Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN)

Configuración De Sistemas De Red Soportados En VLANs (Unidad 3)

Estudiantes:

Breeiner David Sierra Salgado

C.C: 1.103.113.587

Dair José Pérez Flórez

Álvaro Manuel Villamizar

Ángel Rafael Ruiz

Darío Javier Chávez

Grupo:

203092_6

Tutor:

Gerardo Granados Acuña

Universidad Nacional Abierta Y A Distancia Unad

Escuela De Ciencias Básicas Tecnología E Ingeniería "ECBTI"

Corozal – Sucre

2017

Introducción

Dentro del desarrollo de la temática tratada en la unidad 3 y en cada uno de sus capítulos se evidencian y tratan diferentes técnicas de las cuales permitirán garantizar la conexión en los diferentes escenarios que puedan presentarse en el ambiente real dentro de la plataforma de redes de datos, dentro de los ejercicios realizados se afianzan conocimientos sobre: Introducción a redes conmutadas, Configuración y conceptos básicos de Switching, VLANs, Conceptos de Routing, Enrutamiento entre VLANs, Enrutamiento Estático.

Desde los inicios de la civilización, los seres humanos han venido descubriendo diferentes alternativas de comunicación como elemento vital para su desarrollo y evolución, que le han permitido marchar en pro del descubrimiento de las cosas y la concepción del conocimiento para forjar su propio que hacer como individuos razonables y racionales en un mundo globalizado.

En tal caso, los descubrimientos alcanzados han forjado la capacidad del hombre para poner en práctica métodos y conocimientos convertidos en ciencias e ingeniería como la informática y las telecomunicaciones, con las cuales ha surgido todo el conocimiento que ha conllevado a descubrir grandes avances tecnológicos tanto en las comunicaciones, la informática y todos las ciencias afines, que contribuyen hoy por hoy, aportando técnicas para desarrollar toda la infraestructura física y lógica para establecer interconexión entre los seres humanos, los equipos, las organizaciones, los gobiernos, etc.

En este sentido, surge el concepto de red que es inherente la ciencia de las telecomunicaciones, donde se define a una red como, el conjunto de dispositivos conectados por enlaces de un medio físico y lógico. A estos dispositivos también se les denominan nodos que pueden ser computadoras, impresoras o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos que estén conectados a la red. Los dispositivos siempre estarán conectados a través de canales de comunicación, los cuales posibilitan el intercambio de información entre los sistemas conectados, gracias al desarrollo de estándares que se complementan con el desarrollo de hardware y software para el intercambio de información.

Sin embargo, esto no puede ser posible si no logramos entender primero la estructura lógica que debe tener una red, que no solo está compuesta de elementos físicos sino que también esta soportada por diferentes estándares lógicos los cuales incluyen una serie de protocolos que son indispensables y configurables en los equipos y la red para que pueda haber funcionamiento de la misma.

Los estándares desarrollados son gracias a entidades internacionales dedicadas especialmente a trabajar en unanimidad con los fabricantes de hardware y software para que todos sus componentes puedan ser integrados. Los estándares más conocidos es el del

modelo OSI, que funciona en 7 y el modelo TCP/IP, que funciona en 4 capas; donde cada una de ellas tiene una función específica para el control y comportamiento de la red.

Otro elemento fundamental es el direccionamiento IP, que a través de sus diferentes clases son capaces de jerarquizar la estructura de la organización donde se aplica; para ello los protocolos Pv4 y Pv6 tiene la capacidad para jerarquizar el direccionamiento IP para el comportamiento que deben tener los datos que se envían a través del transporte de paquetes.

En este sentido, el diseño, la implementación y la administración de un plan de direccionamiento IP, aportan valor relevante y eficaz para la operación segura y eficiente de la red. Como afirma John Chambers, "ni siquiera pensamos en toda la innovación detrás de nuestras conexiones, pero es alucinante cuando realmente nos damos cuenta de lo mucho que hay conectado y que ha revolucionado casi todas las facetas de la vida en las últimas dos décadas", refiriéndose a la capacidad que han alcanzado las redes en el desarrollo de transmisión de datos y la capacidad para conectar dispositivos.

El documento plasma de forma resumida el desarrollo de la práctica aplicable para la Unidad 3, del Curso de Profundización de Cisco, que requería el desarrollo de los diferentes laboratorios, donde se aplicaron conocimientos sobre Configuración de Sistemas de red soportados en VLANs

Desarrollo De Las Tareas Propuestas

2.1.1.6 Práctica De Laboratorio: Configuración De Los Parámetros Básicos De Un Switch

Topología

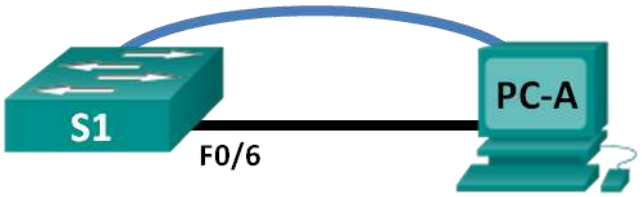


Tabla de direccionamiento

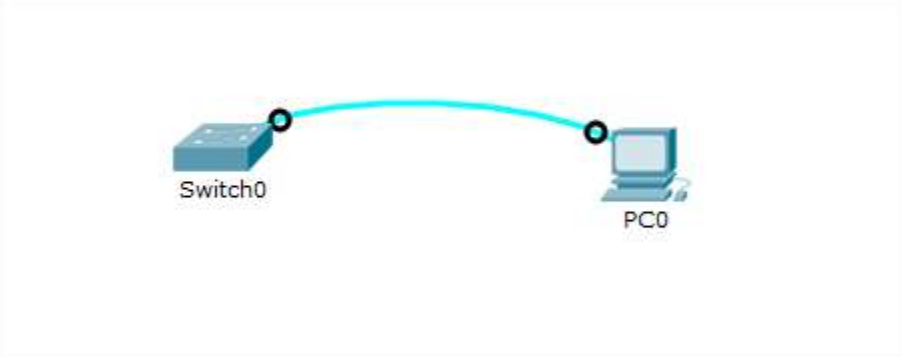
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Parte 1. 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.

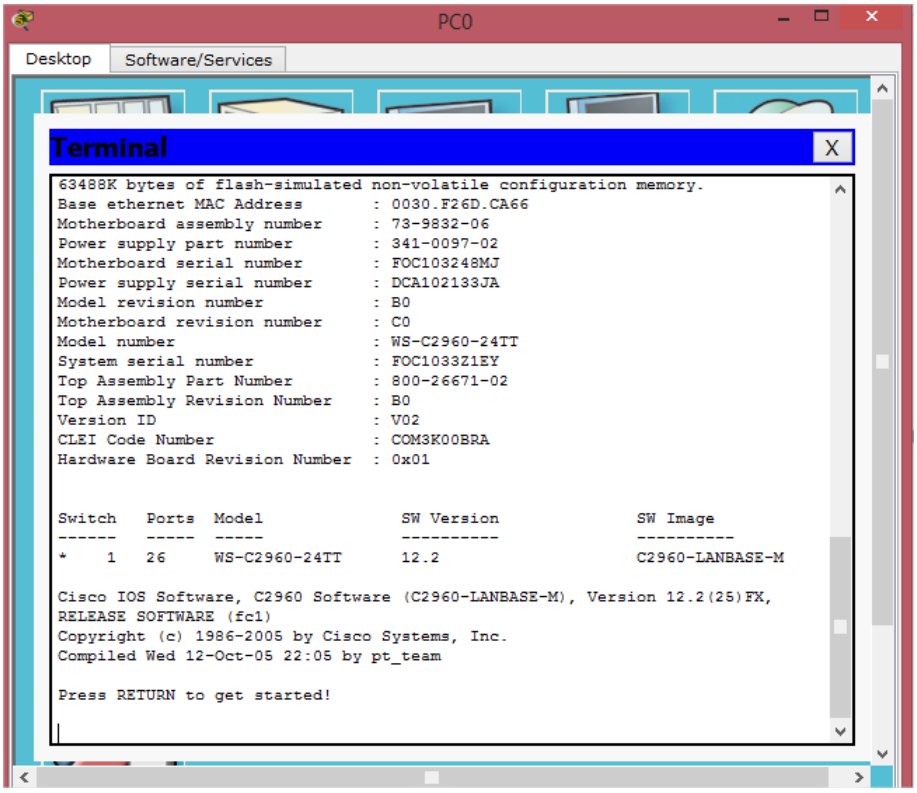
Paso 1. Realizar el cableado de red tal como se muestra en la topología.

