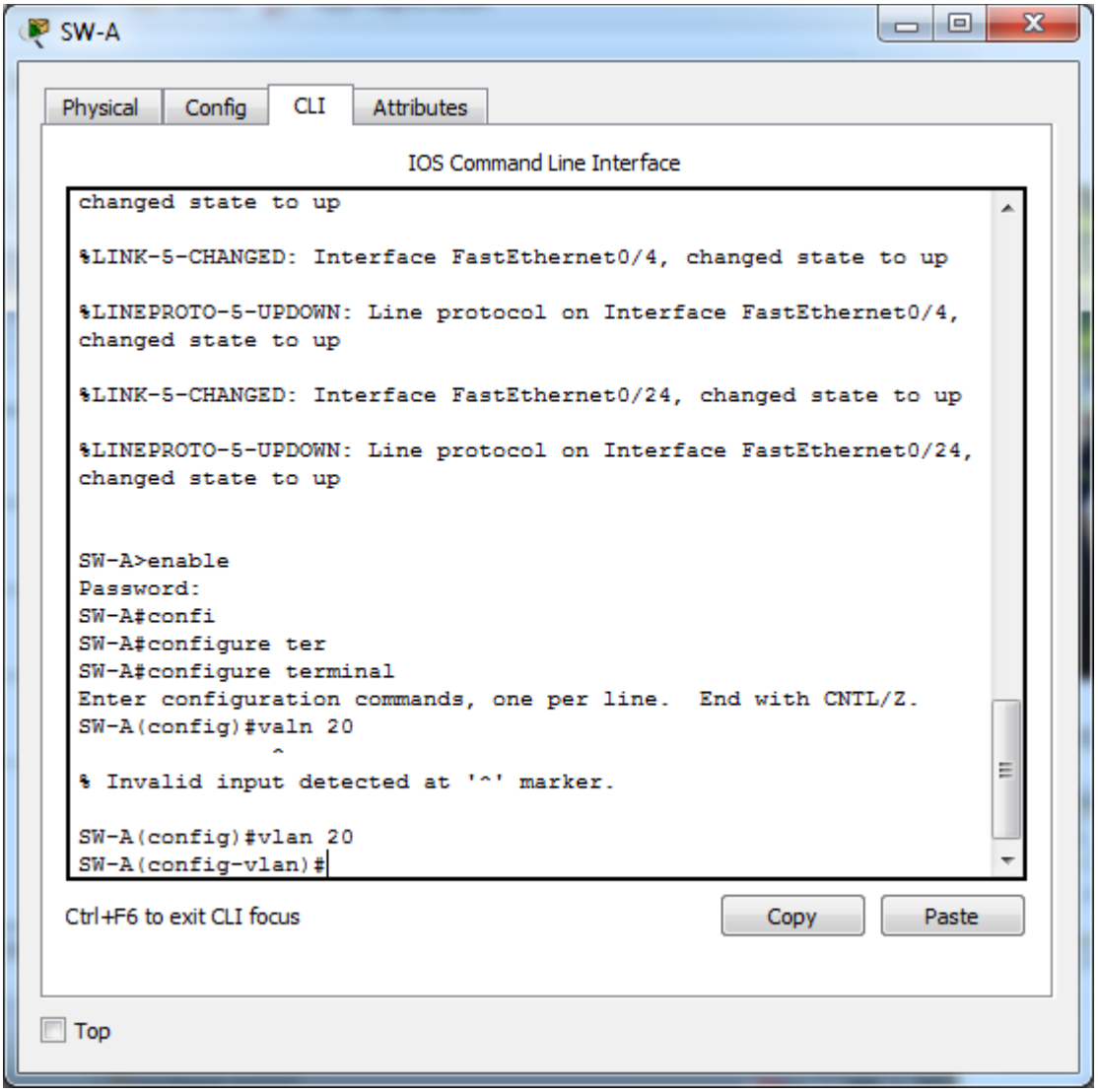
SW-2(config-if)# switchport nonegotiateSW-2(config-if)# no shutdown

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on **SW-A**.



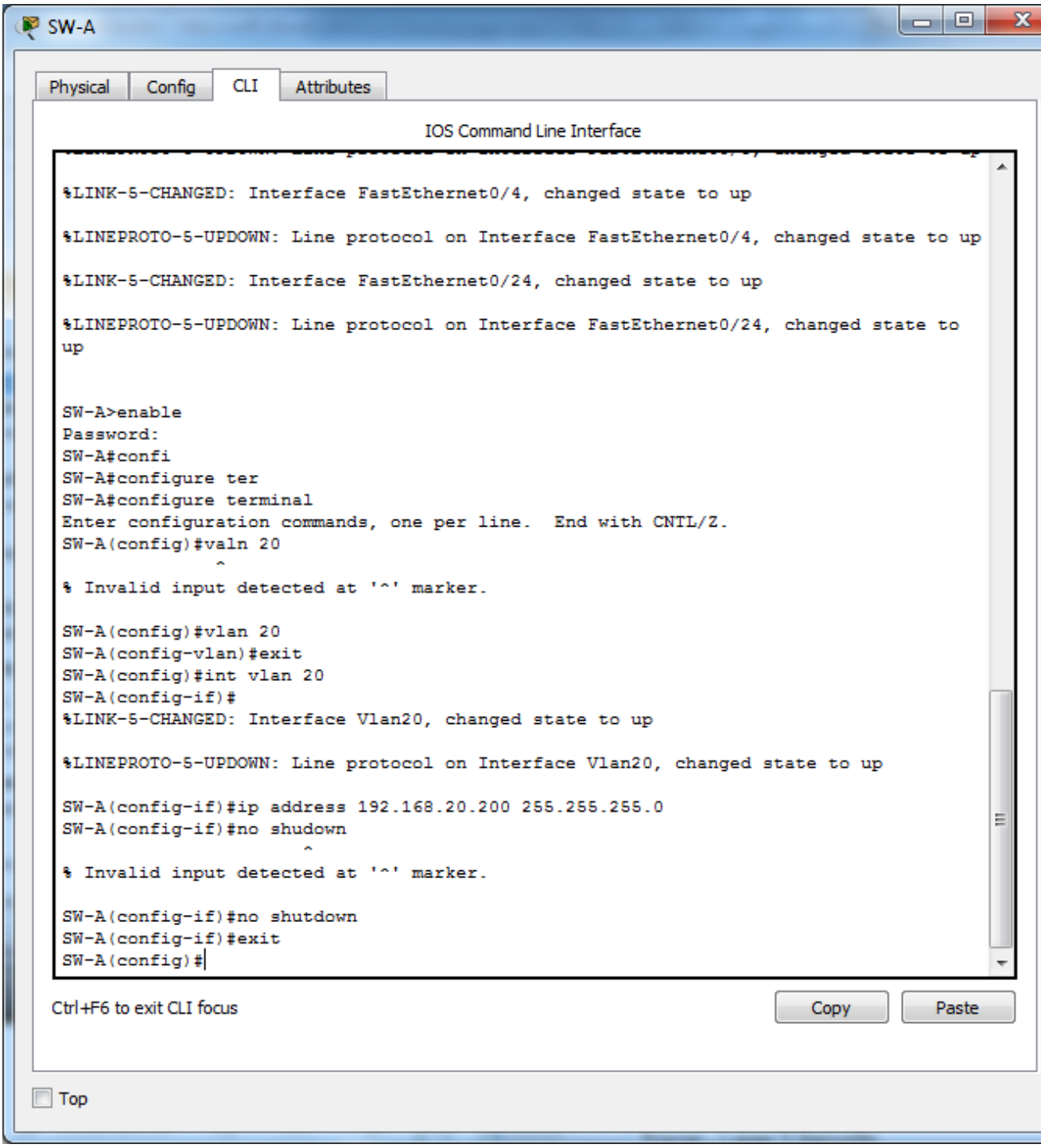
SW-A(config)# vlan 20

SW-A(config-vlan)# exit

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

SW-A(config)# interface vlan 20

SW-A(config-if)# ip address 192.168.20.1 255.255.255.0



Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.

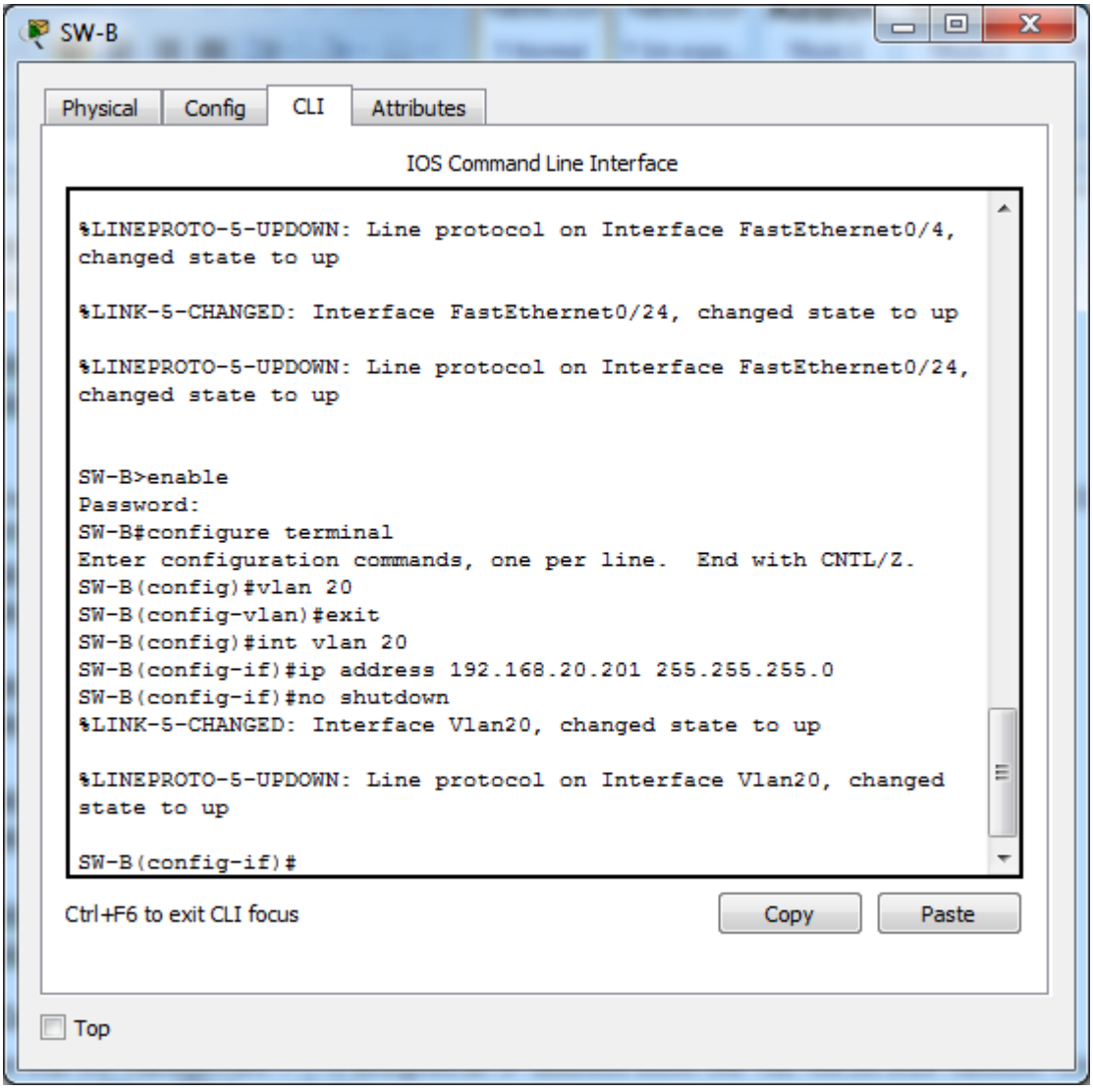
SW-B(config)# vlan 20

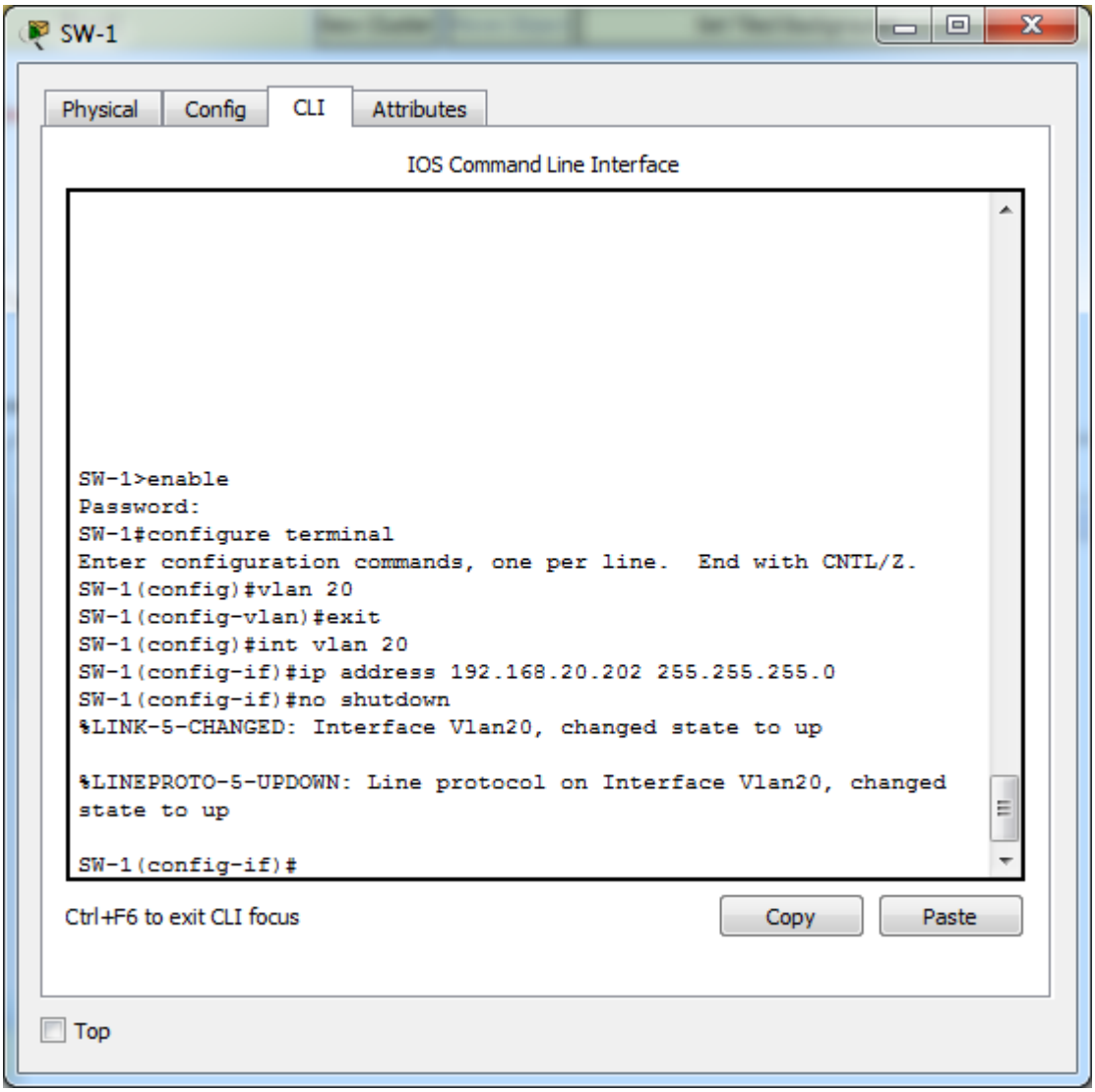
SW-B(config-vlan)# exit

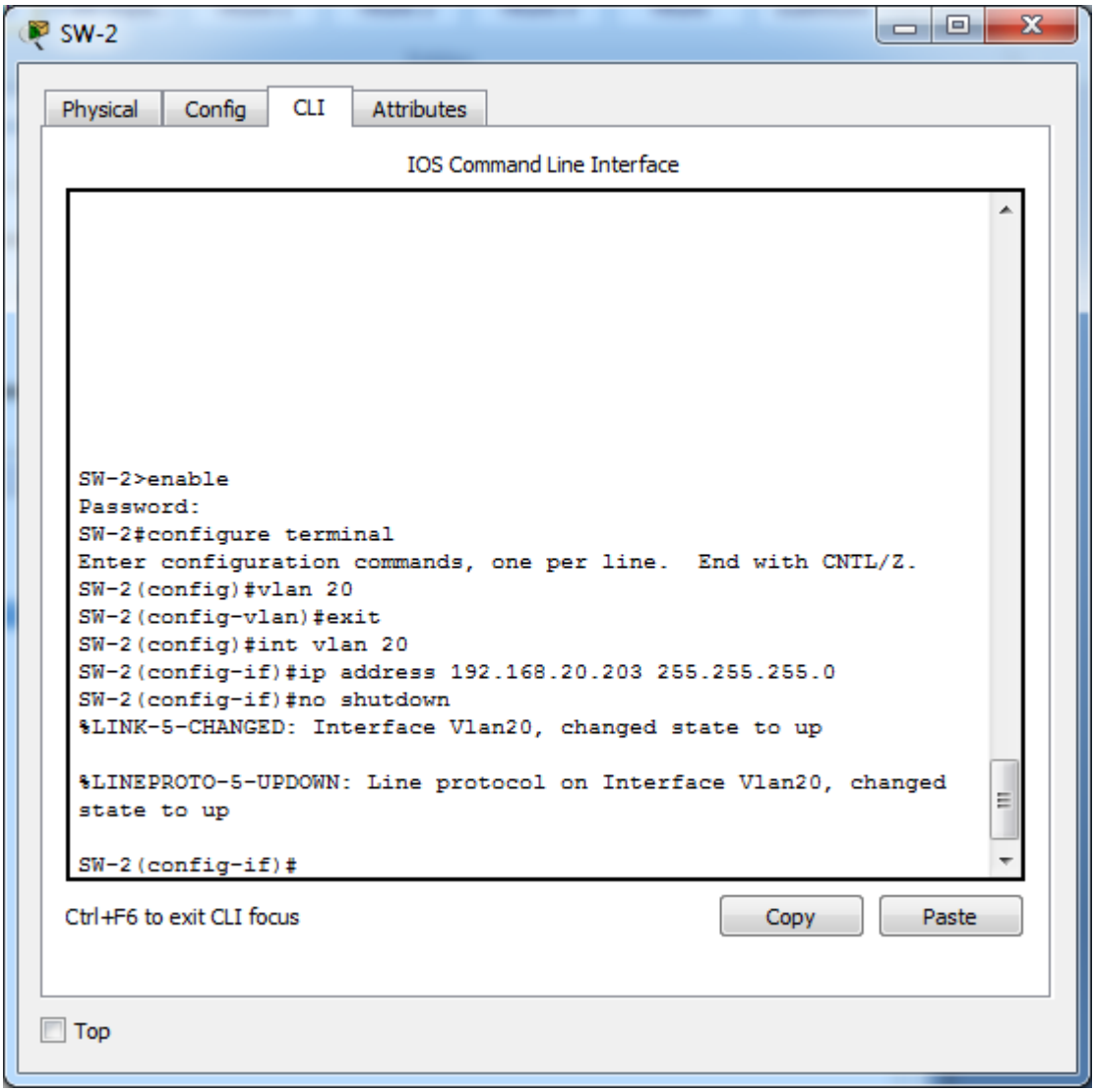
SW-1(config)# vlan 20
SW-1(config-vlan)# exit