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.



Nota: Si utiliza Netlab, puede desactivar F0/6 en el S1, lo que tiene el mismo efecto que no conectar la PC-A al S1.

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?

Porque ni el switch ni el pc tiene configuradas las direcciones ip.

Paso 2. Verificar la configuración predeterminada del switch.

En este paso, examinará la configuración predeterminada del switch, como la configuración actual del switch, la información de IOS, las propiedades de las interfaces, la información de la VLAN y la memoria flash.

Puede acceder a todos los comandos IOS del switch en el modo EXEC privilegiado. Se debe restringir el acceso al modo EXEC privilegiado con protección con contraseña para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento. Establecerá las contraseñas más adelante en esta práctica de laboratorio.

El conjunto de comandos del modo EXEC privilegiado incluye los comandos del modo EXEC del usuario y el comando **configure**, a través del cual se obtiene acceso a los modos de comando restantes. Use el comando **enable** para ingresar al modo EXEC privilegiado.

a) Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del usuario en el switch, con

la petición de entrada Switch>. Use el comando **enable** para ingresar al modo EXEC privilegiado.

Switch> **enable**

Switch#

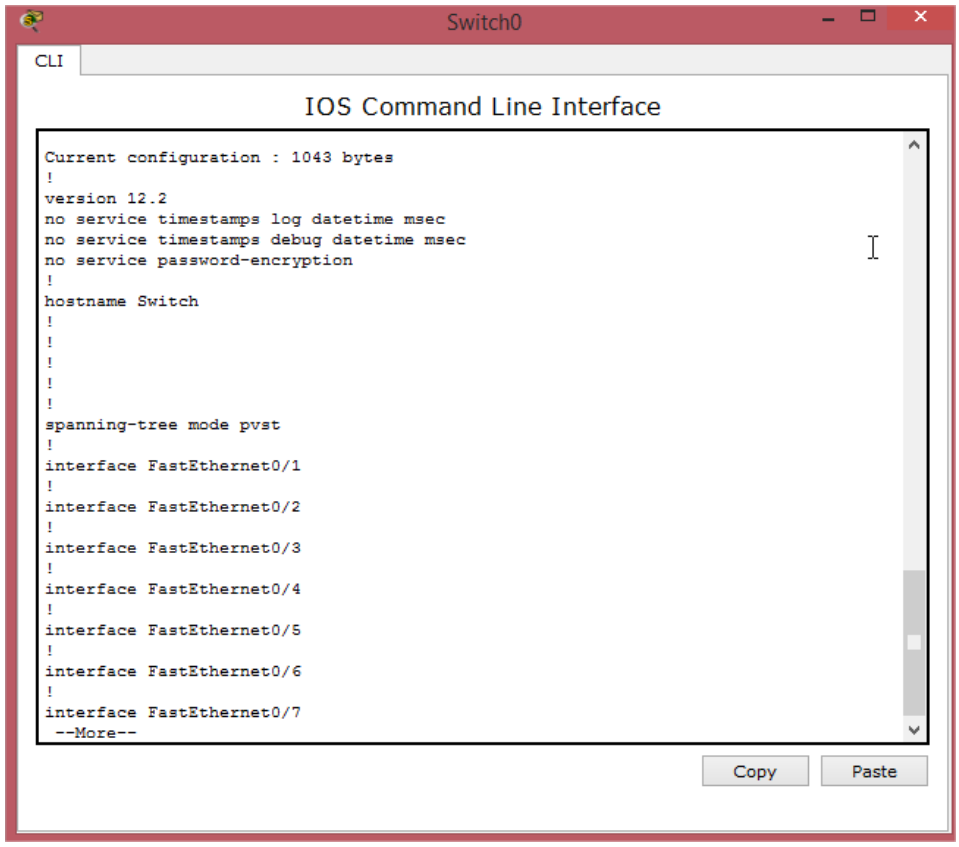
Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

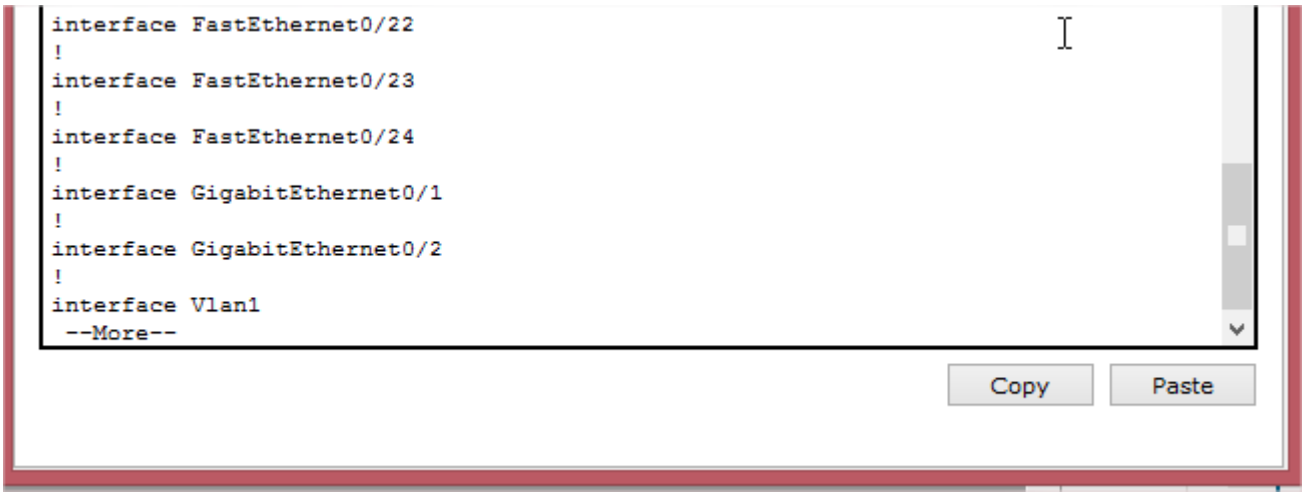
Verifique que el archivo de configuración esté limpio con el comando **show running-config** del modo EXEC privilegiado. Si se guardó un archivo de configuración anteriormente, se debe eliminar. Según cuál sea el modelo del switch y la versión del IOS, la configuración podría variar. Sin embargo, no debería haber contraseñas ni direcciones IP configuradas. Si su switch no tiene una configuración predeterminada, borre y recargue el switch.

Nota: en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

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? Vty 0 4

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? Porque no se ha hecho ni guardado ninguna configuración en la nvram

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

Switch# **show interface vlan1**

```
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0030.f26d.ca66 (bia 0030.f26d.ca66)
  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#
```

Copy Paste

¿Hay alguna dirección IP asignada a la VLAN 1? Aún no

¿Cuál es la dirección MAC de esta SVI? Las respuestas varían. 0001.974a.c013

¿Está activa esta interfaz? No está activa

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

Switch# **show ip interface vlan1**

¿Qué resultado ve?

```
Switch#
Switch#show ip interface vlan1
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
Switch#
```

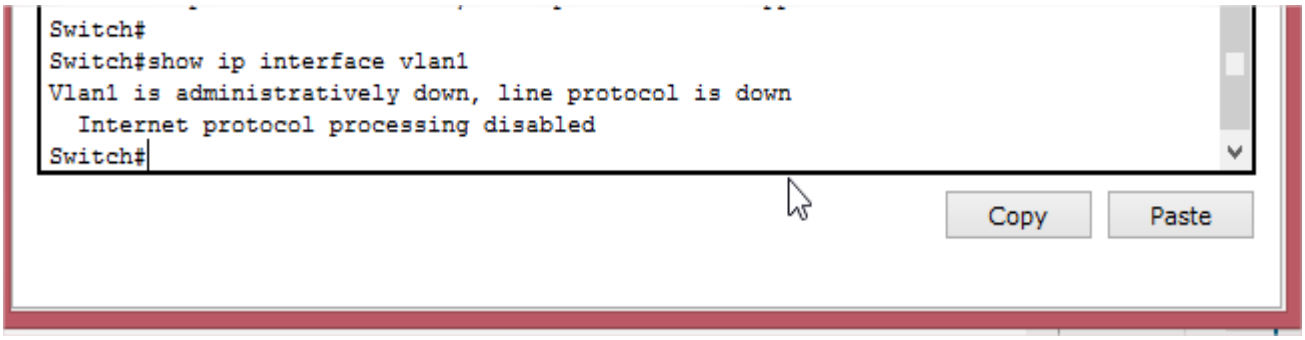
Copy Paste

f) Conecte el cable Ethernet de la PC-A al puerto 6 en el switch y examine las propiedades IP de la VLAN 1 SVI. Aguarde un momento para que el switch y la computadora negocien los parámetros de dúplex y velocidad.