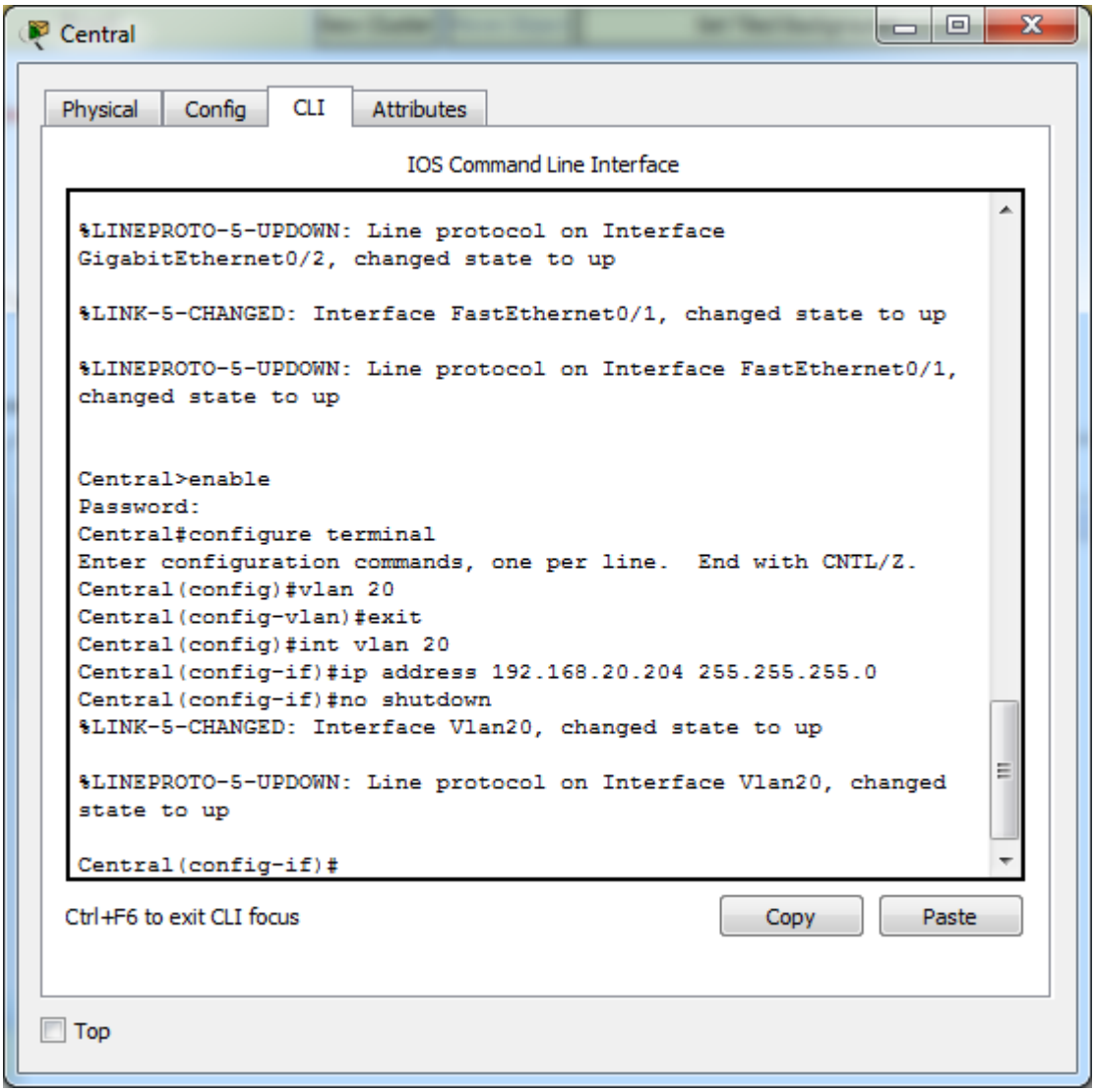
SW-2(config)# vlan 20
SW-2(config-vlan)# exit

Central(config)# vlan 20
Central(config-vlan)# exit




SW-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
SW-1>enable
Password:
SW-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#vlan 20
SW-1(config-vlan)#exit
SW-1(config)#int vlan 20
SW-1(config-if)#ip address 192.168.20.202 255.255.255.0
SW-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SW-1(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


SW-2
Physical
Config
CLI
Attributes
IOS Command Line Interface
SW-2>enable
Password:
SW-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-2(config)#vlan 20
SW-2(config-vlan)#exit
SW-2(config)#int vlan 20
SW-2(config-if)#ip address 192.168.20.203 255.255.255.0
SW-2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SW-2(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

SW-B(config)# interface vlan 20
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0

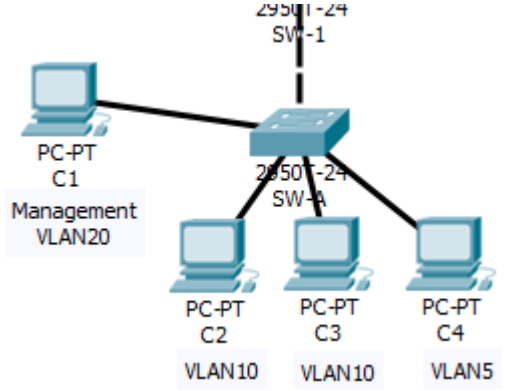
SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

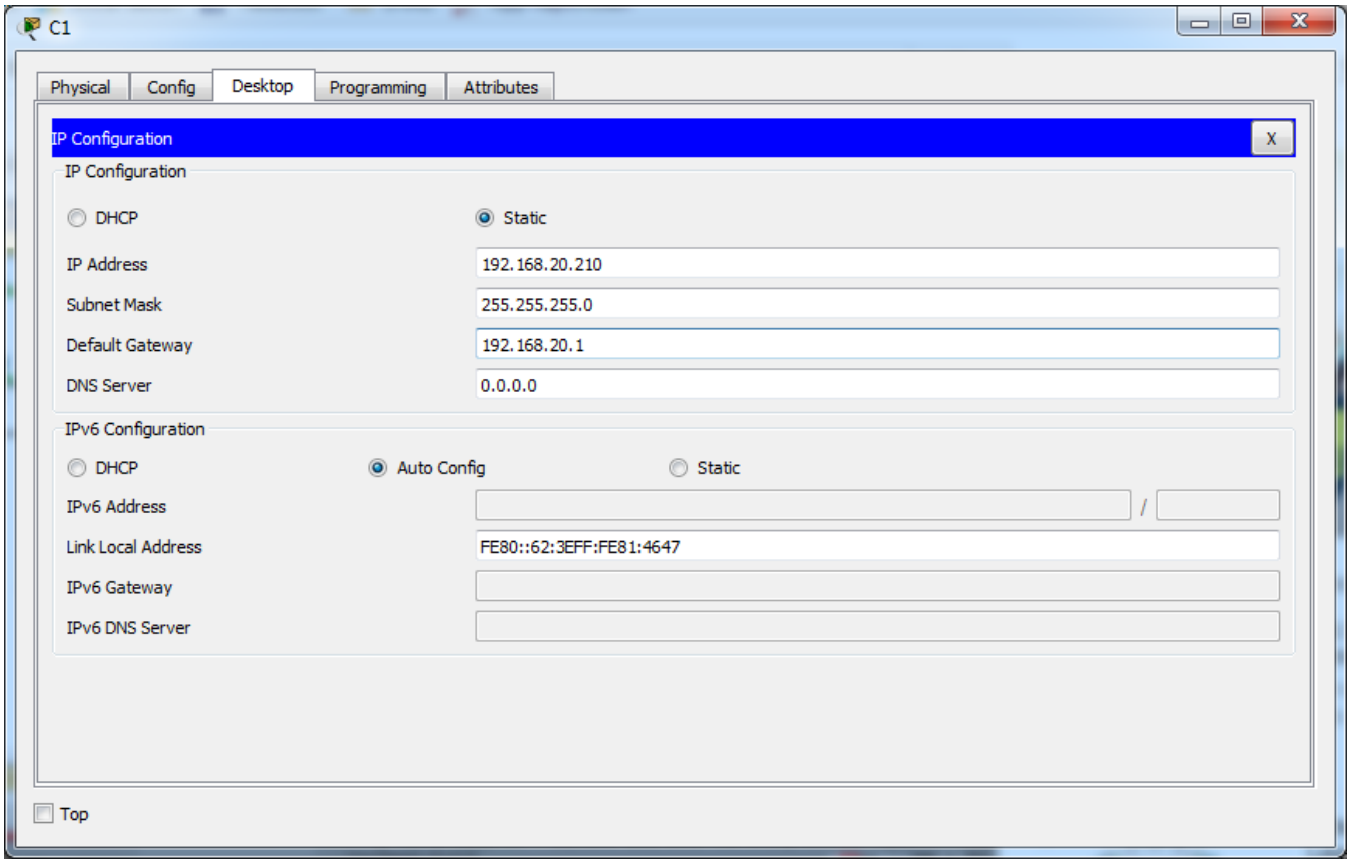
Central(config)# interface vlan 20

Central(config-if)# ip address 192.168.20.5 255.255.255.0

Step 3: Configure the management PC and connect it to SW-A port Fa0/1.

Ensure that the management PC is assigned an IP address within the 192.168.20.0/24 network. Connect the management PC to **SW-A** port Fa0/1.



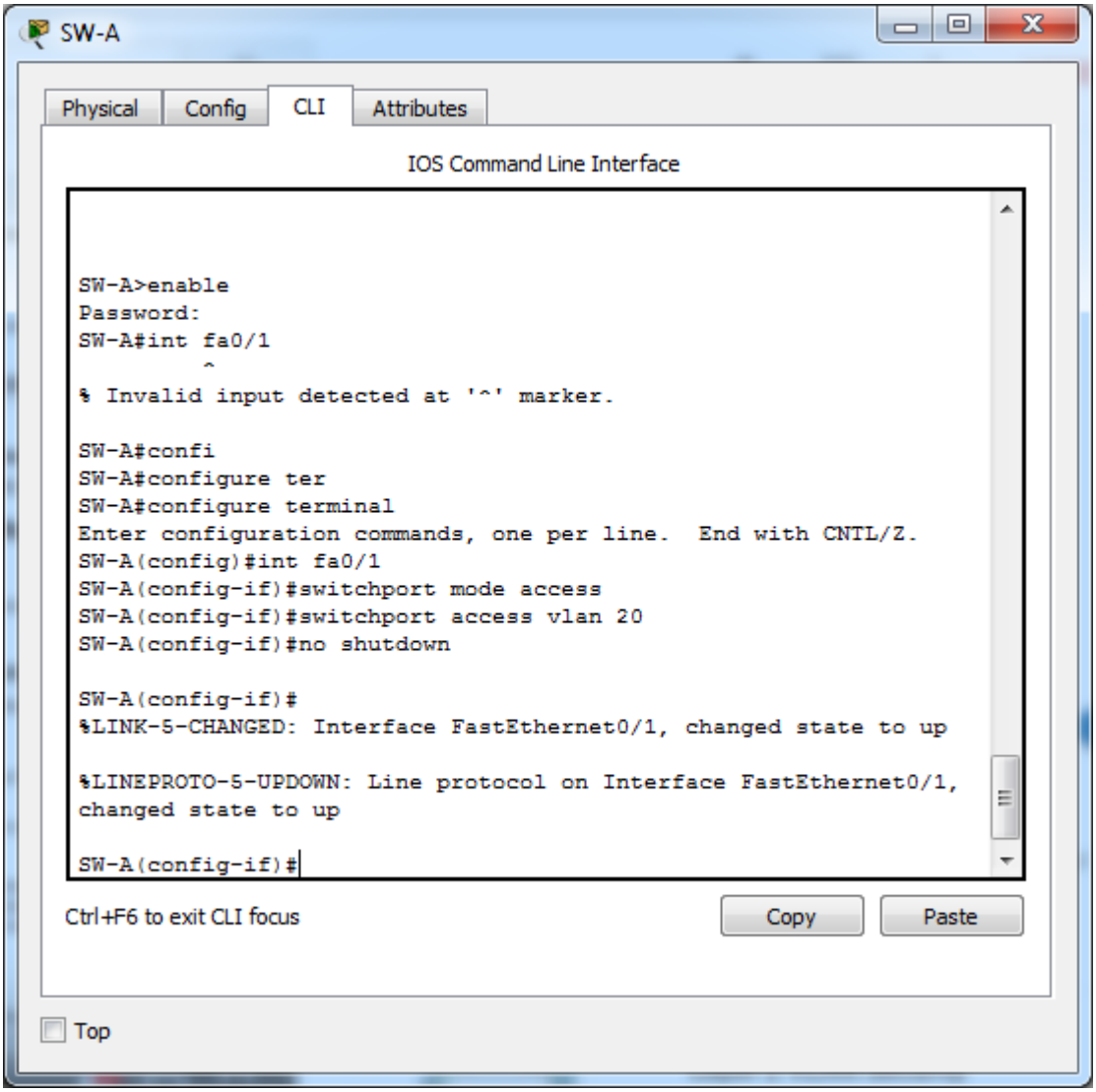


Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface Fa0/1 must be part of VLAN 20.

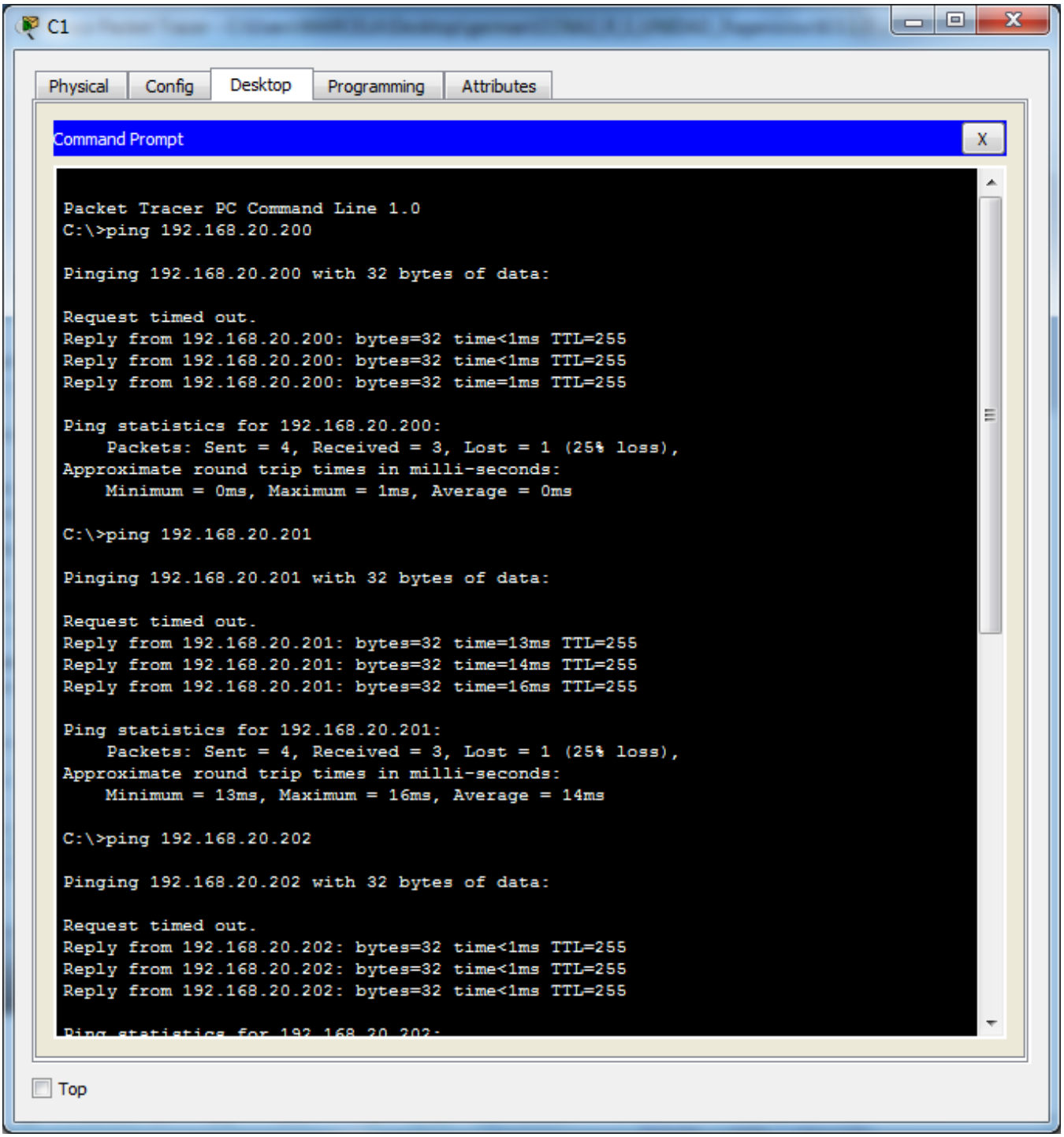
SW-A(config)# interface fa0/1

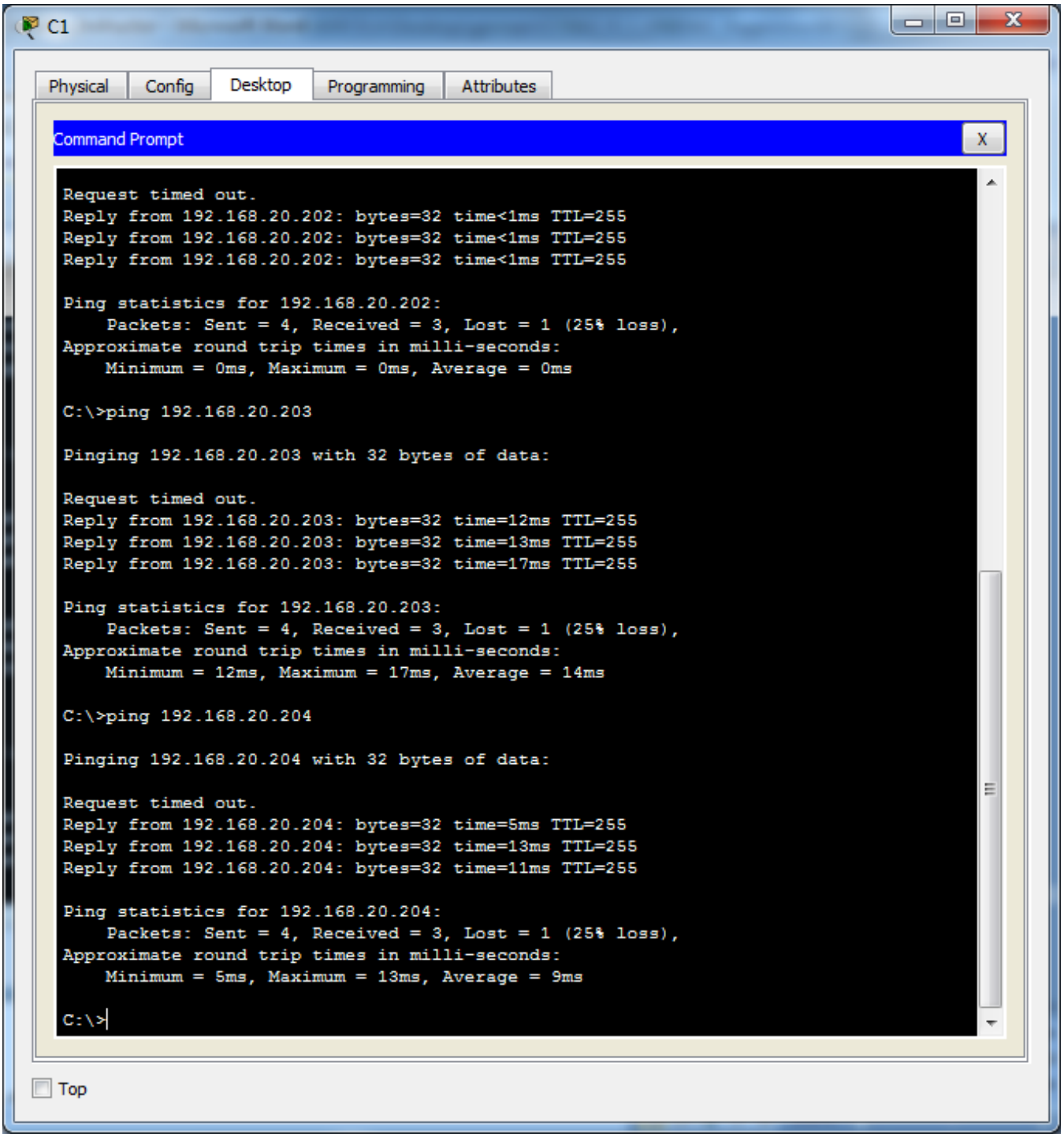
SW-A(config-if)# switchport access vlan 20SW-A(config-if)# no shutdown



Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping **SW-A**, **SW-B**, **SW-1**, **SW-2**, and **Central**.


C1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.200
Pinging 192.168.20.200 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.200: bytes=32 time<1ms TTL=255
Reply from 192.168.20.200: bytes=32 time<1ms TTL=255
Reply from 192.168.20.200: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.20.200:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.20.201
Pinging 192.168.20.201 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.201: bytes=32 time=13ms TTL=255
Reply from 192.168.20.201: bytes=32 time=14ms TTL=255
Reply from 192.168.20.201: bytes=32 time=16ms TTL=255
Ping statistics for 192.168.20.201:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 13ms, Maximum = 16ms, Average = 14ms
C:\>ping 192.168.20.202
Pinging 192.168.20.202 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.202: bytes=32 time<1ms TTL=255
Reply from 192.168.20.202: bytes=32 time<1ms TTL=255
Reply from 192.168.20.202: bytes=32 time<1ms TTL=255
Top



Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface Fa0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

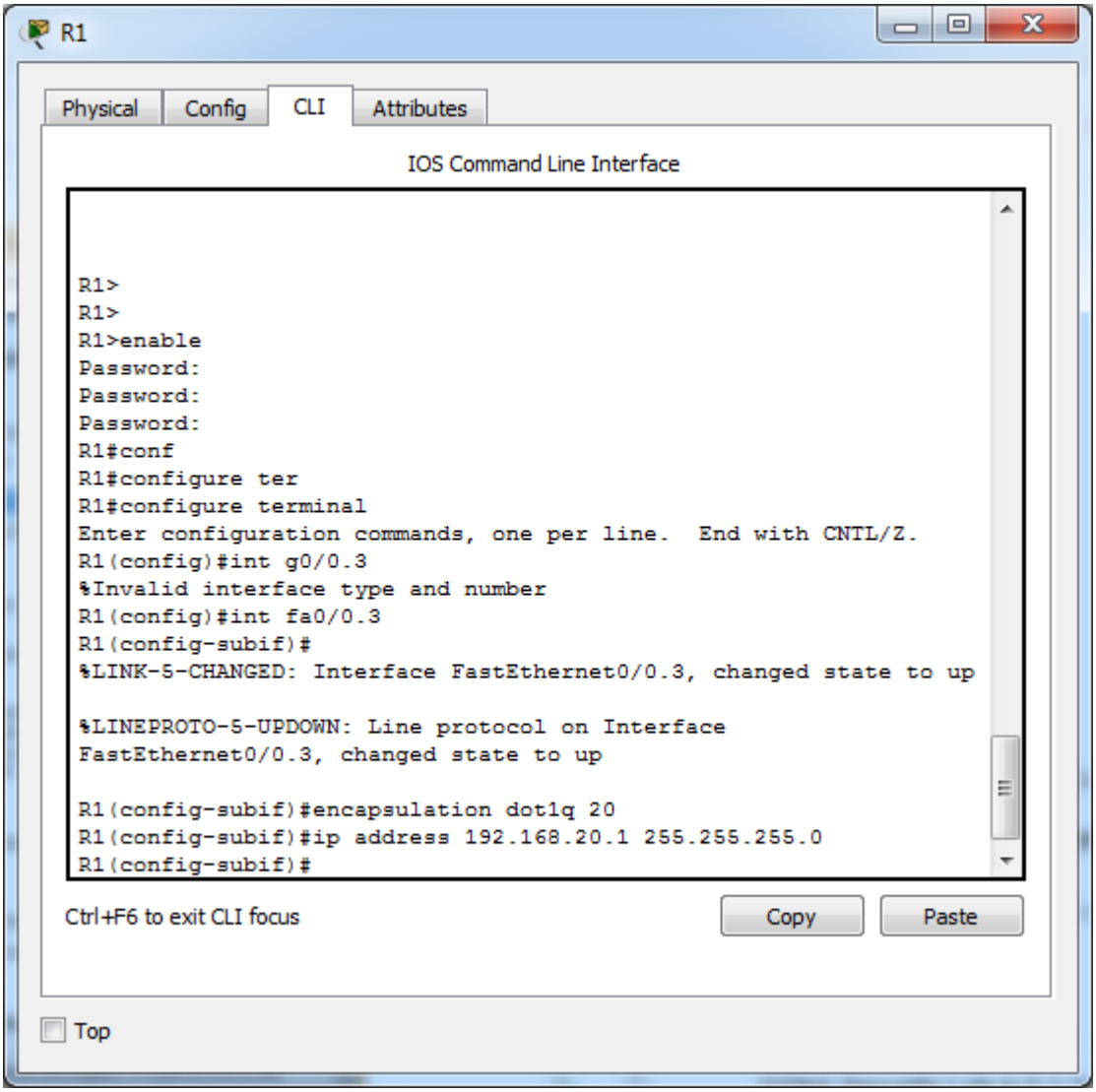
R1(config)# interface fa0/0.3

R1(config-subif)# encapsulation dot1q 20

b. Assign an IP address within the 192.168.20.0/24 network.

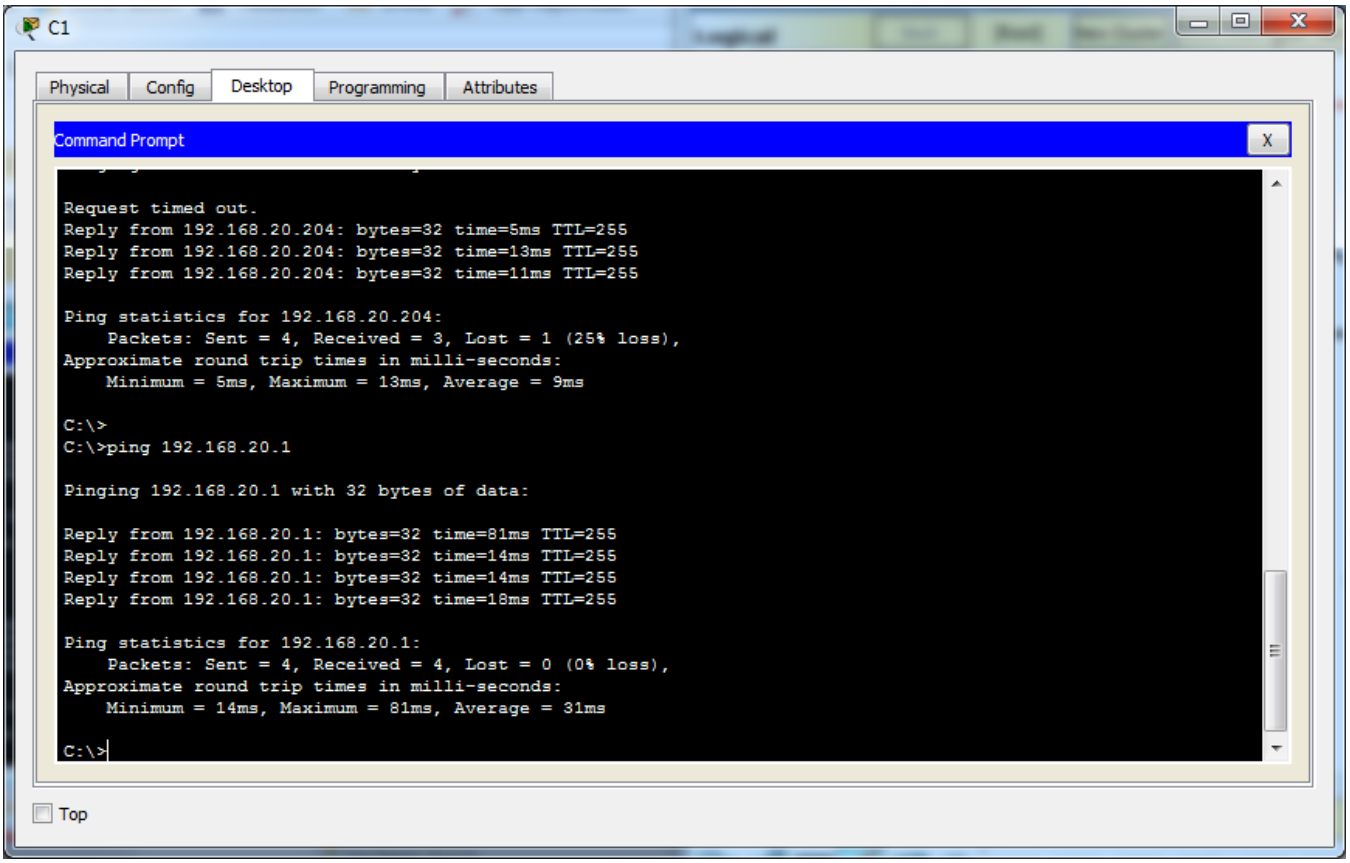
R1(config)# interface fa0/0.3

R1(config-subif)# ip address 192.168.20.100 255.255.255.0



Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.



Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that denies any network from accessing the 192.168.20.0/24 network, but permits all other networks to access one another.

Example: (may vary from student configuration)

R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255

R1(config)# access-list 101 permit ip any any

b. Apply the ACL to the proper interface(s).

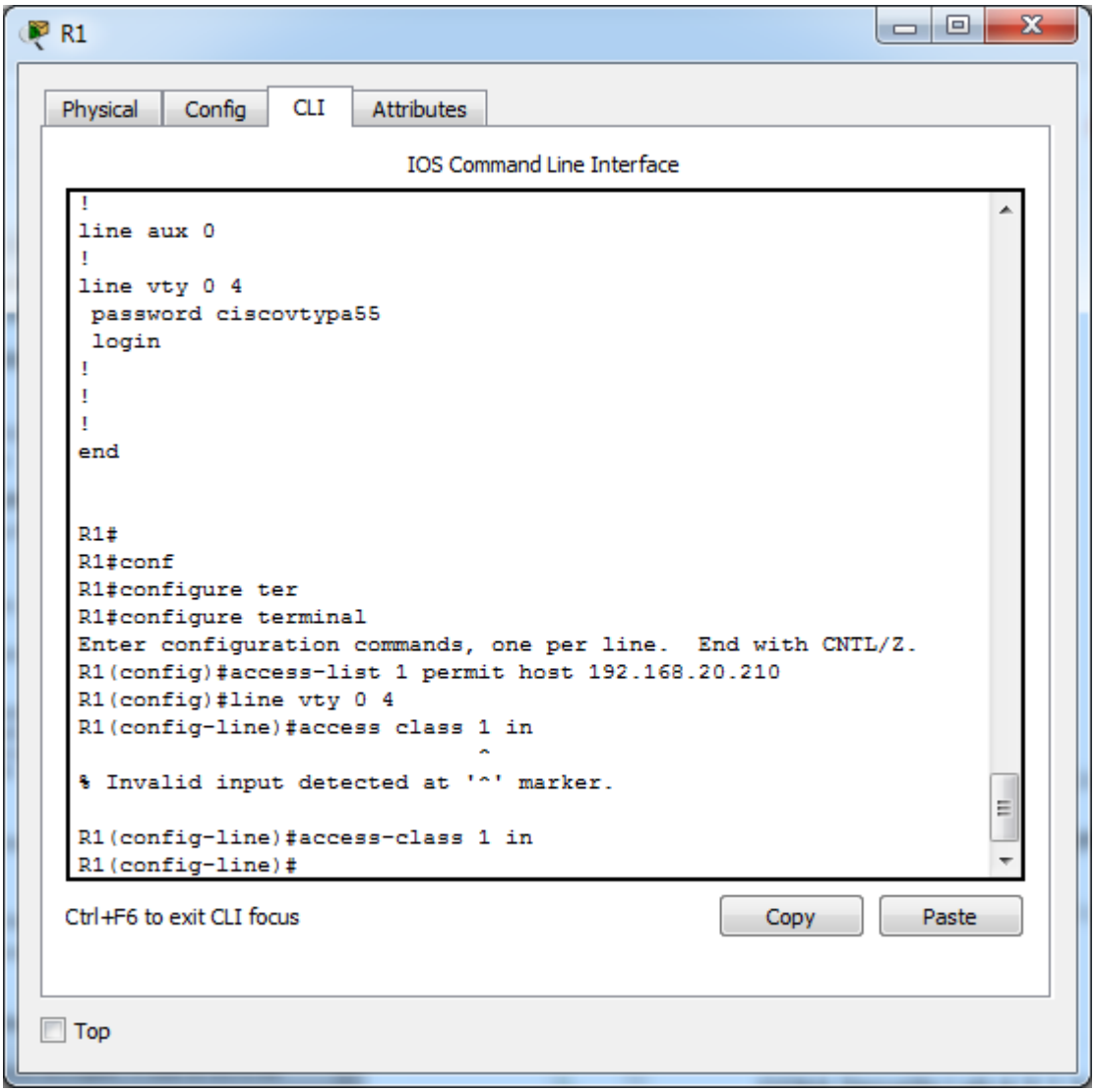
Example: (may vary from student configuration)