Nota: Si utiliza Netlab, habilite la interfaz F0/6 en el S1.

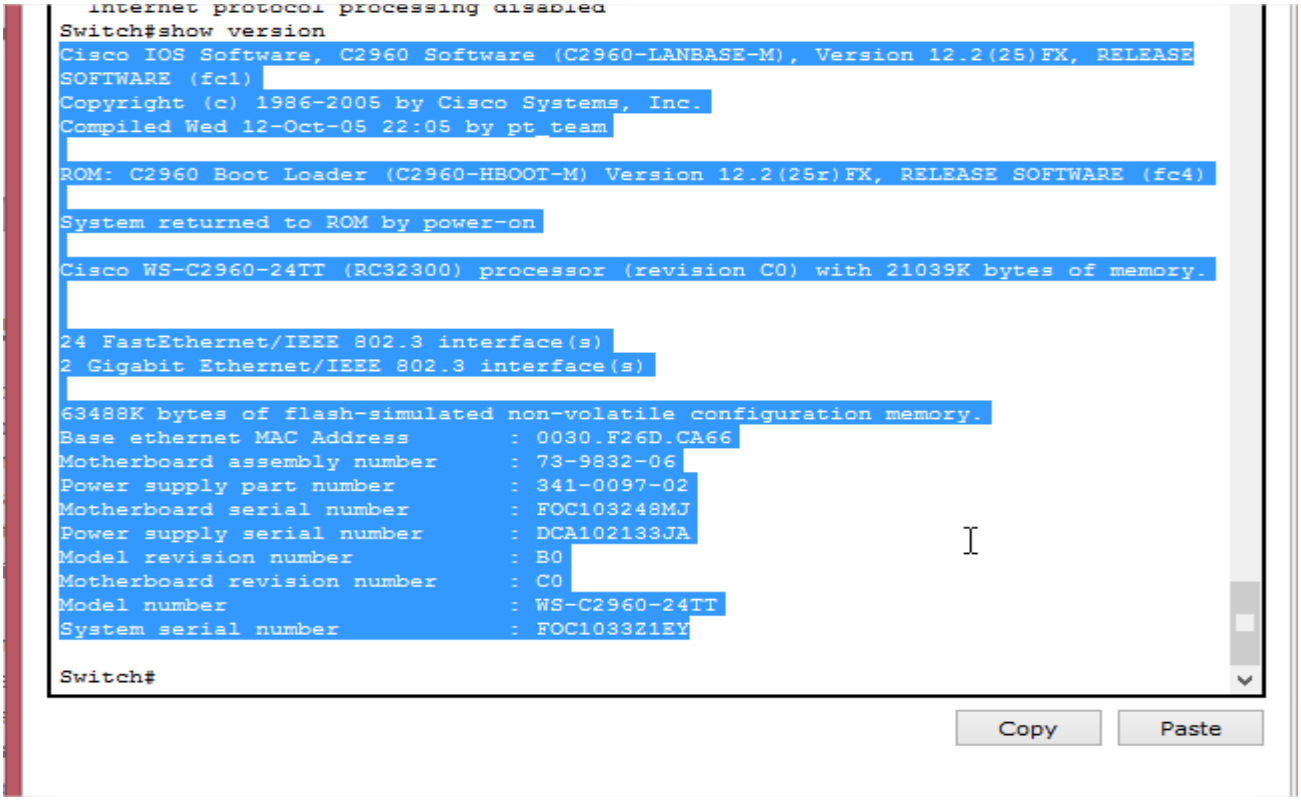
Switch# **show ip interface vlan1**

¿Qué resultado ve?



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

Switch# **show versión**



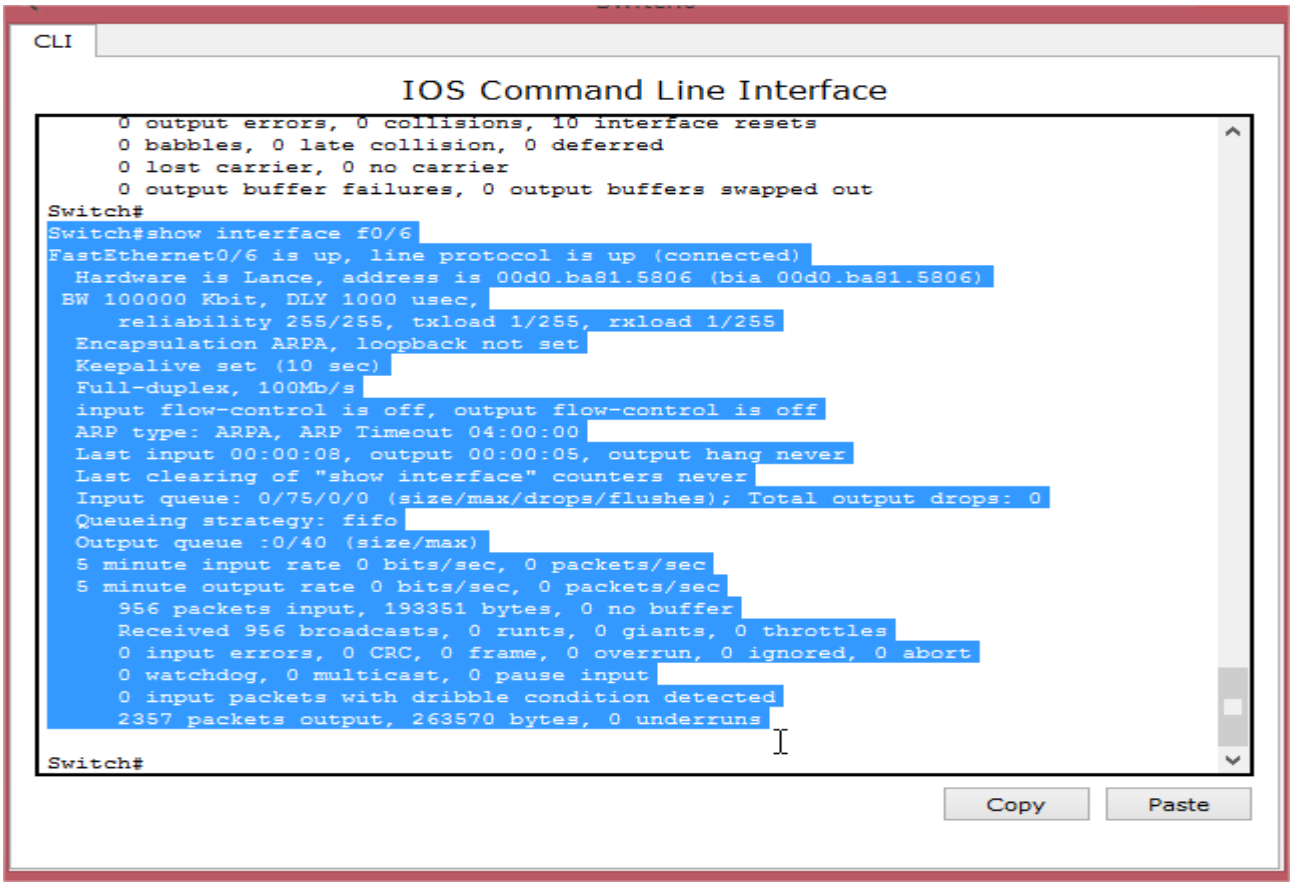
¿Cuál es la versión del IOS de Cisco que está ejecutando el switch? Versión 12.2 (25r) FX

¿Cuál es el nombre del archivo de imagen del sistema? C2960 Boot Loader (C2960-HBOOT-M)

¿Cuál es la dirección MAC base de este switch? Las respuestas varían. 0030.F26D.CA66