R1(config)# interface fa0/0.1

R1(config-subif)# ip access-group 101 in

R1(config-subif)# interface fa0/0.2

R1(config-subif)# ip access-group 101 in



Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

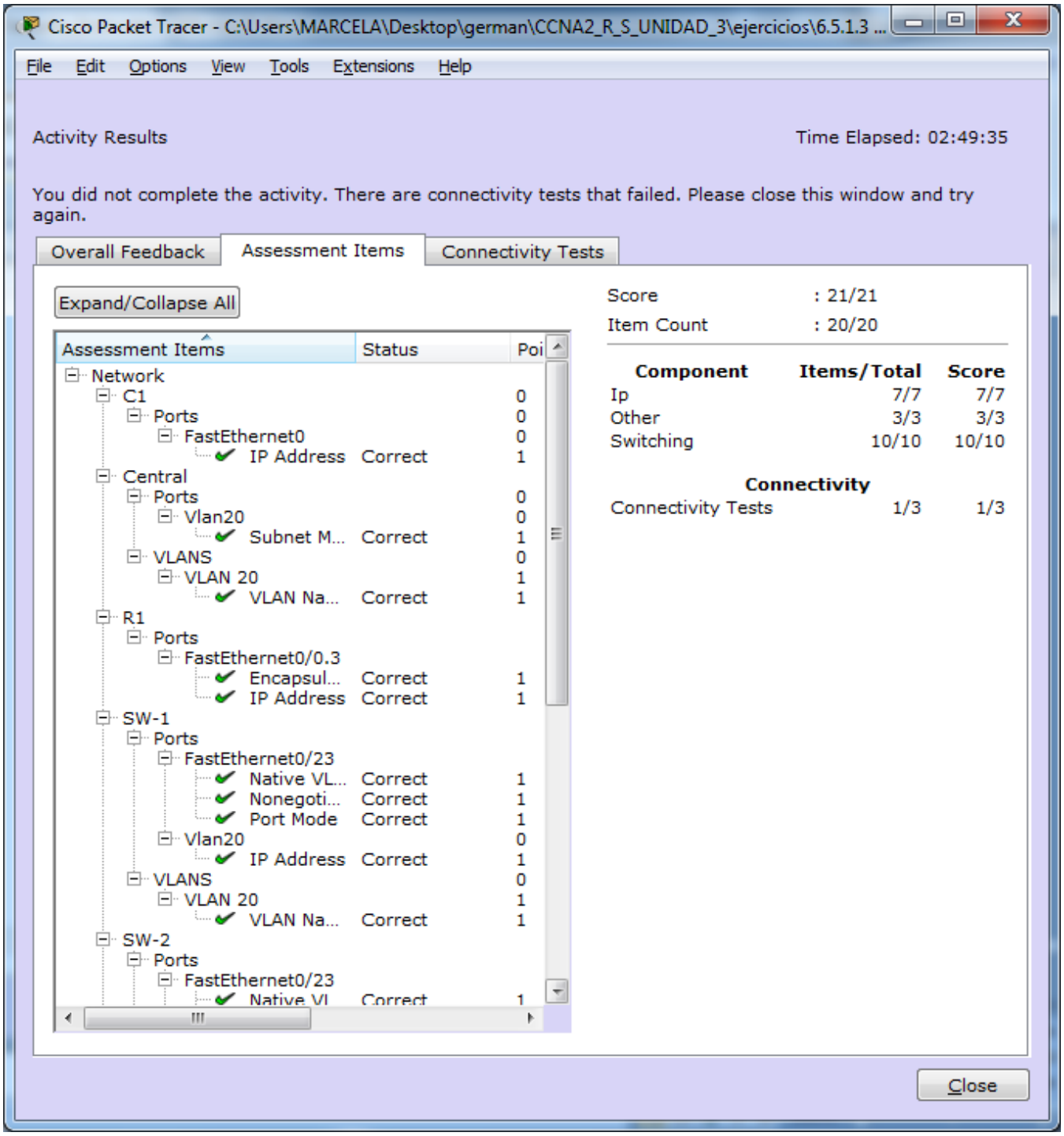
Los pings deberían haber sido exitosos porque todos los dispositivos dentro de la red 192.168.20.0 deberían ser capaz de hacer ping entre sí. Los dispositivos dentro de la VLAN20 no están obligados a enrutar a través del enrutador.

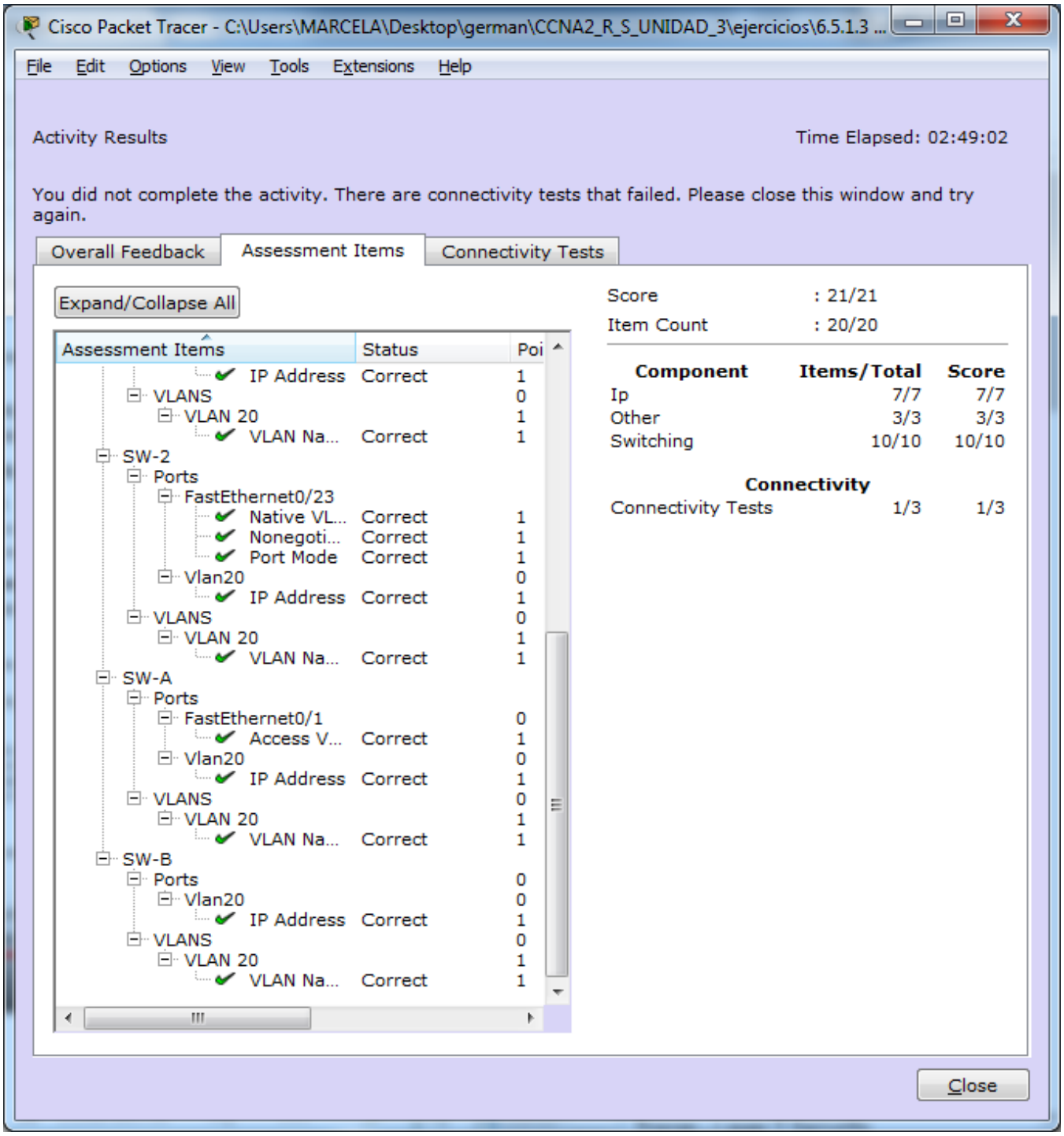
b. From **D1**, ping the management PC. Were the pings successful? Explain.

El ping debería haber fallado. Esto se debe a que para que un dispositivo dentro de una VLAN diferente tenga éxito
hacer ping a un dispositivo dentro de la VLAN20, debe enrutarse. El enrutador tiene una ACL que evita que todos los paquetes accediendo a la red 192.168.20.0.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

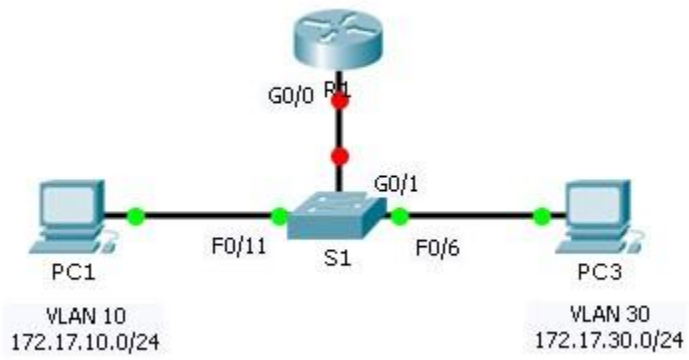
If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.


Cisco Packet Tracer - C:\Users\MARCELA\Desktop\german\CCNA2_R_S_UNIDAD_3\ejercicios\6.5.1.3 ...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 02:49:35
You did not complete the activity. There are connectivity tests that failed. Please close this window and try again.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Poi
Network
C1
0
Ports
0
FastEthernet0
0
IP Address
Correct
1
Central
Ports
0
Vlan20
0
Subnet M...
Correct
1
VLANS
0
VLAN 20
1
VLAN Na...
Correct
1
R1
Ports
FastEthernet0/0.3
Encapsul...
Correct
1
IP Address
Correct
1
SW-1
Ports
FastEthernet0/23
Native VL...
Correct
1
Nonegoti...
Correct
1
Port Mode
Correct
1
Vlan20
0
IP Address
Correct
1
VLANS
0
VLAN 20
1
VLAN Na...
Correct
1
SW-2
Ports
FastEthernet0/23
Native Vl
Correct
1
Score : 21/21
Item Count : 20/20
Component
Items/Total
Score
Ip
7/7
7/7
Other
3/3
3/3
Switching
10/10
10/10
Connectivity
Connectivity Tests
1/3
1/3
Close


Cisco Packet Tracer - C:\Users\MARCELA\Desktop\german\CCNA2_R_S_UNIDAD_3\ejercicios\6.5.1.3 ...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 02:49:02
You did not complete the activity. There are connectivity tests that failed. Please close this window and try again.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Poi
IP Address Correct 1
VLANS 0
VLAN 20 1
VLAN Na... Correct 1
SW-2
Ports
FastEthernet0/23
Native VL... Correct 1
Nonegoti... Correct 1
Port Mode Correct 1
Vlan20 0
IP Address Correct 1
VLANS 0
VLAN 20 1
VLAN Na... Correct 1
SW-A
Ports
FastEthernet0/1 0
Access V... Correct 1
Vlan20 0
IP Address Correct 1
VLANS 0
VLAN 20 1
VLAN Na... Correct 1
SW-B
Ports 0
Vlan20 0
IP Address Correct 1
VLANS 0
VLAN 20 1
VLAN Na... Correct 1
Score : 21/21
Item Count : 20/20
Component Items/Total Score
Ip 7/7 7/7
Other 3/3 3/3
Switching 10/10 10/10
Connectivity
Connectivity Tests 1/3 1/3
Close

5.1.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing Instructions IG

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Objectives

Part 1: Test Connectivity without Inter-VLAN Routing

Part 2: Add VLANs to a Switch

Part 3: Configure Subinterfaces

Part 4: Test Connectivity with Inter-VLAN Routing

Scenario

In this activity, you will check for connectivity prior to implementing inter-VLAN routing. You will then configure VLANs and inter-VLAN routing. Finally, you will enable trunking and verify connectivity between VLANs.

Part 1: Test Connectivity Without Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs are on separate networks and **R1** is not configured, the ping fails.

Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why? The ARP process failed because the ARP request was dropped by PC3. PC1 and PC3 are not on the same network, so PC1 never gets the MAC address for PC3. Without a MAC address, PC1 cannot create an ICMP echo request.

Part 2: Add VLANs to a Switch

Step 1: Create VLANs on S1.

Return to **Realtime** mode and create VLAN 10 and VLAN 30 on **S1**.

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

Step 2: Assign VLANs to ports.

a. Configure interface F0/6 and F0/11 as access ports and assign VLANs.

Assign **PC1** to VLAN 10.

Assign **PC3** to VLAN 30.

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

b. Issue the **show vlan brief** command to verify VLAN configuration.

S1# **show vlan brief**

```
VLAN Name                       Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                          Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                          Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                          Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                          Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                          Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                       active    Fa0/11
30   VLAN0030                       active    Fa0/6
1002 fddi-default                   active
1003 token-ring-default             active
1004 fddinet-default                active
1005 trnet-default                  activ
```

Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful? Each VLAN is a separate network and requires a router or a layer 3 switch to provide communication between them.

Part 3: Configure Subinterfaces

Step 1: Configure subinterfaces on R1 using the 802.1Q encapsulation.

a. Create the subinterface G0/0.10.

Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.

Refer to the **Address Table** and assign the correct IP address to the subinterface. b. Repeat for the G0/0.30 subinterface.

R1(config)# **int g0/0.10**

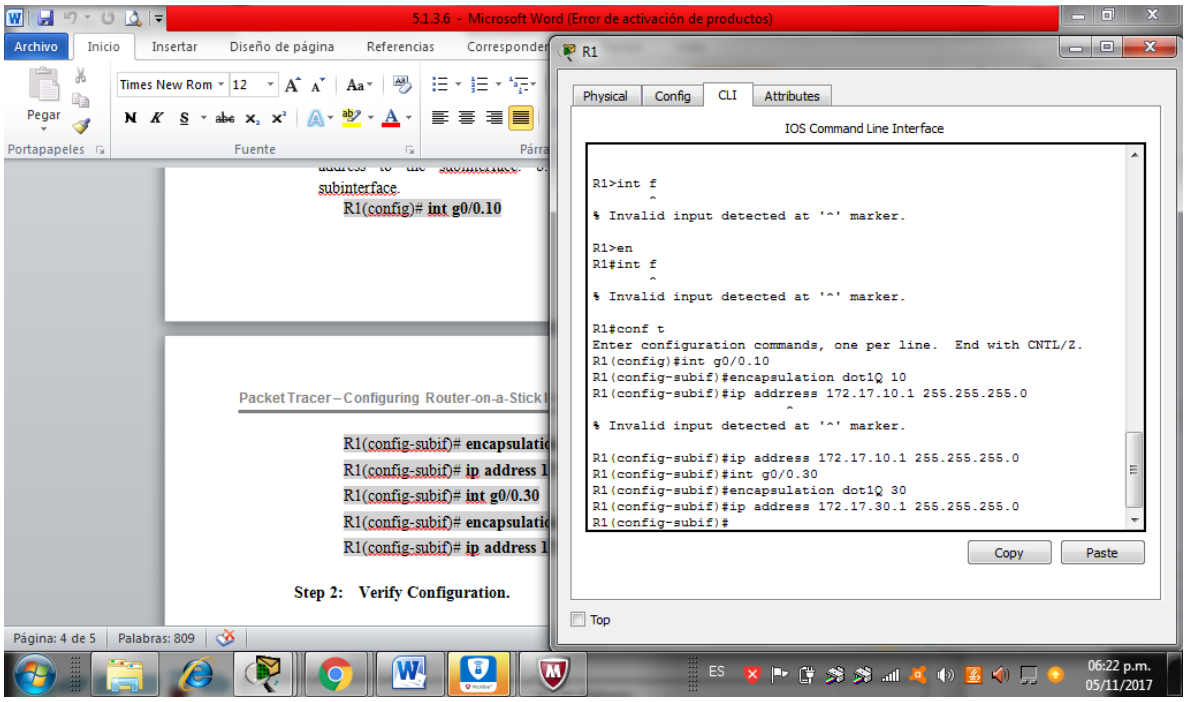
R1(config-subif)# **encapsulation dot1Q 10**

R1(config-subif)# **ip address 172.17.10.1 255.255.255.0**

R1(config-subif)# **int g0/0.30**

R1(config-subif)# **encapsulation dot1Q 30**

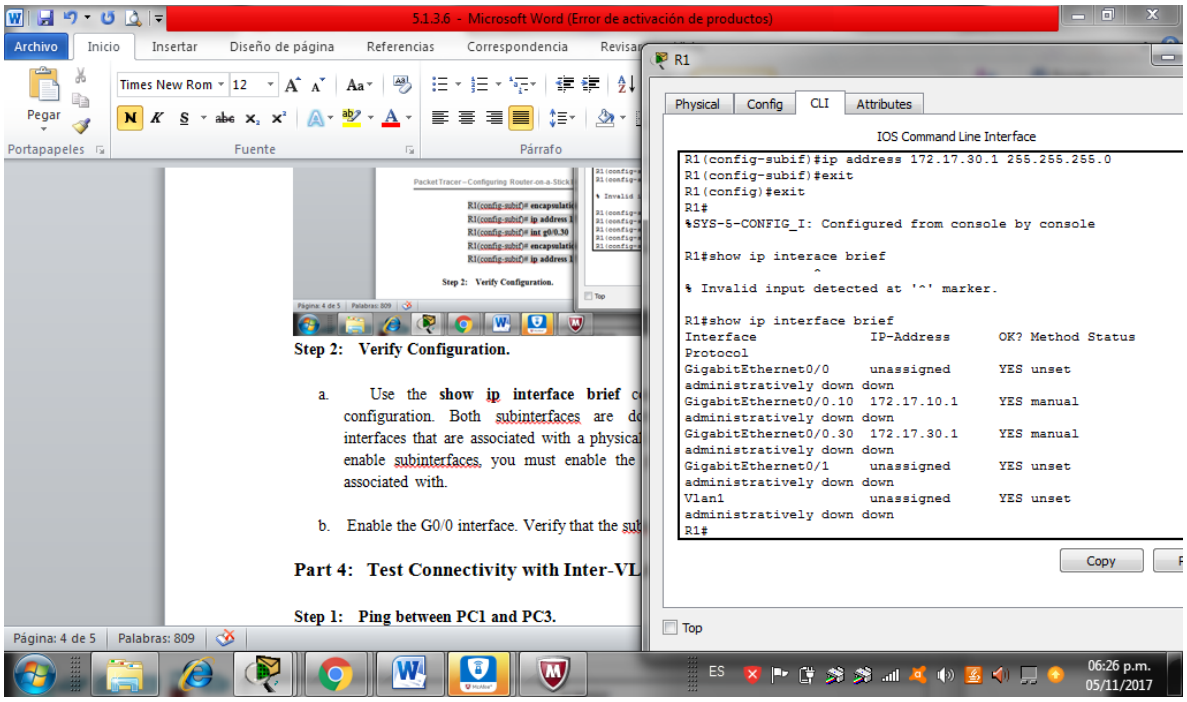
R1(config-subif)# **ip address 172.17.30.1 255.255.255.0**



Step 2: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

b. Enable the G0/0 interface. Verify that the subinterfaces are now active.



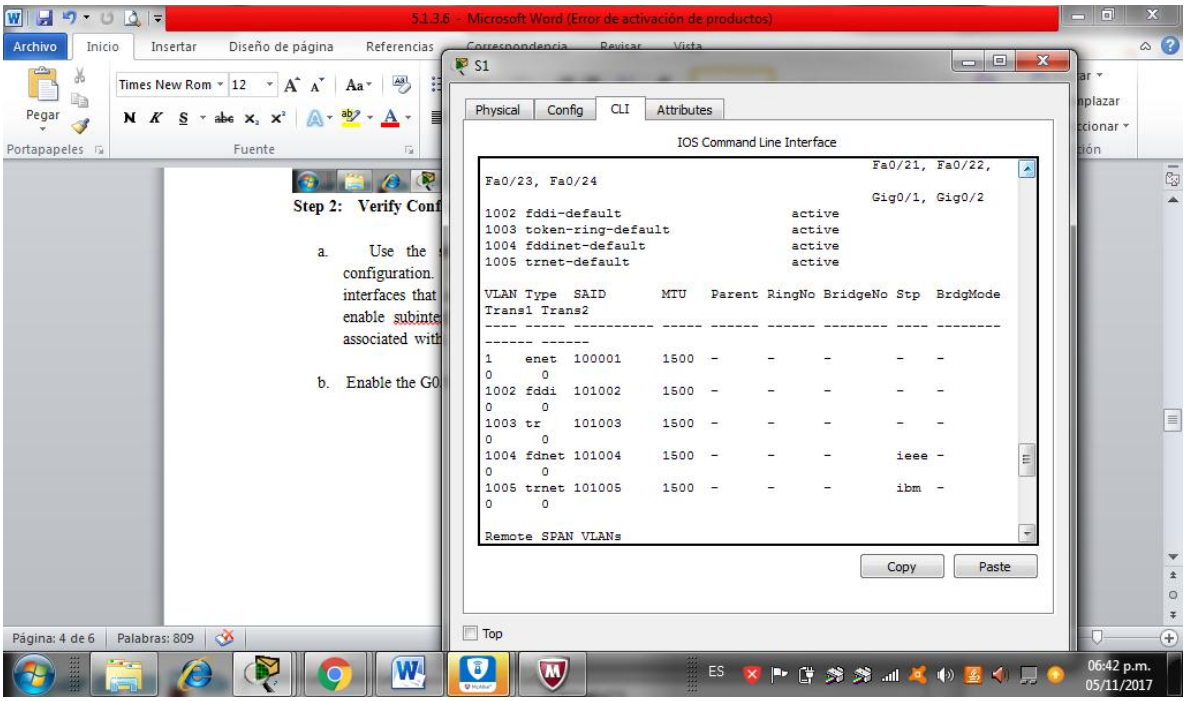
Part 4: Test Connectivity with Inter-VLAN Routing

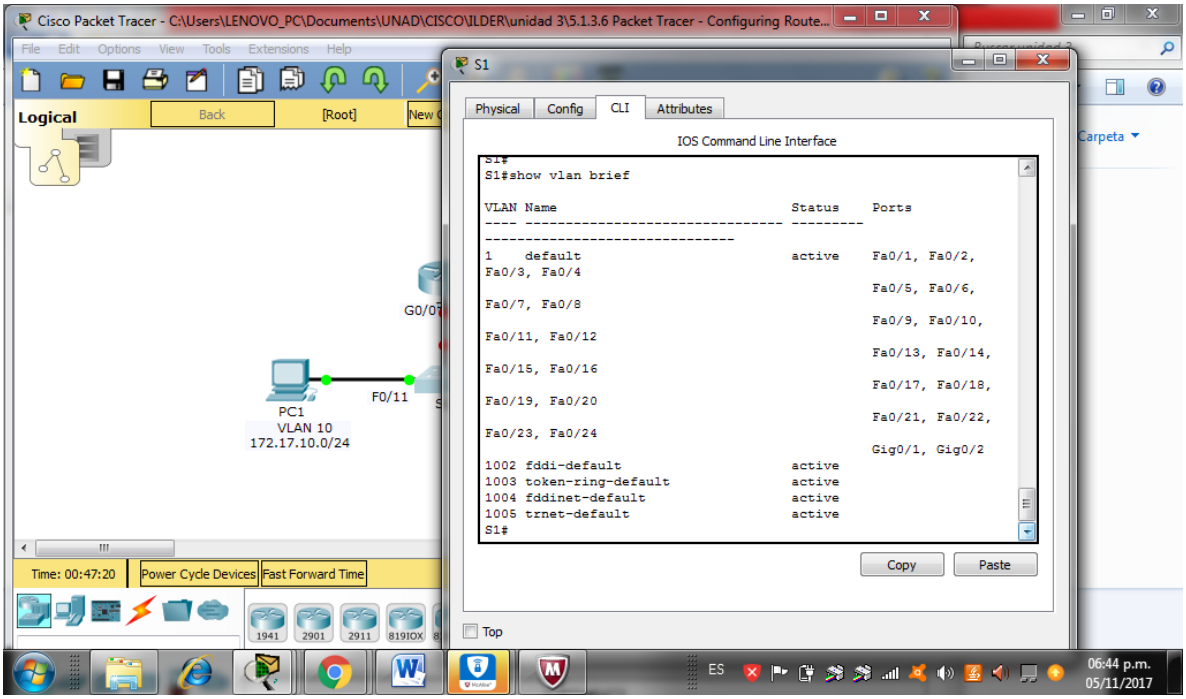
Step 1: Ping between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail.

Step 2: Enable trunking.

a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to? VLAN 1



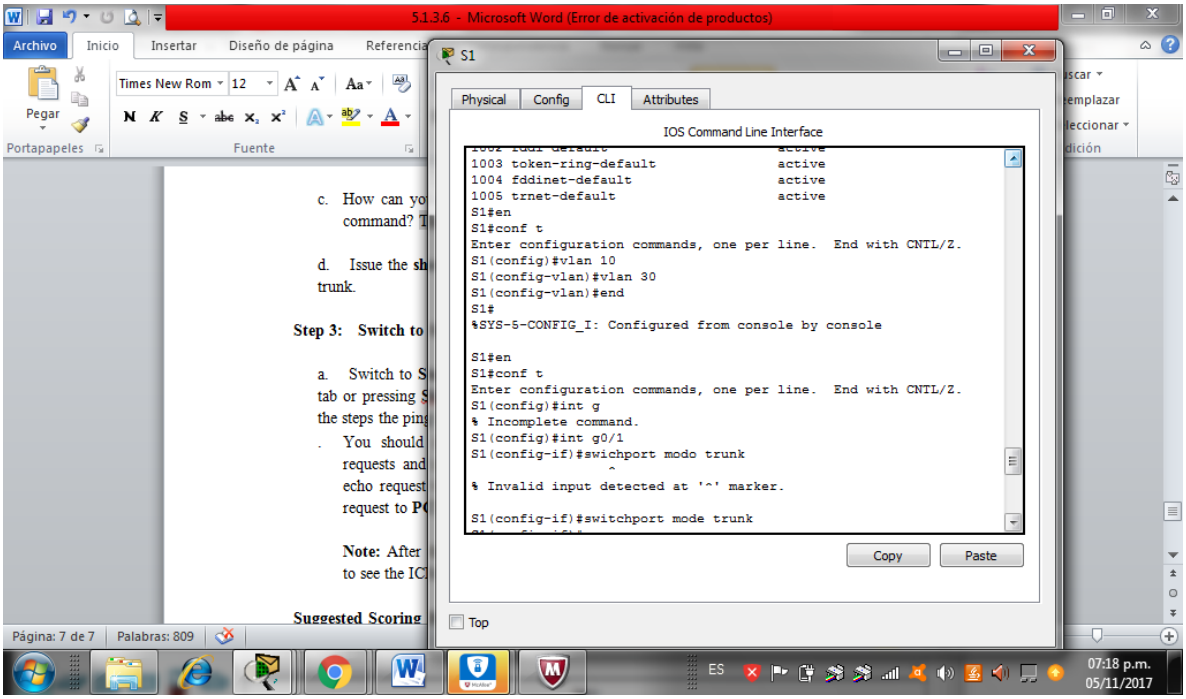


b. Because the router was configured with multiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk. Enable trunking on interface G0/1.

S1(config-if)# **int g0/1**

S1(config-if)# **switchport mode trunk**

c. How can you determine that the interface is a trunk port using the **show vlan** command? The interface is no longer listed under VLAN 1.



d. Issue the **show interface trunk** command to verify the interface is configured as a trunk.

Step 3: Switch to Simulation mode to monitor pings.

a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**. b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.

. You should see ARP requests and replies between **S1** and **R1**. Then ARP requests and replies between **R1** and **S3**. Then **PC1** can encapsulate an ICMP echo request with the proper data-link layer information and R1 will route the request to **PC3**.

Note: After the ARP process finishes, you may need to click Reset Simulation to see the ICMP process complete.

Suggested Scoring Rubric

Packet Tracer scores 60 points. The four questions are worth 10 points each.

3.3.2.2 Lab - Implementing VLAN Security

Práctica de laboratorio: implementación de seguridad de VLAN

Topología

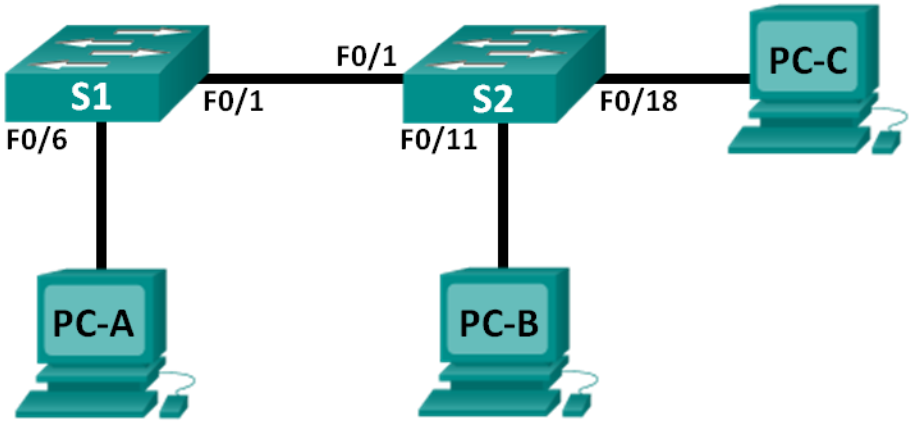


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

Objetivos

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

Parte 2: implementar seguridad de VLAN en los switches

Información básica/situación

La práctica recomendada indica que se deben configurar algunos parámetros básicos de seguridad para los puertos de enlace troncal y de acceso en los switches. Esto sirve como protección contra los ataques de VLAN y la posible detección del tráfico de la red dentro de esta.

En esta práctica de laboratorio, configurará los dispositivos de red en la topología con algunos parámetros básicos, verificará la conectividad y, a continuación, aplicará medidas de seguridad más estrictas en los switches. Utilizará varios comandos **show** para analizar la forma en que se comportan los switches Cisco. Luego, aplicará medidas de seguridad.

Nota: los switches que se utilizan en esta práctica de laboratorio son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros 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.

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

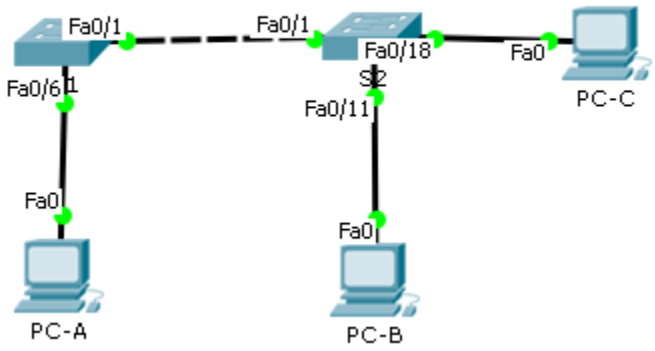
Recursos necesarios

- 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, como se muestra en la topología

Parte 1. Armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, configurará los parámetros básicos en los switches y las computadoras. Consulte la tabla de direccionamiento para obtener información sobre nombres de dispositivos y direcciones.

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

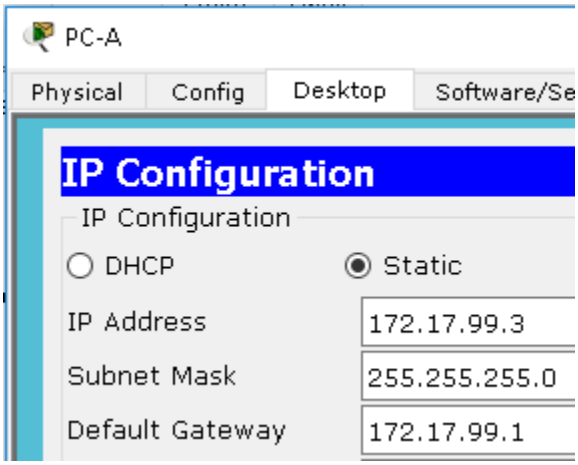


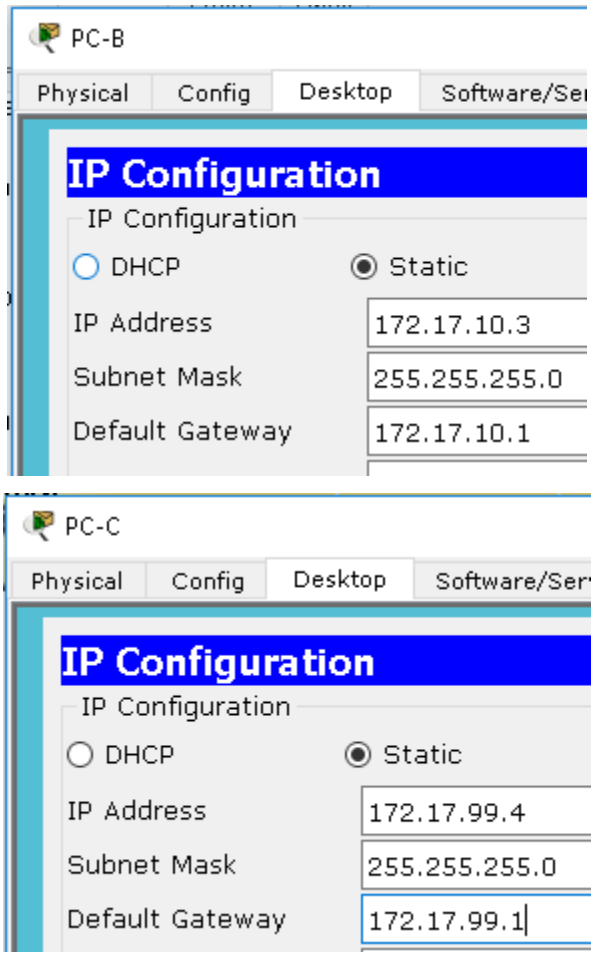
Paso 2. inicializar y volver a cargar los switches.

```
Switch>ena
Switch#relo
Switch#reload
Proceed with reload? [confirm]
```

Paso 3. configurar las direcciones IP en la PC-A, la PC-B y la PC-C.

Consulte la tabla de direccionamiento para obtener la información de direcciones de las computadoras.





Paso 4. configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

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

c. Asigne **class** como la contraseña del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de VTY y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

e. Configure el inicio de sesión sincrónico para las líneas de vty y de consola.

Para SW1

```
Switch>
Switch>
Switch>enable
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-loo
S1(config)#banner motd "Acceso restrigido"
S1(config)#service password-enc
S1(config)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#logging synch
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

En el SW 2

```
Switch>
Switch>
Switch>
Switch>enable
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-loo
S2(config)#banner motd "Acceso restrigido"
S2(config)#service password-enc
S2(config)#enable secret class
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#logging synch
S2(config-line)#
S2(config-line)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 5. configurar las VLAN en cada switch.

a. Cree las VLAN y asígneles nombres según la tabla de asignaciones de VLAN.

```
S1#conf t
Enter configuration commands, one per li
S1(config)#
S1(config)#vlan 10
S1(config-vlan)#name Data
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name BlackHole
S1(config-vlan)#
```

```
S2#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Data
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name BlackHole
S2(config-vlan)#exit
```

b. Configure la dirección IP que se indica para la VLAN 99 en la tabla de direccionamiento en ambos switches.

```
S1(config)#inter vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip addres 172.17.99.11 255.255.255.0
S1(config-if)#exit
S1(config)#ip defaul-g
S1(config)#ip def
S1(config)#ip default-gateway 172.17.99.1
```

```
S2(config)#int vlan 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shut
S2(config-if)#exit
S2(config)#ip d
S2(config)#ip de
S2(config)#ip default-gateway 172.17.99.1
```

c. Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.

```
S1(config)#interface fastEthernet 0/6
S1(config-if)#swi
S1(config-if)#switchport acc
S1(config-if)#switchport access vlan 99
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#
```

d. Configure F0/11 en el S2 como puerto de acceso y asígnelo a la VLAN 10.

```
S2(config)#interface fastEthernet 0/11
S2(config-if)#s
S2(config-if)#sw
S2(config-if)#switchport acc
S2(config-if)#switchport access vlan 10
S2(config-if)#
```

e. Configure F0/18 en el S2 como puerto de acceso y asígnelo a la VLAN 99.

```
S2(config)#interface fastEthernet 0/18
S2(config-if)#switchport access vlan 99
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S2(config-if)#
```

f. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN y de puertos.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   Data                              active
99   Management&Native                 active    Fa0/6
999  BlackHole                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Data                              active    Fa0/11
99   Management&Native                 active    Fa0/18
999  BlackHole                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
```

¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2?

Todos lo puertos por defecto se asigna a la Vlan 1__

Paso 6. configurar la seguridad básica del switch.

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

b. Encripte todas las contraseñas.