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

Switch# **show interface f0/6**



¿La interfaz está activa o desactivada? Activa

¿Qué haría que una interfaz se active? La conexión física del cable

¿Cuál es la dirección MAC de la interfaz? 00d0.ba81.5806

¿Cuál es la configuración de velocidad y de dúplex de la interfaz? 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
```

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

¿Qué puertos hay en esta VLAN? 26

¿La VLAN 1 está activa? Active

¿Qué tipo de VLAN es la VLAN predeterminada? 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:**

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

Los archivos poseen una extensión, tal como .bin, al final del nombre del archivo. Los directorios no tienen una extensión de archivo.

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

Parte2. Configurar los parámetros básicos de los dispositivos de red

En la parte 2, configurará los parámetros básicos para el switch y la computadora.

Paso 3. 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.

En este paso, configurará la computadora y los parámetros básicos del switch, como el nombre de host y la dirección IP para la SVI de administración del switch. La asignación de una dirección IP en el switch es solo el primer paso. Como administrador de red, debe especificar cómo se administra el switch. Telnet y SSH son los dos métodos de administración que más se usan. No obstante, Telnet no es un protocolo seguro. Toda la información que fluye entre los dos dispositivos se envía como texto no cifrado. Las contraseñas y otra información confidencial pueden ser fáciles de ver si se las captura mediante un programa detector de paquetes.

a. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la NVRAM, verifique que usted esté en el modo EXEC privilegiado. Introduzca el comando **enable** si la petición de entrada volvió a cambiar a Switch>.

Switch> **enable**
Switch#

b. Ingrese al modo de configuración global.

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

La petición de entrada volvió a cambiar para reflejar el modo de configuración global.

c. Asigne el nombre de host del switch.

Switch (config) # **hostname S1**
S1 (config) #

d. Configurar la encriptación de contraseñas.

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

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

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

f. Evite las búsquedas de DNS no deseadas.

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

g. Configure un mensaje MOTD.

S1 (config) # **banner motd #**

Enter Text message. End with the character '#'.

Unauthorized access is strictly prohibited. #

h. 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? _____

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

S1> **enable**

Password:

S1#

Nota: Cuando se introduce la contraseña, esta no se muestra.

```
S1>configure terminal
              ^
% Invalid input detected at '^' marker.

S1>
S1>enable
Password:
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

j. Ingrese al modo de configuración global para establecer la dirección IP de la SVI del switch. Esto permite la administración remota del switch.

Antes de poder administrar el S1 en forma remota desde la PC-A, debe asignar una dirección IP al switch. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica

recomendada para la configuración básica del switch es cambiar la VLAN de administración a otra VLAN distinta de la VLAN 1.

Con fines de administración, utilice la VLAN 99. La selección de la VLAN 99 es arbitraria y de ninguna manera implica que siempre deba usar la VLAN 99.

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.

S1# **configure terminal**

S1 (config) # **vlan 99**

S1 (config-vlan) # **exit**

S1 (config) # **interface vlan99**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

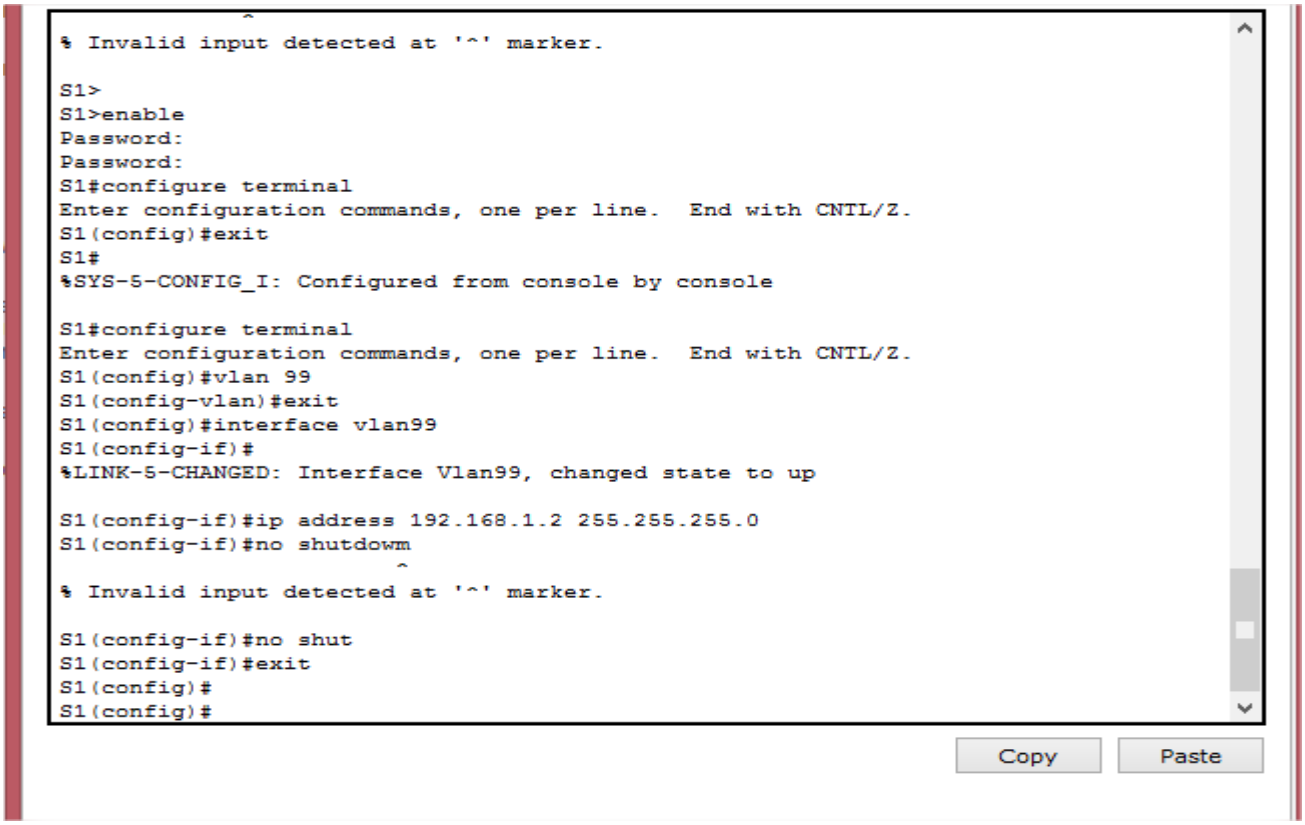
S1 (config-if) # **ip address 192.168.1.2 255.255.255.0**

S1 (config-if) # **no shutdown**

S1 (config-if) # **exit**

S1 (config) #

Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando **no shutdown**. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del switch a la VLAN 99.



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

S1 (config) # **interface range f0/1 – 24,g0/1 - 2**

S1 (config-if-range) # **switchport access vlan 99**

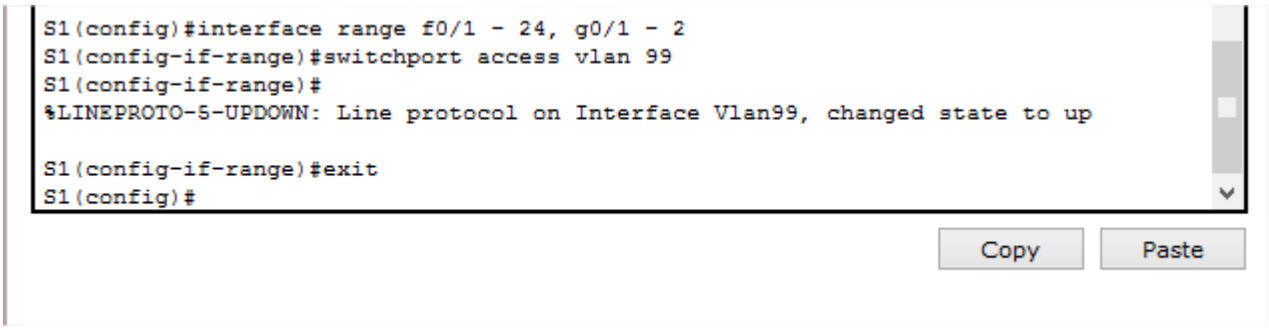
S1 (config-if-range) # **exit**

S1 (config) #

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Para establecer la conectividad entre el host y el switch, los puertos que usa el host deben estar en la misma VLAN que el switch. Observe que, en el resultado de arriba, la interfaz VLAN 1 queda en estado down porque no se asignó ninguno de los puertos a la VLAN 1. Después de unos segundos, la VLAN 99 pasa al estado up porque ahora se le asigna al menos un puerto activo (F0/6 con la PC-A conectada).