```
Switch>
Switch>
Switch>enable
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-loo
S1(config)#banner motd "Acceso restrigido"
S1(config)#service password-enc
S1(config)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#logging synch
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch>
Switch>
Switch>
Switch>enable
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-loo
S2(config)#banner motd "Acceso restrigido"
S2(config)#service password-enc
S2(config)#enable secret class
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#logging synch
S2(config-line)#
S2(config-line)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Desactive todos los puertos físicos sin utilizar.

```
S1(config)#interface range fas 0/2-5, fas 0/7-24, g0/1-2
S1(config-if-range)#shut
S1(config-if-range)#shutdown
```

```
S2(config)#interface range fas 0/2-10, fas 0/12-1, fas 0/19-24, g0/1-2
S2(config-if-range)#shut
S2(config-if-range)#shutdown
```

d. Deshabilite el servicio web básico en ejecución.

S1(config)# **no ip http server**

```
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#no ip http server
                  ^
% Invalid input detected at '^' marker.

S1(config)#
```

S2(config)# **no ip http server**

```
S2(config)#no ip http server
                  ^
% Invalid input detected at '^' marker.
```

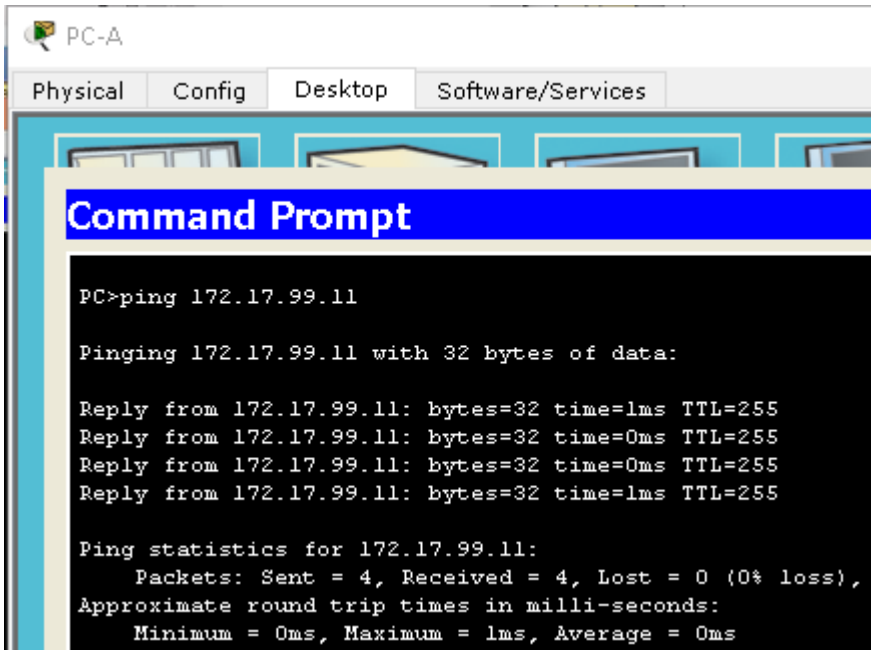
e. Copie la configuración en ejecución en la configuración de inicio.

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

```
S2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Paso 7. verificar la conectividad entre la información de VLAN y los dispositivos.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?



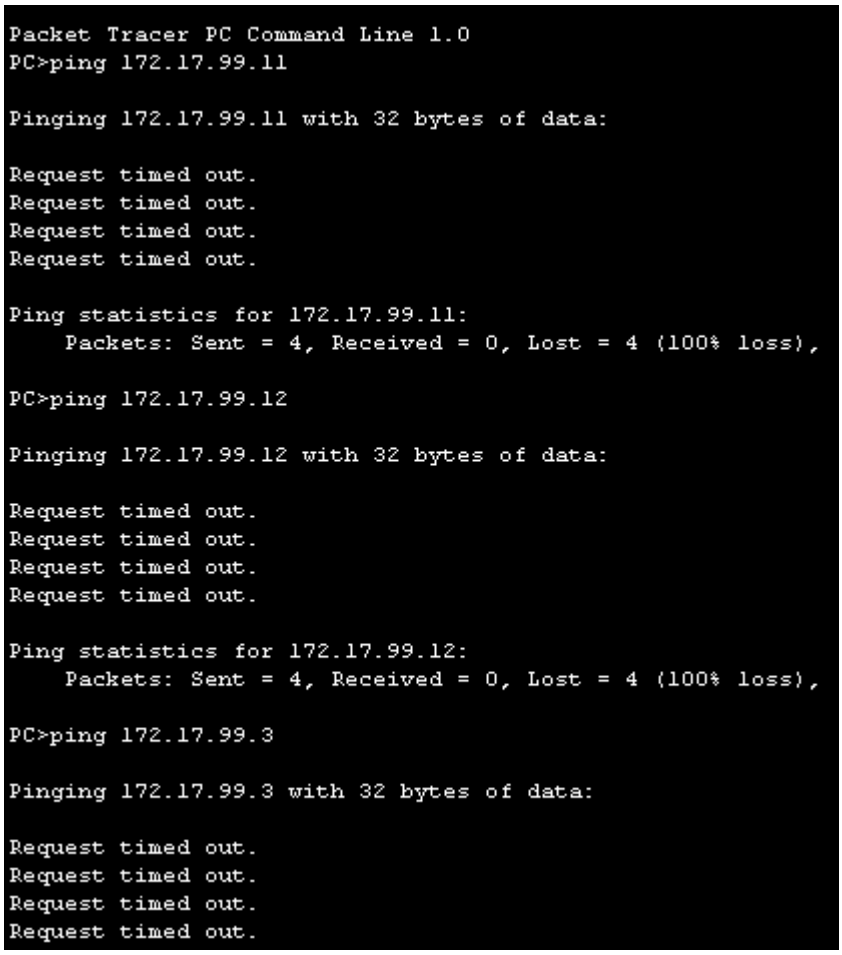
Es satisfactirio porque el PC esta en la misma Vlan y la direccion administrativa.

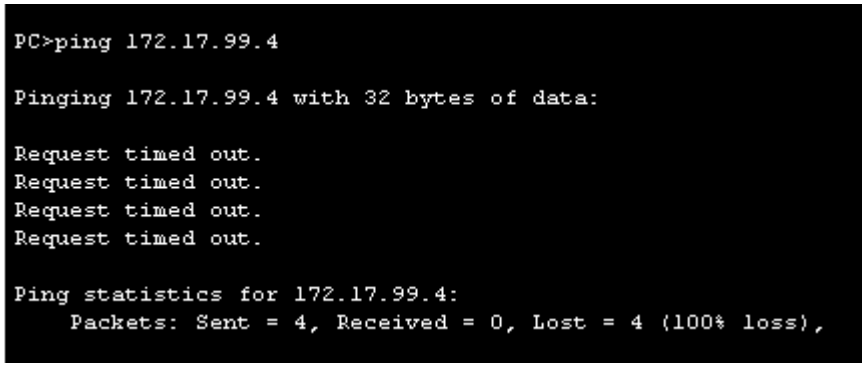
b. Desde el S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

El ping no es satisfactorio porque la dirección administrativa en S1 en el Switch 1 y 2 son la misma pero la interface F0/1 no esta configurada como Puerto troncal. El Puerto F0/1 esta en la Vlan 1 y no en la Vlan 99

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?





Los pigns a S1, S2, PC-A y PC-C desde el PC-B no son satisfactorios. Porque el PC-B esta en la Vlan 10 y a S1, S2, PC-A y PC-C estan el la Vlan 99. No hay dispositivo de capa 3 que pueda entutar los paquetes entre las redes

d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2. ¿Tuvo éxito? ¿Por qué?

```
Packet Tracer PC Command Line 1.0
PC>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

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

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Solo se reciben paquetes en el S2, El PC-C hace parte de la mismo Vlan de S1 y S2. Pero la PC-C no puede hacer ping a S1 porque no tiene un enlace troncal para llegar a él.

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

Parte 3. implementar seguridad de VLAN en los switches

Paso 1. configurar puertos de enlace troncal en el S1 y el S2.

e. Configure el puerto F0/1 en el S1 como puerto de enlace troncal.

S1(config)# **interface f0/1**
S1(config-if)# **switchport mode trunk**

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode trunk
```

f. Configure el puerto F0/1 en el S2 como puerto de enlace troncal.

S2(config)# **interface f0/1**
S2(config-if)# **switchport mode trunk**

```
S2(config)#interface fastEthernet 0/1
S2(config-if)#switchport mode trunk
```

g. Verifique los enlaces troncales en el S1 y el S2. Emita el comando **show interface trunk** en los dos switches.

S1# **show interface trunk**

```
S1(config)#show interface trunk
           ^
% Invalid input detected at '^' marker.

S1(config)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

```
S2(config-if)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,99,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,99,999

Paso 2. cambiar la VLAN nativa para los puertos de enlace troncal en el S1 y el S2.

Es aconsejable para la seguridad cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.

a. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?

En los SW están en la vlan nativa 1

b. Configure la VLAN nativa de la interfaz de enlace troncal F0/1 del S1 en la VLAN 99 Management&Native.

S1# **config t**

S1(config)# **interface f0/1**

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

Espere unos segundos. Debería comenzar a recibir mensajes de error en la sesión de consola del S1. ¿Qué significa el mensaje %CDP-4-NATIVE_VLAN_MISMATCH:?

```
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(99), with S2 FastEthernet0/1 (1).
```

Este es un mensaje Cisco Discovery Protocol(CDP) este mensaje indica que el S1 y S2 que las Vlan no coinciden, S2 tiene la Valn 1. Y S1 tiene la Vlan 99

___

c. Configure la VLAN 99 como VLAN nativa de la interfaz de enlace troncal F0/1 del S2.

S2(config)# **interface f0/1**

S2(config-if)# **switchport trunk native vlan 99**

```
S2(config)#interface f0/1
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on
VLAN0099. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port
consistency restored.
```

d. Verifique que ahora la VLAN nativa sea la 99 en ambos switches. A continuación, se muestra el resultado del S1.

```
S2(config-if)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

```
S1(config-if)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

S1# **show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,99,999

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	10,999

Paso 3. verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.

a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

```
PC>
PC>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Reply from 172.17.99.11: bytes=32 time=1ms TTL=255
Reply from 172.17.99.11: bytes=32 time=0ms TTL=255
Reply from 172.17.99.11: bytes=32 time=0ms TTL=255
Reply from 172.17.99.11: bytes=32 time=0ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

El ping es satisfactorio, el pc esta en la misma Vlan que la interfase administrativa del SW

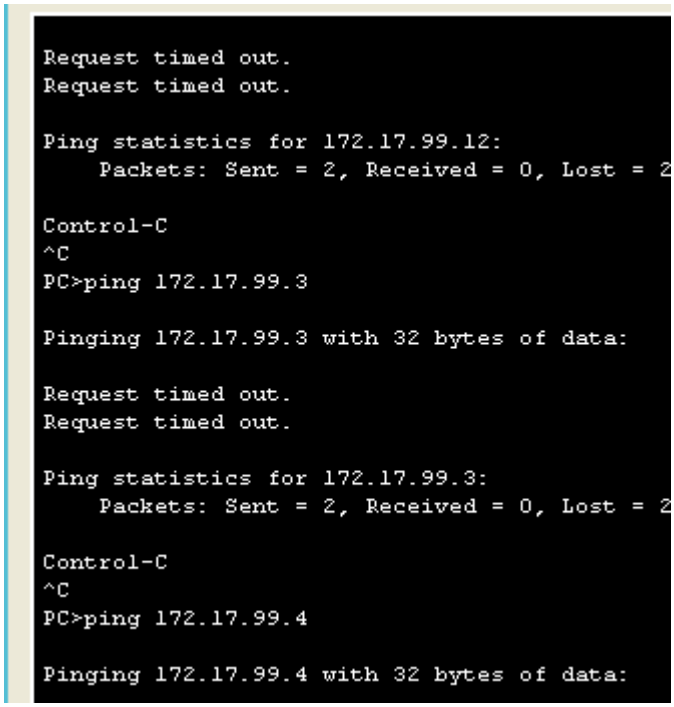
b. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

```
S1(config)#do ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

El ping fue satisfactorio, las troncales fueron correctamente establacidad para la Vlan 99

—

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?



Los pings no fueron satisfactorios porque la PC-B esta en la Vlan 10 y los otros equipos estan en la Vlan 99. No hay dispositovo de enrutamiento.

—

d. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A. ¿Tuvo éxito? ¿Por qué?

```
Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

PC>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Reply from 172.17.99.3: bytes=32 time=0ms TTL=128
Reply from 172.17.99.3: bytes=32 time=0ms TTL=128
Reply from 172.17.99.3: bytes=32 time=0ms TTL=128
Reply from 172.17.99.3: bytes=32 time=0ms TTL=128

Ping statistics for 172.17.99.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Los Pings fueron satisfactorios porque el PC-C esta en la misma Vlan de S1, S2 y PC-A

Paso 4. impedir el uso de DTP en el S1 y el S2.

Cisco utiliza un protocolo exclusivo conocido como “protocolo de enlace troncal dinámico” (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del siguiente comando:

S1# **show interface f0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

<Output Omitted>

```
S1(config)#do show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

a. Desactive la negociación en el S1.

S1(config)# **interface f0/1**

S1(config-if)# **switchport nonegotiate**

```
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
```

b. Desactive la negociación en el S2.

S2(config)# **interface f0/1**

S2(config-if)# **switchport nonegotiate**

```
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
```

c. Verifique que la negociación esté desactivada mediante la emisión del comando **show interface f0/1 switchport** en el S1 y el S2.

S1# **show interface f0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: Off

<Output Omitted>

```
S1(config)#do show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

```
S2(config)#do show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

Paso 5. implementar medidas de seguridad en los puertos de acceso del S1 y el S2.

Aunque desactivó los puertos sin utilizar en los switches, si se conecta un dispositivo a uno de esos puertos y la interfaz está habilitada, se podría producir un enlace troncal. Además, todos los puertos están en la VLAN 1 de manera predeterminada. Se recomienda colocar todos los puertos sin utilizar en una VLAN de "agujero negro". En este paso, deshabilitará los enlaces troncales en todos los puertos sin utilizar. También asignará los puertos sin utilizar a la VLAN 999. A los fines de esta práctica de laboratorio, solo se configurarán los puertos 2 a 5 en ambos switches.

a. Emita el comando **show interface f0/2 switchport** en el S1. Observe el modo administrativo y el estado para la negociación de enlaces troncales.

S1# **show interface f0/2 switchport**

Name: Fa0/2

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: down

Administrative Trunking Encapsulation: dot1q

Negotiation of Trunking: On

<Output Omitted>

```
S1(config)#do show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

b. Deshabilite los enlaces troncales en los puertos de acceso del S1.

S1(config)# **interface range f0/2 – 5**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**

```
S1(config)#interface range f0/2-5
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
```

c. Deshabilite los enlaces troncales en los puertos de acceso del S2.

```
S2(config)#int range fa0/2-5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
```

d. Verifique que el puerto F0/2 esté establecido en modo de acceso en el S1.

S1# **show interface f0/2 switchport**

Name: Fa0/2

Switchport: Enabled

Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>

```
S1(config)#interface range f0/2-5
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#do show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

e. Verifique que las asignaciones de puertos de VLAN en ambos switches sean las correctas. A continuación, se muestra el S1 como ejemplo.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Data	active	
99	Management&Native	active	Fa0/6
999	BlackHole	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Restrict VLANs allowed on trunk ports.

```
S1(config)#do show vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1(config)#
```

De manera predeterminada, se permite transportar todas las VLAN en los puertos de enlace troncal. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.

f. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10 y 99.

S1(config)# **interface f0/1**

S1(config-if)# **switchport trunk allowed vlan 10,99**

```
S1(config)#interface f0/1
S1(config-if)#switchport trunk allowed vlan 10,99
```

g. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10 y 99.

```
S2(config)#int range fa0/2-5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
```

h. Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo EXEC privilegiado en el S1 y el S2

S1# **show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	10,99

Port	Vlans allowed and active in management domain
Fa0/1	10,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 10,99

```
S1(config-if)#do sho int tru
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

¿Cuál es el resultado?

Solo la Vlan 10 y 99 están permitadas en el enlace troncal entre S1 y S2

–

Reflexión

¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco?

Todos los puertos están asignados a la Valn 1 por defecto, eso es un problema de seguridad. Algunos Switches cisco las trocales están en auto negociación los cuales los enlaces troncales pueden ser encendidos por cualquier persona. Los password de consola están mostrados como tipo texto.

3.2.2.4 Packet Tracer - Configuring Trunks Instructions IG

Tabla de direccionamiento

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

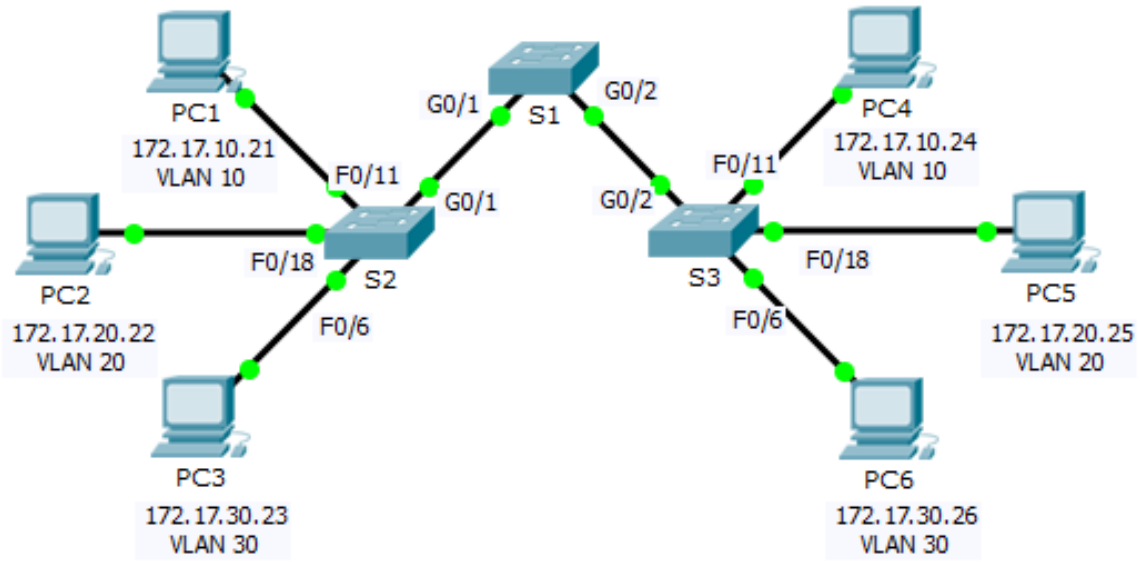
Objetivos

Parte 1: verificar las VLAN

Parte 2: configurar enlaces troncales

Información básica

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



Parte 1: verificar las VLAN

Paso 1: mostrar las VLAN actuales.

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

```
S1>
S1>en
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
S1#
```

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

```
S2>
S2>en
S2#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                   Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                   Fa0/24, Gig0/1, Gig0/2
10   Faculty/Staff                       active    Fa0/11
20   Students                            active    Fa0/18
30   Guest(Default)                      active    Fa0/6
99   Management&Native                   active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
```

```
S3>en
S3#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   Faculty/Staff                     active    Fa0/11
20   Students                          active    Fa0/18
30   Guest(Default)                    active    Fa0/6
99   Management&Native                 active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
```

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

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

Parte 2: configurar los enlaces troncales

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

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

```
S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#inter range g0/1-g0/2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport native vlan 99
S1(config-if-range)#
```

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

```
S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#inter range g0/1-g0/2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport native vlan 99
S1(config-if-range)#
```

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

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

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

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

Si bien hay una incompatibilidad de VLAN nativa, los pings entre las computadoras de la misma VLAN ahora se realizan de forma correcta.

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

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

S2

```
S2>
S2>en
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30
S2#
```

S3

```
S3>en
S3#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/2      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      10,20,30
S3#
```

¿Qué VLAN activas se permiten a través del enlace troncal?

Respuesta: La vlan 1.

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

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

```
S2(config)#interface g0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport native vlan 99
```

```
S3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface g0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport native vlan 99
S3(config-if)#exit
S3(config)#
```

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

S1

```
S1>
S1>
S1>en
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99
Gig0/2      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,99
Gig0/2      1,10,20,30,99
S1#
S1#
```

S2

```
S2>en
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,99
S2#
S2#
S2#
```

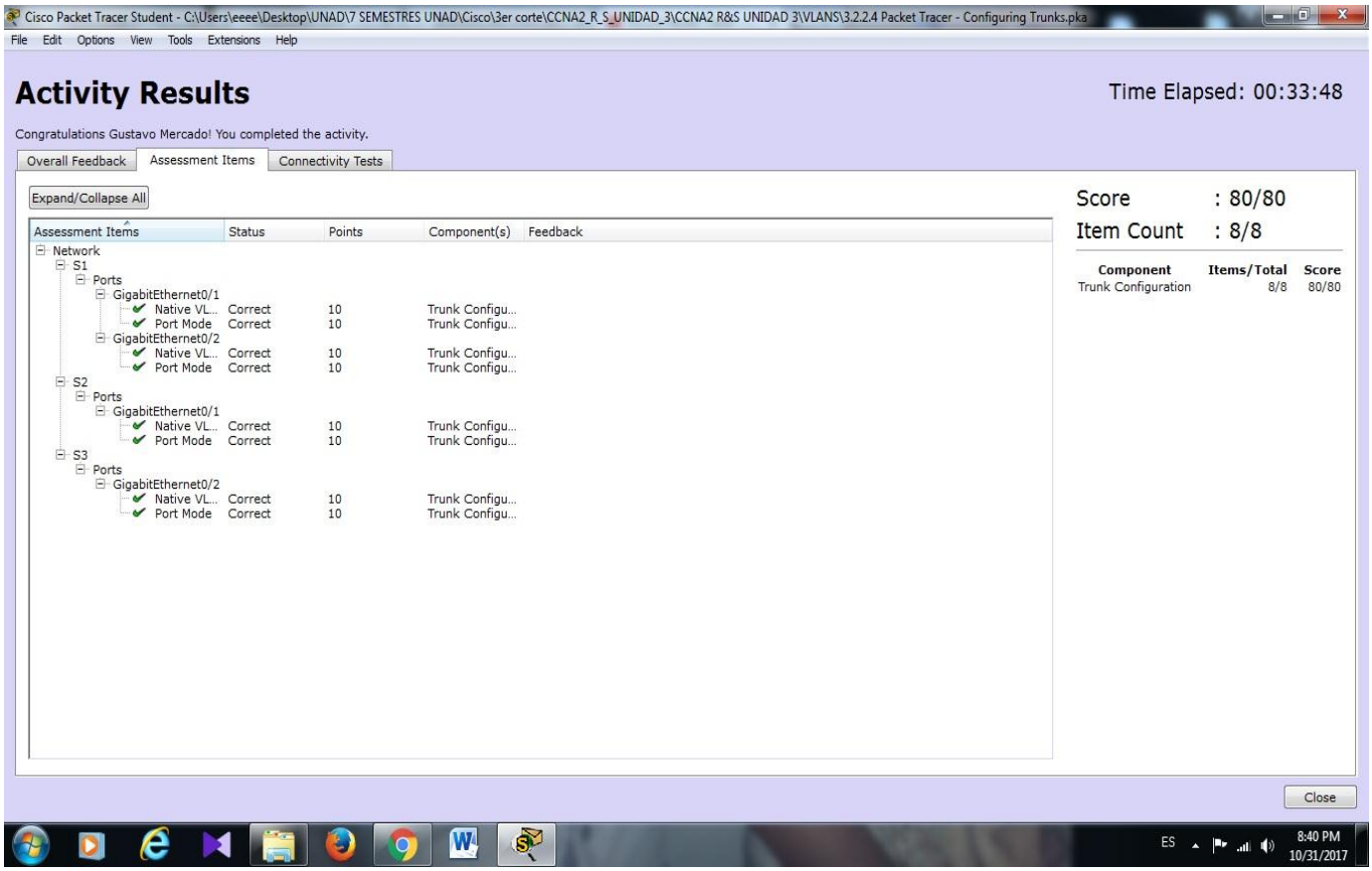
S3

```
S3>en
S3#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/2      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      1,10,20,30,99
S3#
```

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

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

a. Emita el comando show vlan para mostrar información acerca de las VLAN configuradas. ¿Por qué el puerto G0/1 en el S2 ya no está asignado a la VLAN 1?

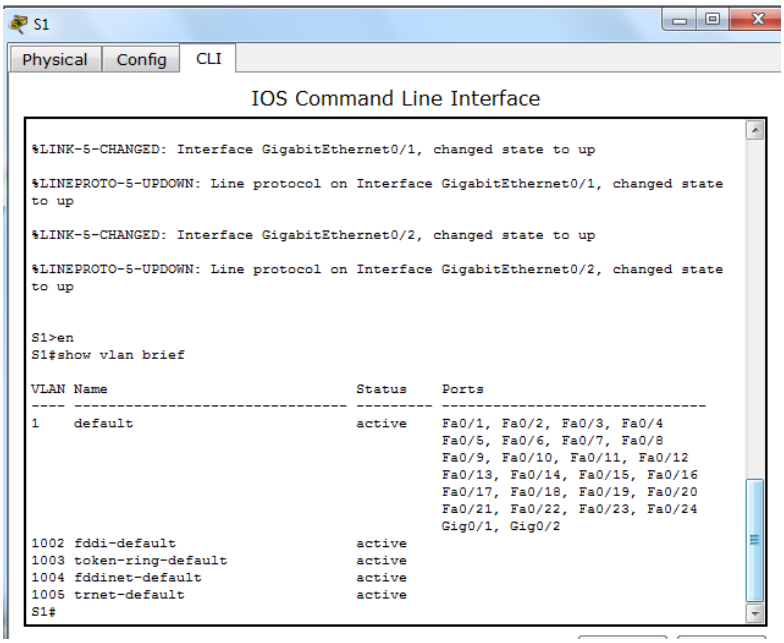


3.2.1.7 Packet Tracer - Configuring VLANs Instructions IG

Parte 1: Ver la configuración de VLAN predeterminada

Paso 1: muestra las VLAN actuales.

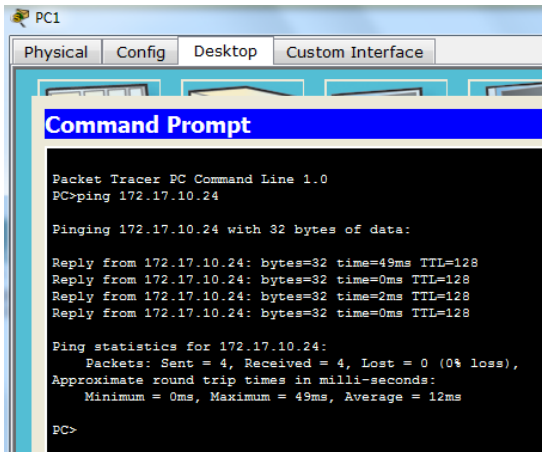
En S1, emita el comando que muestra todas las VLAN configuradas. Por defecto, todas las interfaces están asignadas a la VLAN 1.



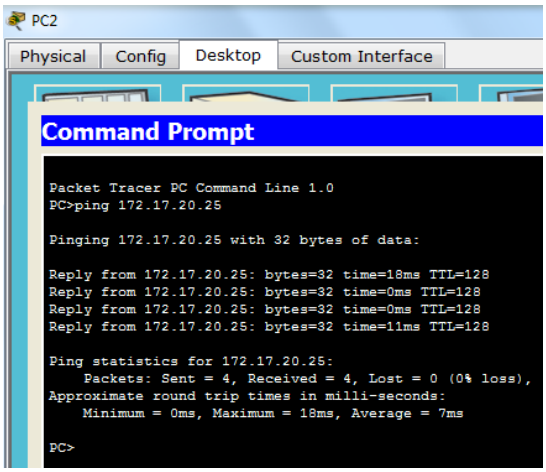
Paso 2: Verifique la conectividad entre las PC en la misma red.

Tenga en cuenta que cada PC puede hacer ping a la otra PC que comparte la misma red.

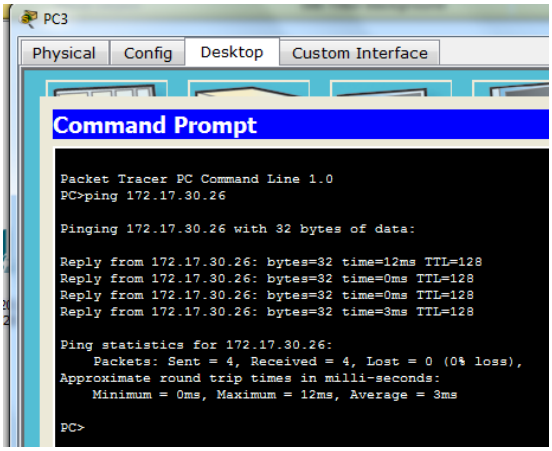
· PC1 puede hacer ping a PC4



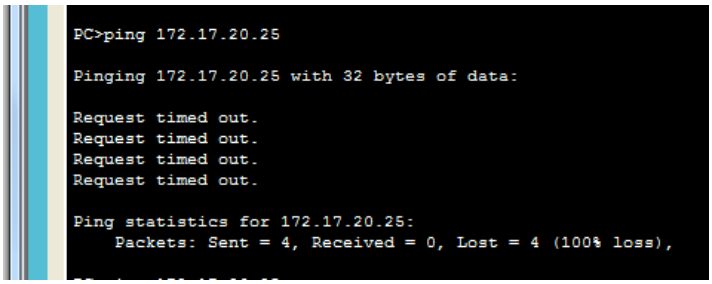
· PC2 puede hacer ping a PC5



· PC3 puede hacer ping a PC6



- Pings a PC en otras redes fallan.



¿Qué beneficio proporcionará la configuración de las VLAN a la configuración actual? **Los principales beneficios del uso de VLAN son los siguientes: seguridad, reducción de costos, mayor rendimiento, mitigación de tormentas de difusión, mejor eficiencia del personal de TI y administración más simple de proyectos y aplicaciones. Prevenir que exista mucho tráfico de broadcast**

Parte 2: Configurar VLAN

Paso 1: crea y nombra VLAN en S1.

Crea las siguientes VLAN. Los nombres distinguen mayúsculas y minúsculas:

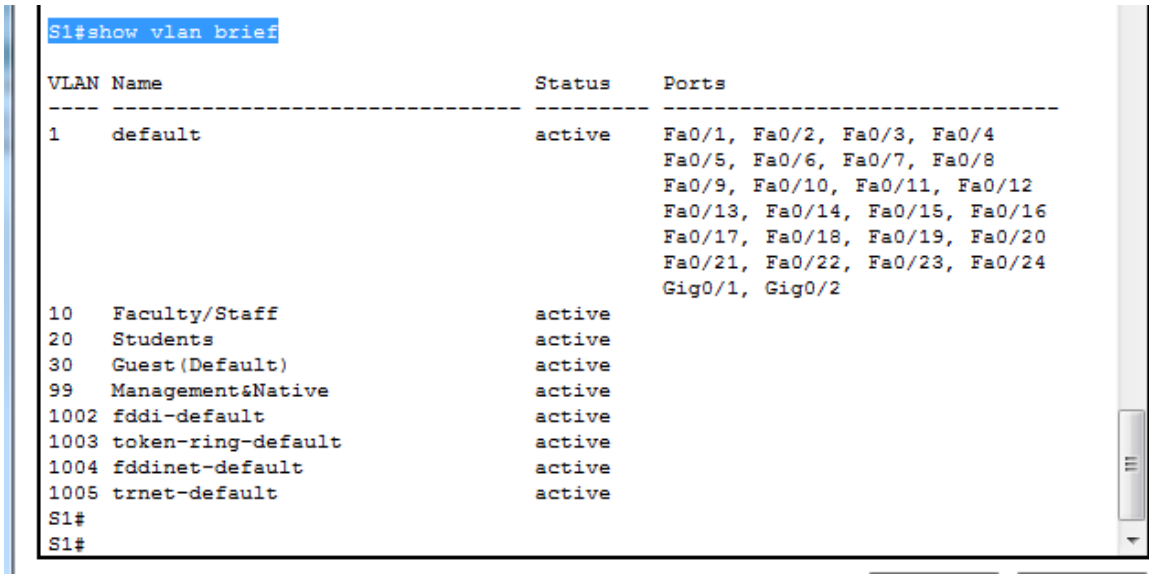
- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native

```
S1>en
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#Students
                ^
% Invalid input detected at '^' marker.

S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Paso 2: Verifica la configuración de la VLAN.

¿Qué comando solo mostrará el nombre, el estado y los puertos asociados de la VLAN en un conmutador?

S1#show vlan brief



```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
S1#
```

Paso 3: Crea las VLAN en S2 y S3.

Usando los mismos comandos del Paso 1, cree y nombre las mismas VLAN en S2 y S3.

Paso 4: Verifica la configuración de la VLAN.

VLANs PARA EL S2:

```
S2>en
S2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Faculty/Staff
S2(config-vlan)#vlan 20
S2(config-vlan)#name Students
S2(config-vlan)#vlan 30
S2(config-vlan)#name Guest(Default)
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Faculty/Staff                    active
20   Students                         active
30   Guest(Default)                   active
99   Management&Native                active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLANs PARA EL S3:

```
S3>en
S3#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#vlan 10
S3(config-vlan)#name Faculty/Staff
S3(config-vlan)#vlan 20
S3(config-vlan)#name Students
S3(config-vlan)#vlan 30
S3(config-vlan)#Guest(Default)
               ^
% Invalid input detected at '^' marker.

S3(config-vlan)#name Guest(Default)
S3(config-vlan)#vlan 99
S3(config-vlan)#name Management&Native
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

```
S3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Faculty/Staff                    active
20   Students                         active
30   Guest(Default)                   active
99   Management&Native                active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S3#
```

Parte 3: Asignar VLAN a puertos

Paso 1: Asigna VLAN a los puertos activos en S2.

Asignar las VLAN a los siguientes puertos:

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

```
S2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface f0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#interface f0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```

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

S3 usa las mismas asignaciones de puerto de acceso de VLAN que S2.

```
S3#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface f0/11
S3(config-if)#switchport access vlan 10
S3(config-if)#interface f0/18
S3(config-if)#switchport access vlan 20
S3(config-if)#interface f0/6
S3(config-if)#switchport access vlan 30
S3(config-if)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

Paso 3: Verificar la pérdida de conectividad.

Anteriormente, las PC que compartían la misma red podían hacer ping entre sí con éxito. Intente hacer ping entre PC1 y PC4. Aunque los puertos de acceso están asignados a las VLAN apropiadas, ¿fueron exitosos? ¿Por qué? **No, los pings fallaron porque los puertos entre los Switchs están en VLAN 1 y PC1 y PC4 están en VLAN 10.**

```
PC>ping 172.17.10.24

Pinging 172.17.10.24 with 32 bytes of data:

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

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

¿Qué se puede hacer para resolver este problema? Configurar los puertos entre los Switchs como puertos troncales (trunk port).