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

S1# **show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active

99 VLAN0099 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
Gi0/1, Gi0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

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

S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
99   VLAN0099                          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                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

m. 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.

S1 (config) # **ip default-gateway 192.168.1.1**

S1 (config) #

n. 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**.

S1 (config) # **line con 0**

S1 (config-line) # **password cisco**

S1 (config-line) # **login**

S1 (config-line) # **logging synchronous**

S1 (config-line) # **exit**

S1 (config) #

o. 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.

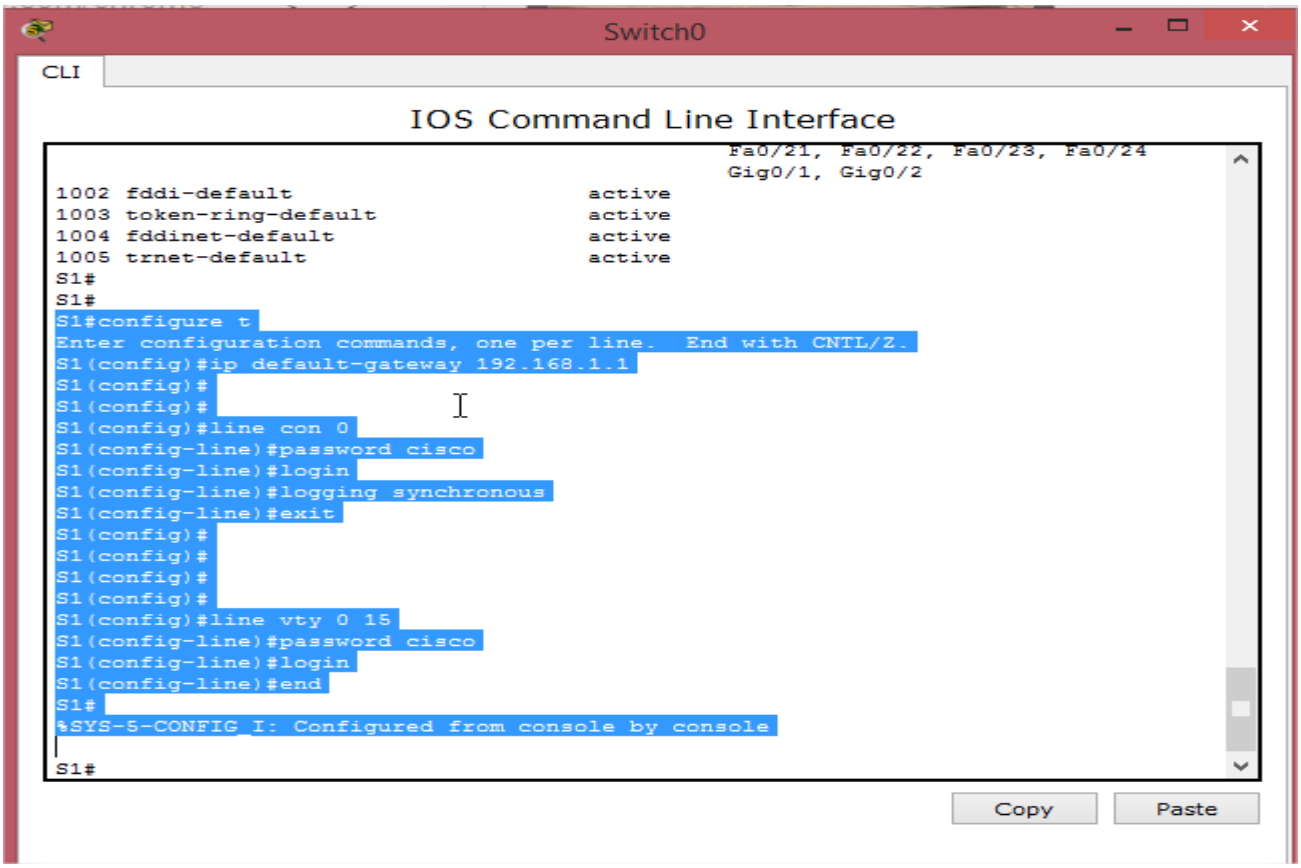
S1 (config) # **line vty 0 15**

S1 (config-line) # **password cisco**

S1 (config-line) # **login**

S1 (config-line) # **end**

S1#
*Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console



¿Por qué se requiere el comando **login**? Sin este "login" el switch no solicitara el Password

---

Paso 4. 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**.

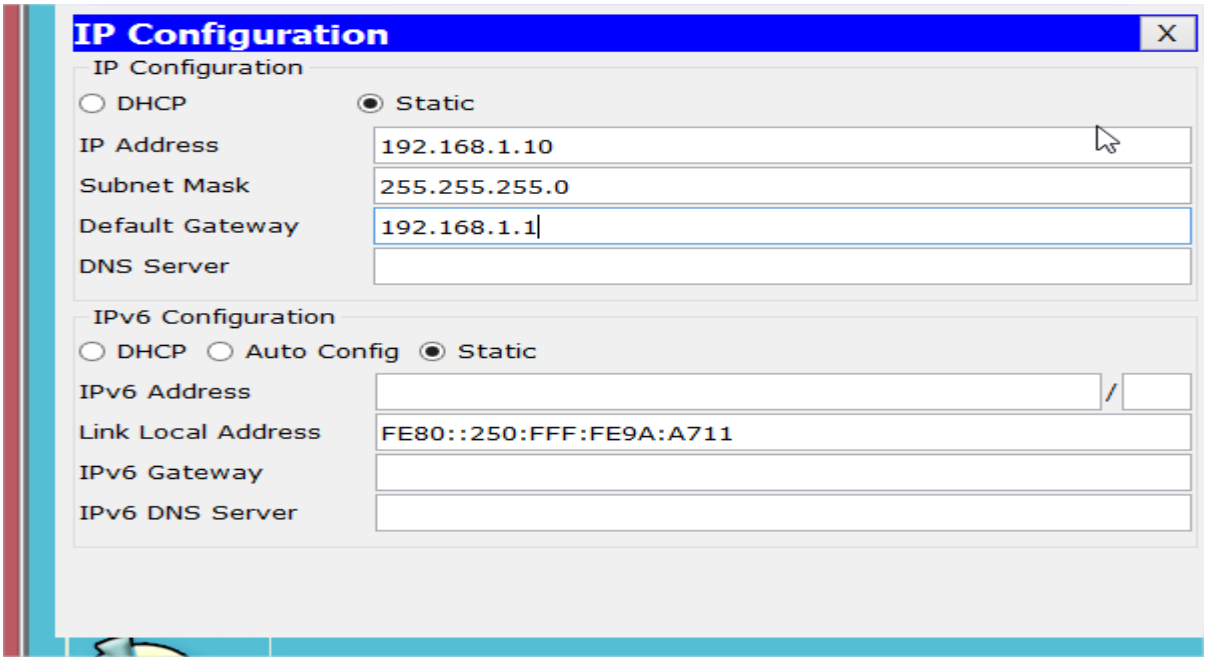
2) Haga clic en **Ver por:** y elija **Íconos pequeños**.

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 2. 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.

Paso 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.