2.2.4.9 Packet Tracer - Configuring Switch Port Security

Parte 1: configurar la seguridad del puerto

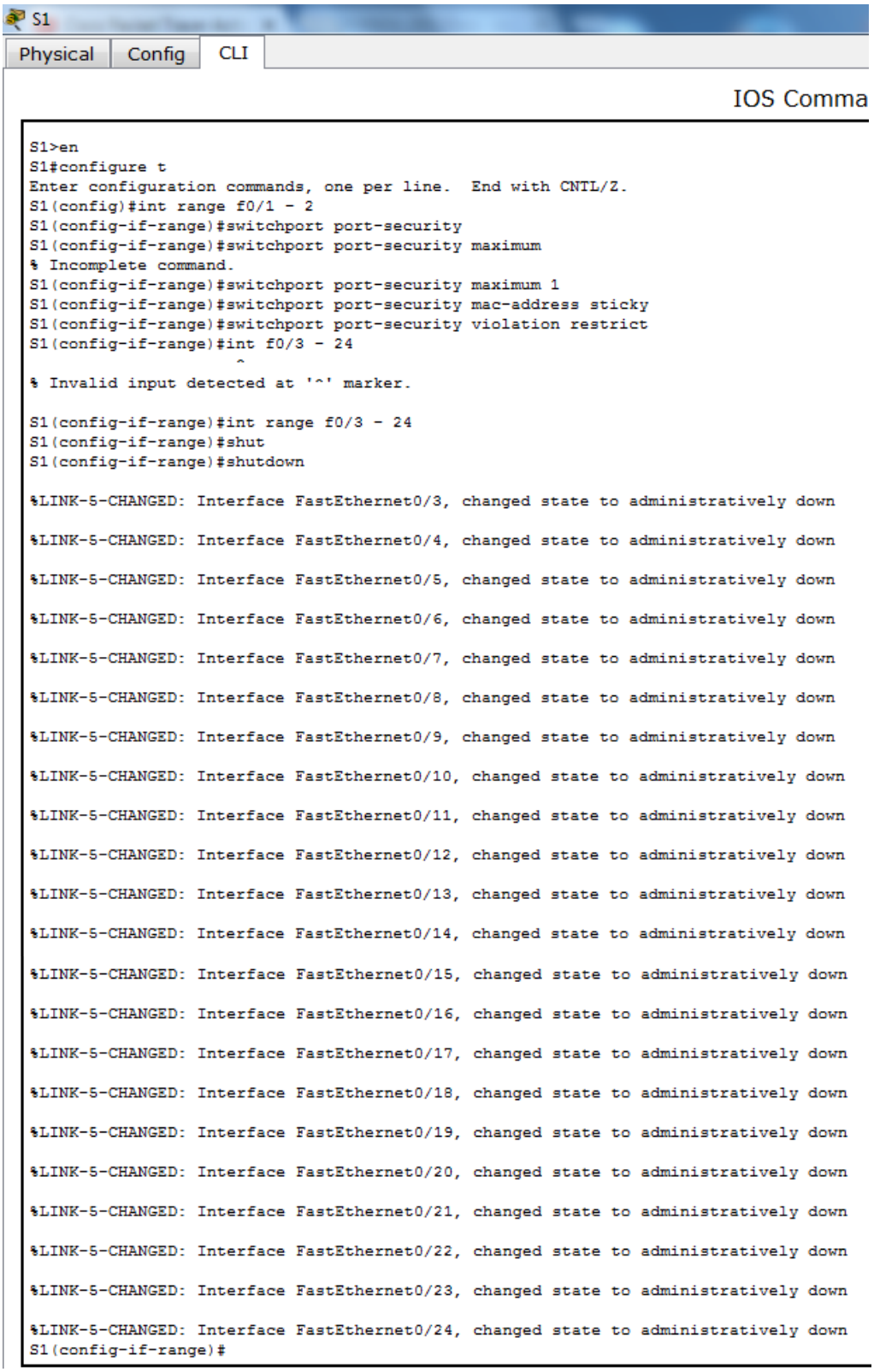
a. Acceda a la línea de comando para S1 y habilite la seguridad del puerto en los puertos Fast Ethernet 0/1 y 0/2.

b. Establezca el máximo para que solo un dispositivo pueda acceder a los puertos Fast Ethernet 0/1 y 0/2.

c. Asegure los puertos para que la dirección MAC de un dispositivo se aprenda dinámicamente y se agregue a la configuración en ejecución.

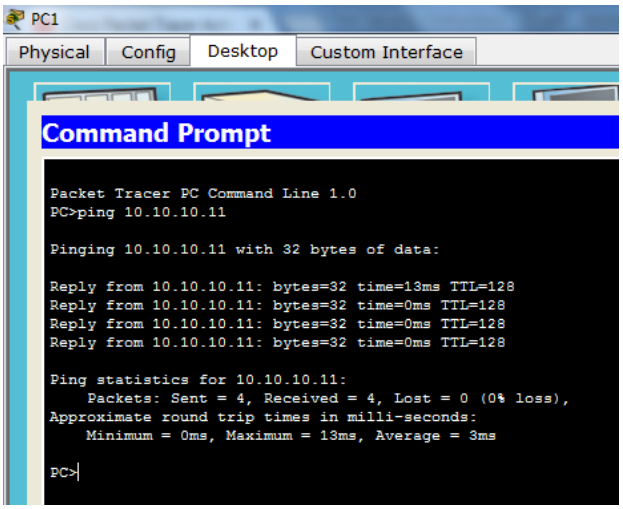
d. Establezca la infracción para que los puertos Fast Ethernet 0/1 y 0/2 no se deshabiliten cuando se produce una infracción, pero los paquetes se eliminan de una fuente desconocida.

e. Deshabilite todos los puertos restantes no utilizados. Sugerencia: utilice la palabra clave range para aplicar esta configuración a todos los puertos simultáneamente.


S1
Physical
Config
CLI
IOS Comma
S1>en
S1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range f0/1 - 2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum
% Incomplete command.
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
S1(config-if-range)#int f0/3 - 24
^
% Invalid input detected at '^' marker.
S1(config-if-range)#int range f0/3 - 24
S1(config-if-range)#shut
S1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#

Part 2: Verify Port Security

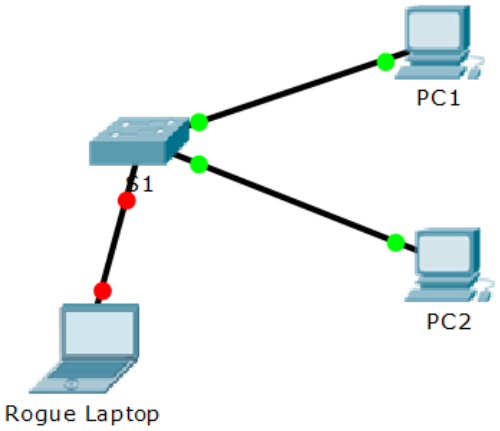
a. Hacer Ping desde el **PC1 a PC2**.



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

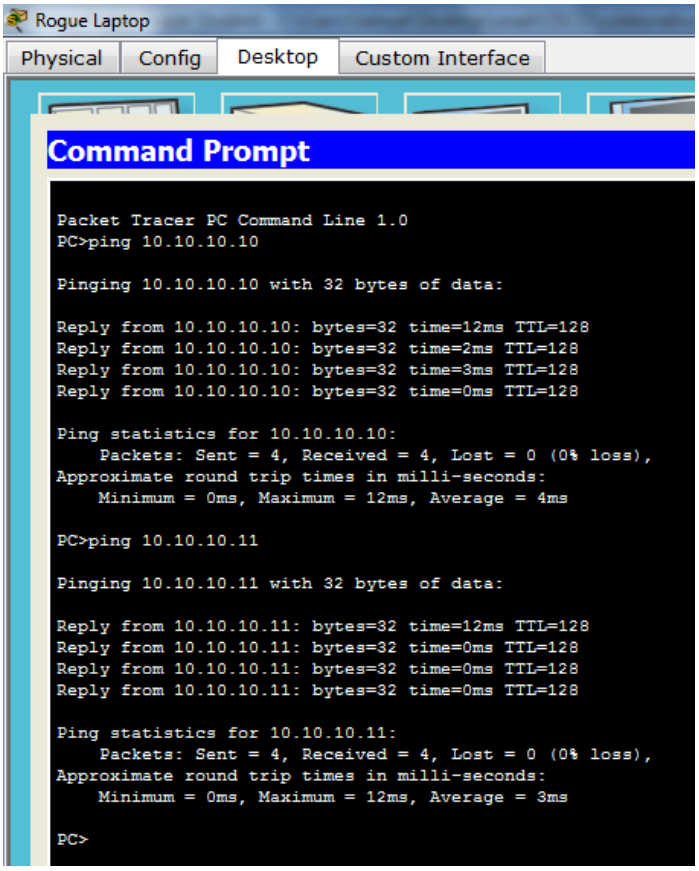
```
S1#show run
Building configuration...

Current configuration : 1675 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.B027.2245
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.647C.697E
!
```

c. Conecte la **Rogue Laptop** a cualquier puerto del **Switch** no utilizado y observe que las luces del enlace están en rojo.

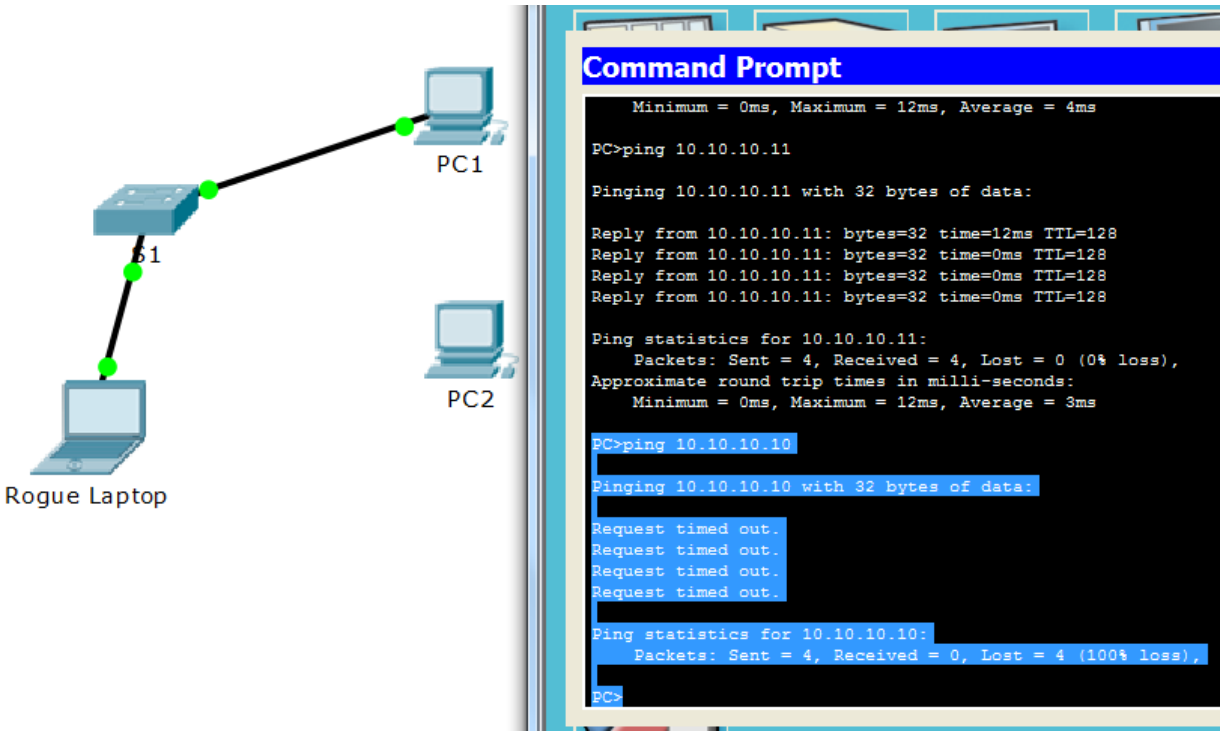


d. Habilite el puerto y verifique que **Rogue Laptop** pueda hacer **ping** a **PC1** y **PC2**. Después de la verificación, apague el puerto conectado a Rogue Laptop.

```
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#int f0/3
S1(config-if)#no sh
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

S1(config-if)#
```


Rogue Laptop
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=12ms TTL=128
Reply from 10.10.10.10: bytes=32 time=2ms TTL=128
Reply from 10.10.10.10: bytes=32 time=3ms TTL=128
Reply from 10.10.10.10: bytes=32 time=0ms TTL=128
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 4ms
PC>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=12ms TTL=128
Reply from 10.10.10.11: bytes=32 time=0ms TTL=128
Reply from 10.10.10.11: bytes=32 time=0ms TTL=128
Reply from 10.10.10.11: bytes=32 time=0ms TTL=128
Ping statistics for 10.10.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
PC>
```
```

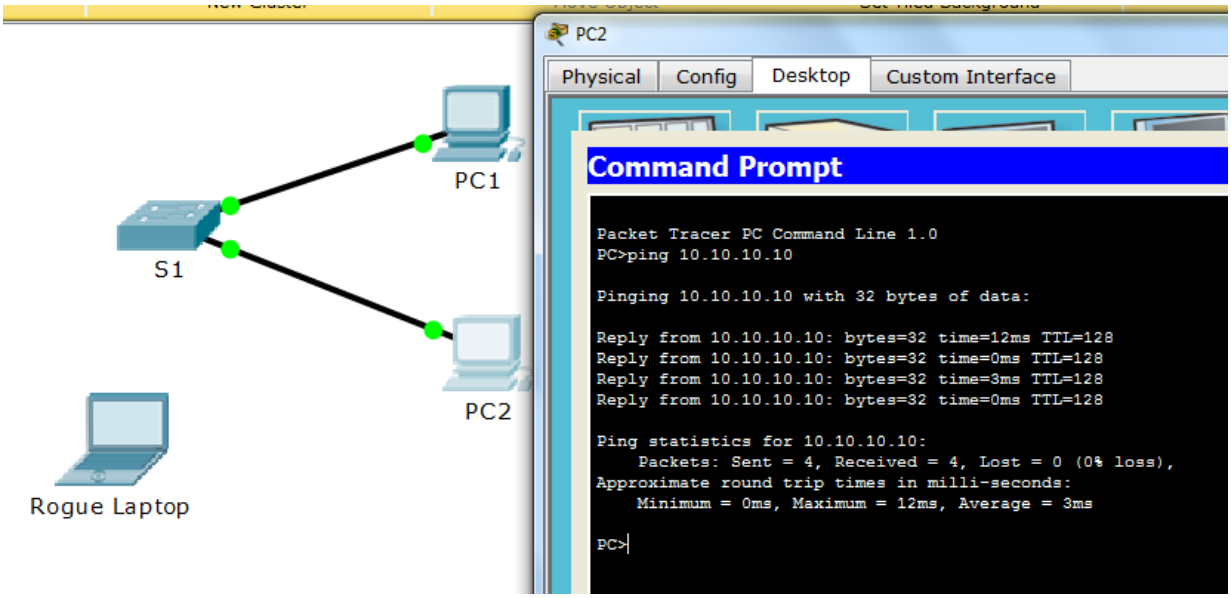
e. Desconecte **PC2** y conecte **Rogue Laptop** al puerto de **PC2**. Verificar que Rogue Laptop no pueda hacer **ping a PC1**.



Muestre las violaciones de seguridad del puerto para el puerto al que está conectado **Rogue Laptop**

```
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0002.4A42.C51C:1
Security Violation Count   : 4

S1#
```

f. Desconecte Rouge Laptop y vuelva a conectar la PC2. Verifique que PC2 pueda hacer ping a PC1.



g. ¿Por qué PC2 puede hacer ping a PC1, pero el Rouge Laptop no? **La seguridad del puerto que se habilitó solo permite que el dispositivo que fue configurado inicialmente acceda al puerto y evite el acceso de todos los demás dispositivos que no tengan la misma dirección MAC que el primer dispositivo configurado.**

CONCLUSIONES

Se han puesto en práctica los conocimientos adquiridos en el Diplomado de profundización Cisco usando la herramienta de simulación Cisco Packet Tracert en el desarrollo de cada una de las actividades propuestas donde se realizaron diferentes tipos de configuraciones a los distintos dispositivos que componen una red para luego realizar pruebas en donde se identificaban las causas del porque el sistema no estaba bien configurado o también se verificaba su correcto funcionamiento.

Adicional se realizaron ejercicios de configuración y habilitación de permisos como parte del aprendizaje para determinar un nivel de seguridad en la red, permitiendo o no el acceso de otros dispositivos a la red.

BIBLIOGRAFÍA

- **Guía de actividades y rúbrica de evaluación - Paso 5 - Actividad Colaborativa 3 – 203092.**
- **https://onedrive.live.com/?authkey=%21AMHKLfFEcuHljfg&cid=483D35BEE8610962&id=483D35BEE8610962%212954&parId=483D35BEE8610962%212952&action=locate**