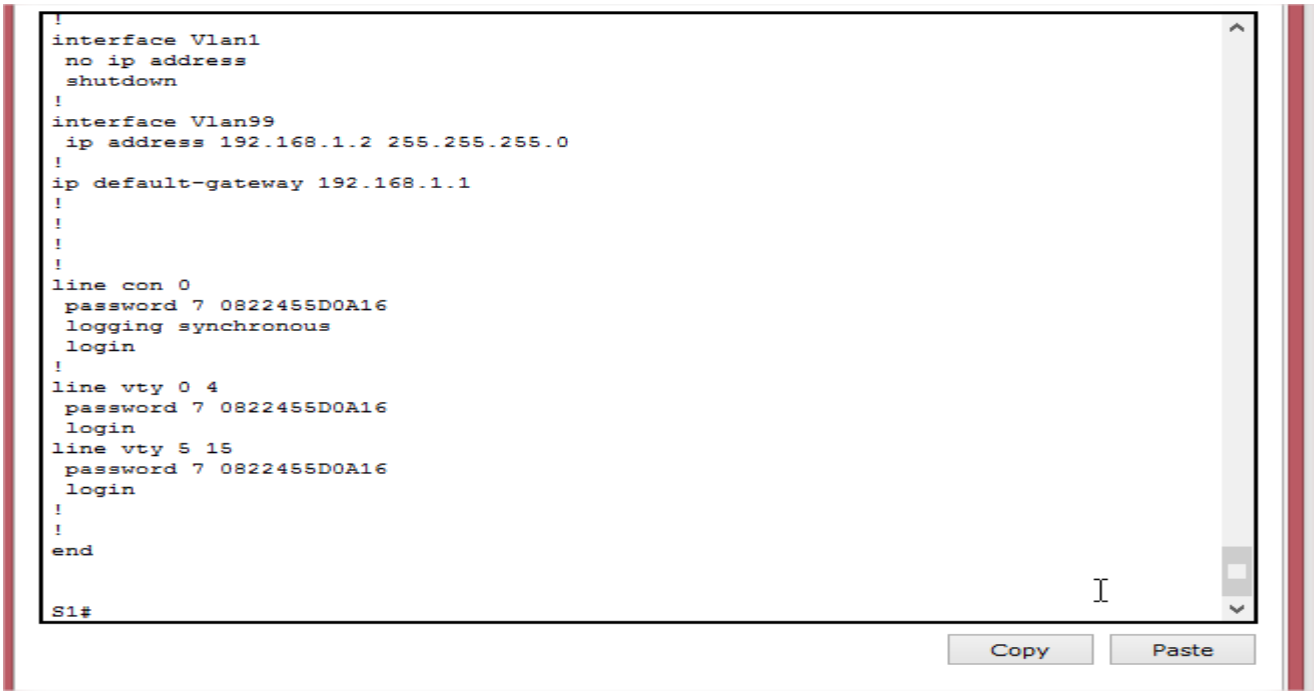
S1# **show run**
Building configuration...

Current configuration : 2206 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

```
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<Output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
```

line con 0
 password 7 104D000A0618
 logging synchronous
 login
line vty 0 4
 password 7 14141B180F0B
 login
line vty 5 15
 password 7 14141B180F0B
 login
!
end

S1#

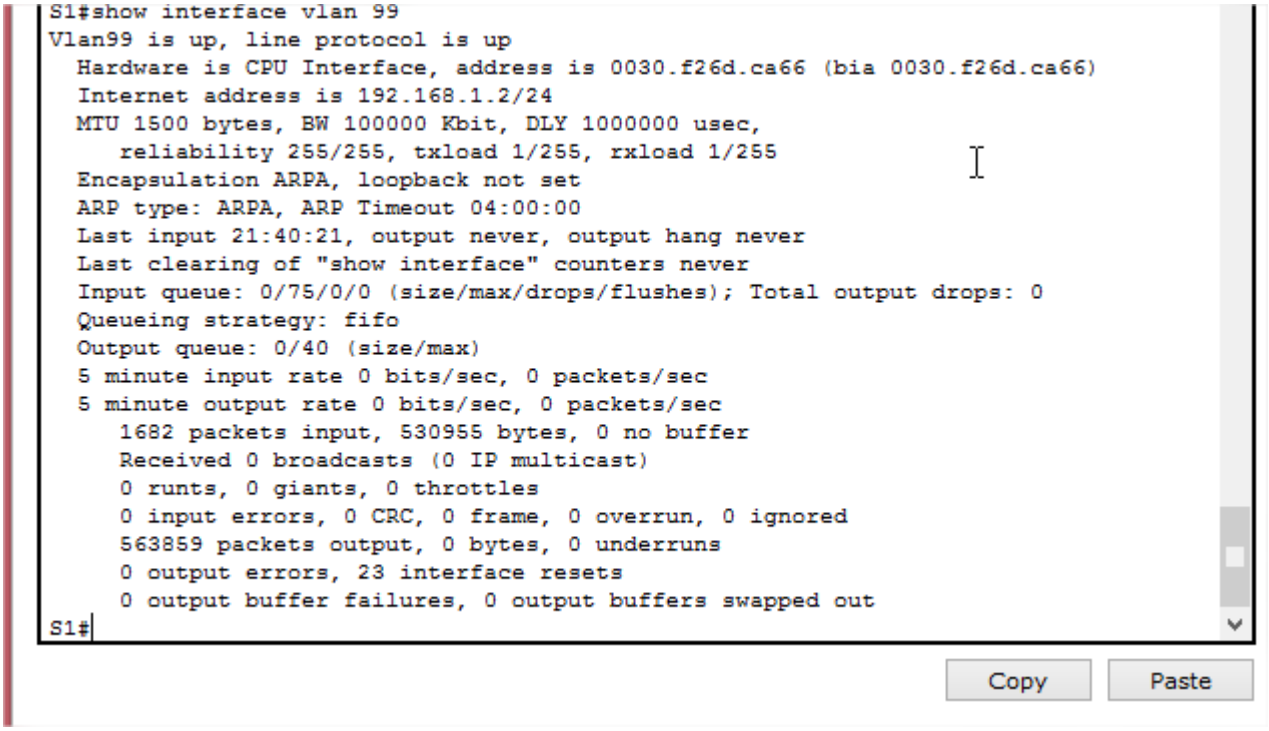


b. Verifique la configuración de la VLAN 99 de administración.

S1# **show interface vlan 99**

Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 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 00:00:06, output 00:08:45, 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
175 packets input, 22989 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
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 interface resets
0 output buffer failures, 0 output buffers swapped out



¿Cuál es el ancho de banda en esta interfaz? 100 mbps

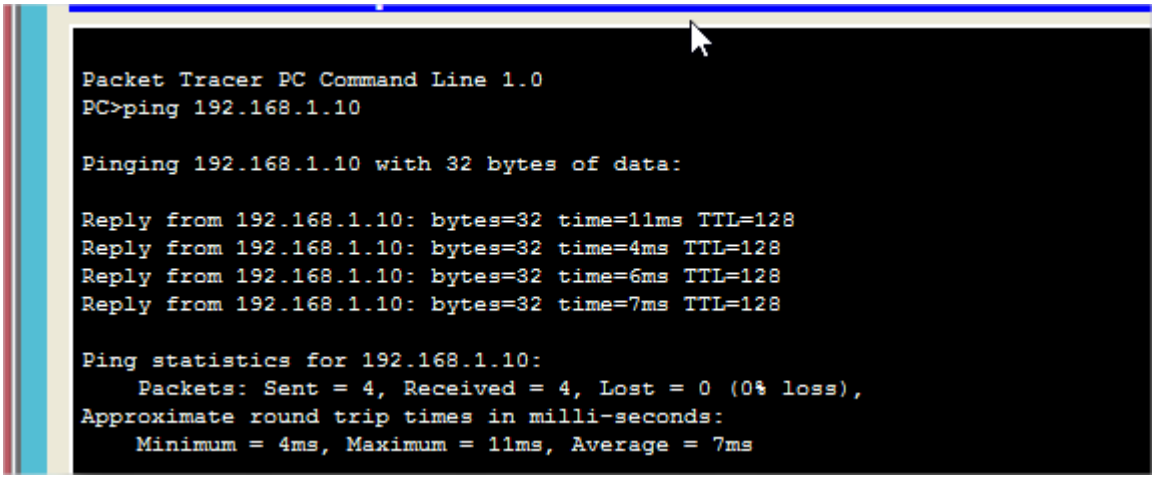
¿Cuál es el estado de la VLAN 99? Up – active

¿Cuál es el estado del protocolo de línea? Up – active.

Paso 2. Probar la conectividad de extremo a extremo con ping.

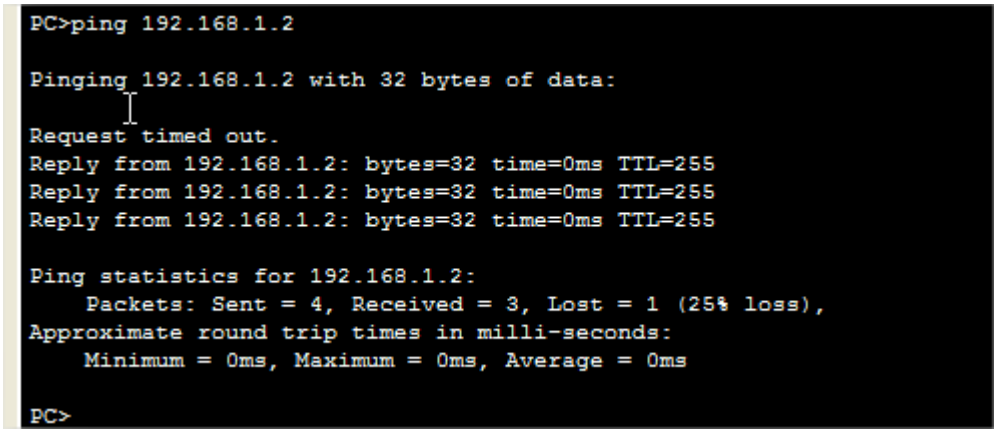
a. En el símbolo del sistema de la PC-A, haga ping a la dirección de la propia PC-A primero.

C:\Users\User1> **ping 192.168.1.10**



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

C:\Users\User1> **ping 192.168.1.2**



Debido a que la PC-A debe resolver la dirección MAC del S1 mediante ARP, es posible que se agote el tiempo de espera del primer paquete. Si los resultados del ping siguen siendo incorrectos, resuelva los problemas de configuración de los parámetros básicos del dispositivo. Revise el cableado físico y el direccionamiento lógico, si es necesario.

Paso 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.

Nota: si utiliza Windows 7, es posible que el administrador deba habilitar el protocolo Telnet. Para instalar el cliente de Telnet, abra una ventana cmd y escriba **pkgmgr /iu:"TelnetClient"**. A continuación, se muestra un ejemplo.

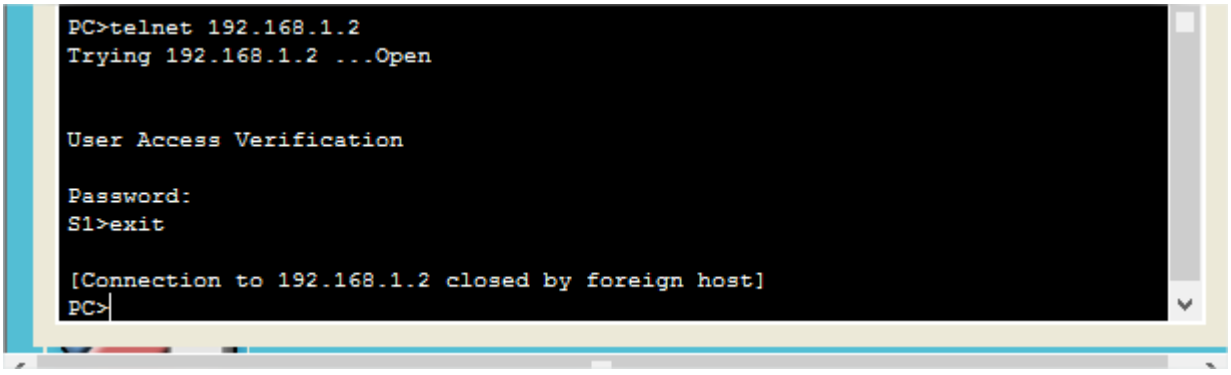
C:\Users\User1> **pkgmgr /iu:"TelnetClient"**

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**.

C:\Users\User1> **telnet 192.168.1.2**

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

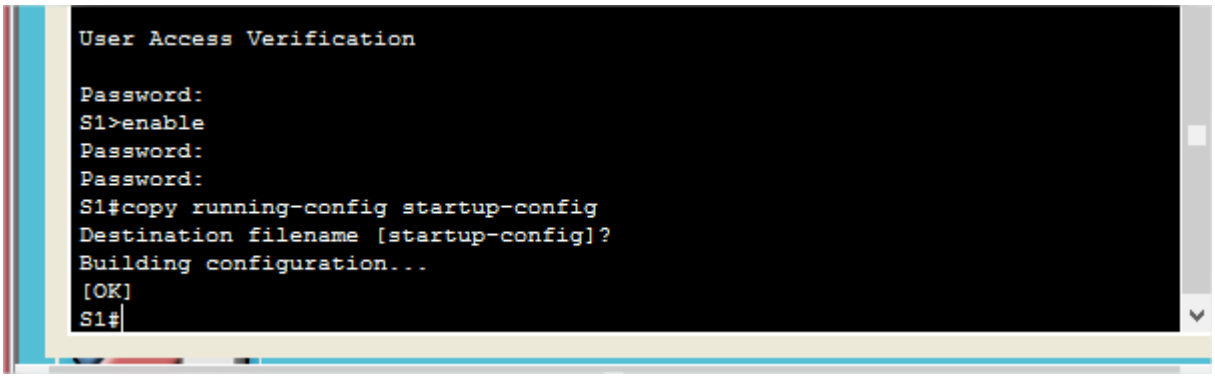
c. Escriba **exit** para finalizar la sesión de Telnet.



Paso 4. Guardar el archivo de configuración en ejecución del switch.

Guarde la configuración.

S1# **copy running-config startup-config**
Destination filename [startup-config]? **[Enter]**
Building configuration...
[OK]
S1#

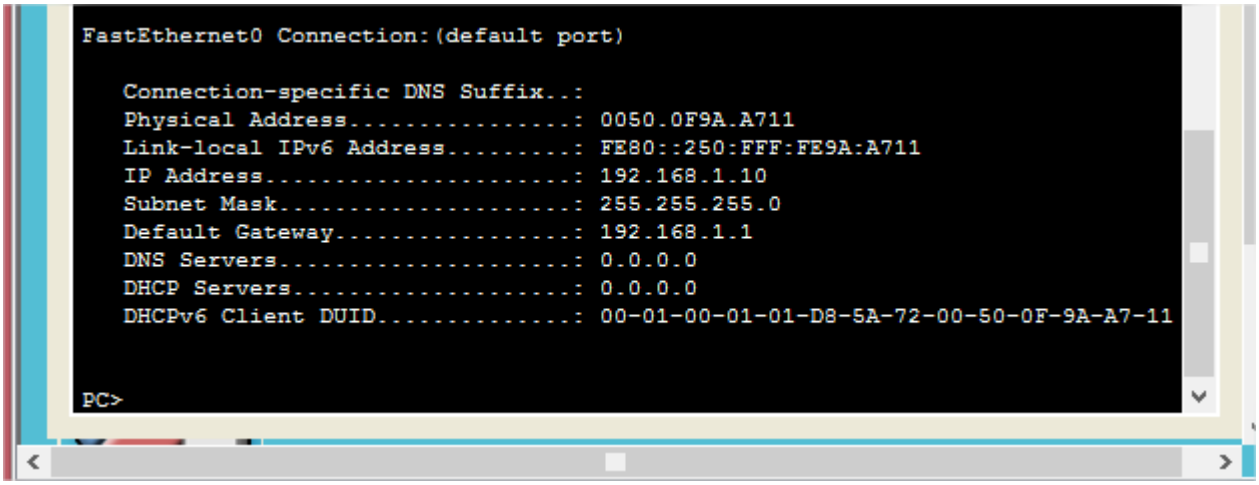


Parte 3. Administrar la tabla de direcciones MAC

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.

Paso 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.



_____

_____

Paso 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**

```
User Access Verification

Password:

S1>enable
Password:
S1#show mac address-table
          Mac Address Table
-------------------------------------------

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

  99    0050.0f9a.a711    DYNAMIC     Fa0/6
S1#
```

Copy Paste

¿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 coincide.

Paso 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
          Mac Address Table
-------------------------------------------

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

S1#
```

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

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>**

Paso 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 mac address-table
S1#
```

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

S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay? 0

¿Cuántas direcciones dinámicas hay? 0

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**

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

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

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

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

S1#
```

¿Cuántas direcciones dinámicas hay? No hay.

¿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**.

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. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe usar la dirección MAC de su PC-A, que es distinta de la del ejemplo.

S1(config)# **mac address-table static 0050.0f9a.a711 vlan 99 interface fastethernet 0/6**

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

```
S1#sow mac address-table
       ^
% Invalid input detected at '^' marker.

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

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

  99    0050.0f9a.a711    STATIC      Fa0/6
S1#
```

S1# **show mac address-table**

¿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.

Nota: la dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC-A.

S1(config)# **no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

g. Verifique que la dirección MAC estática se haya borrado.

S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay en total?0

```
S1(config)#no mac address-table static 0050.0f9a.a711 vlan 99 interface
fastethernet 0/6
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

S1#
```

Copy Paste

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch? Para poder acceder por telnet al switch.

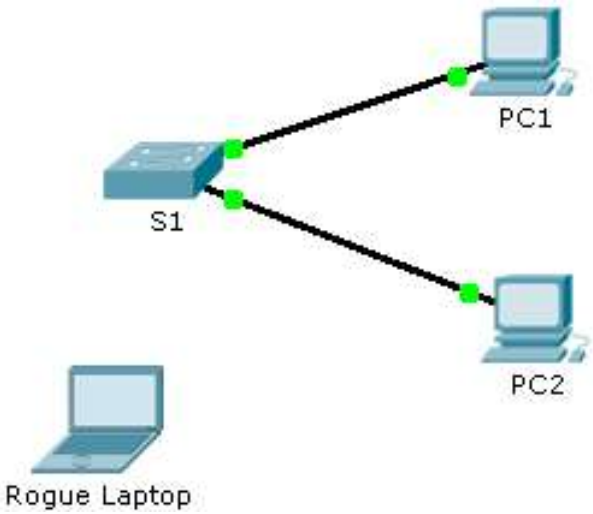
2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente? Porque vlan almacena todos los puertos de manera predeterminada

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado? Con un aviso de precaución o encriptandolas

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto? Para que solo lo pueda usar el dispositivo registrado.

2.2.4.9 Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

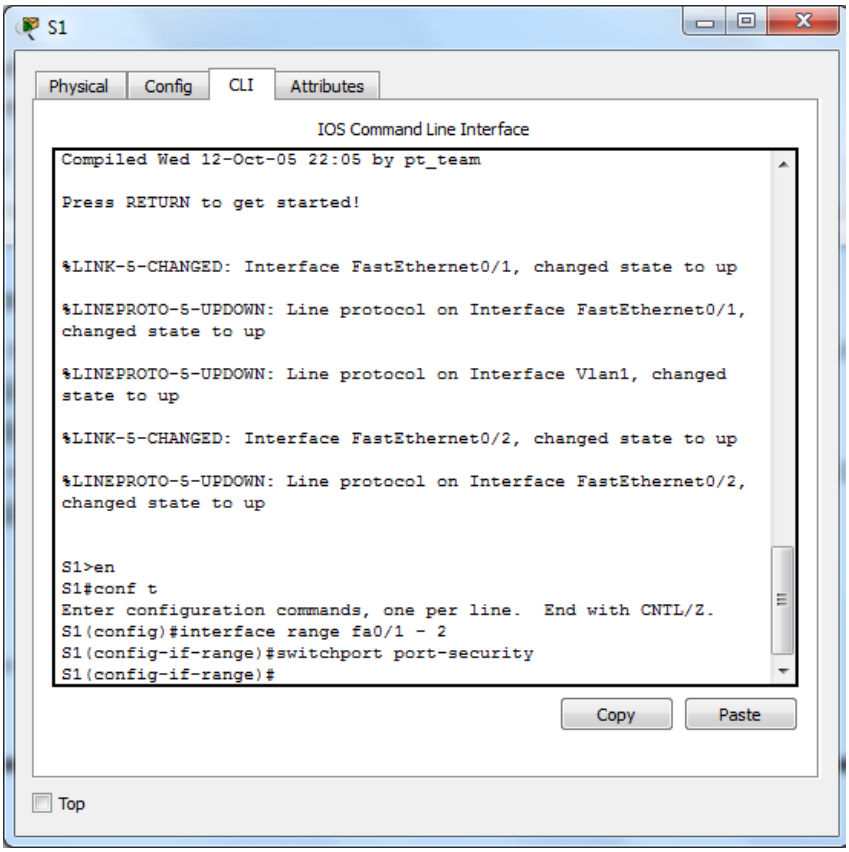
Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Part 1: Configure Port Security

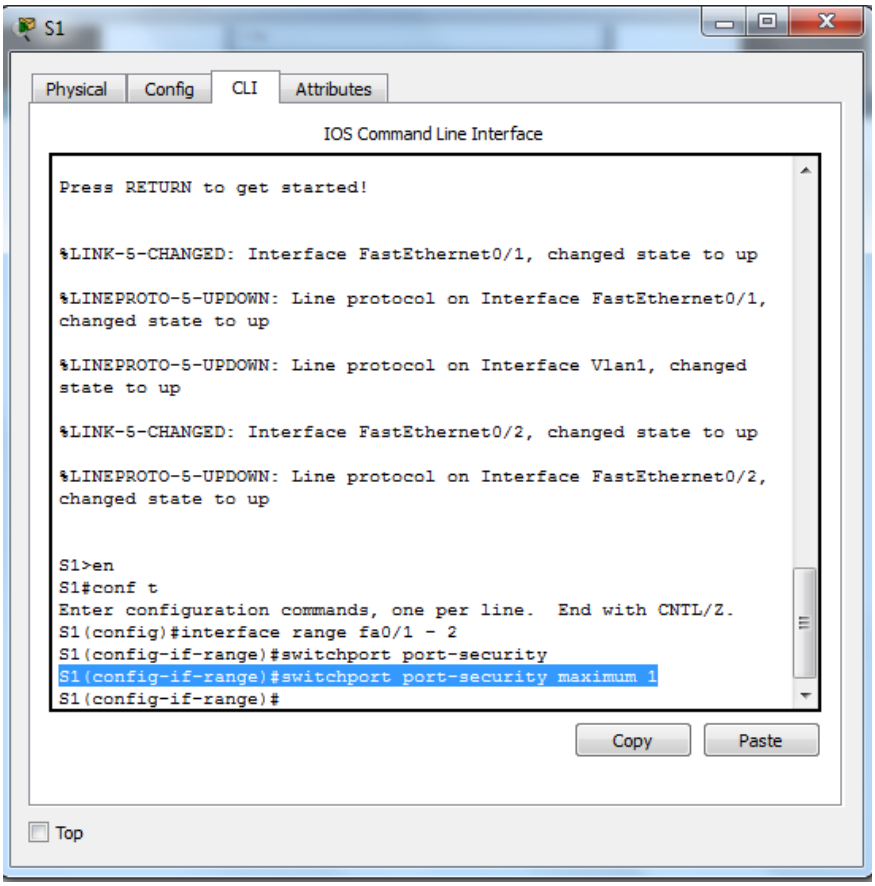
a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

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



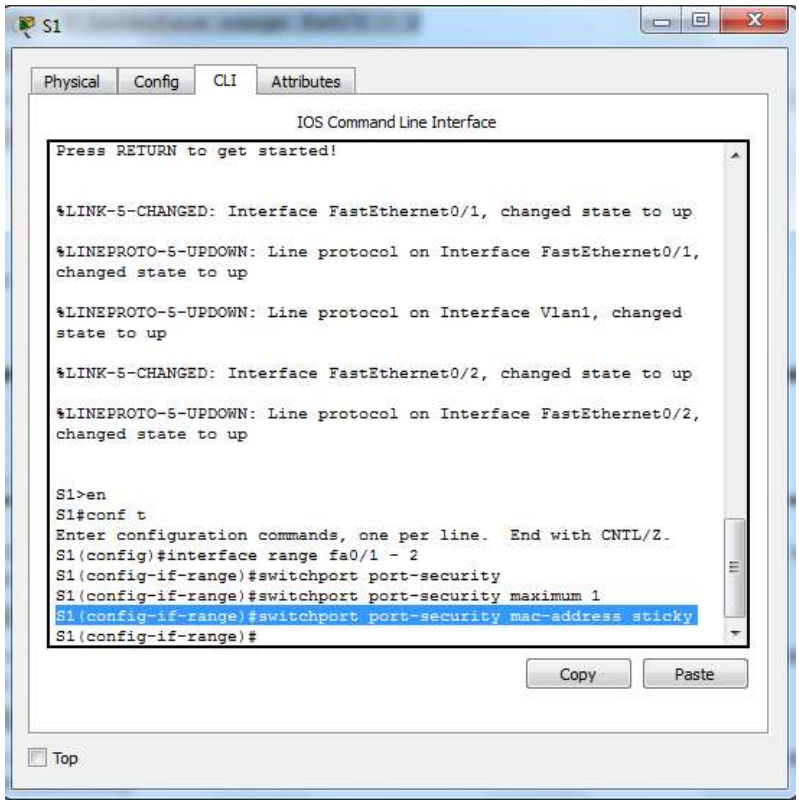
b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

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



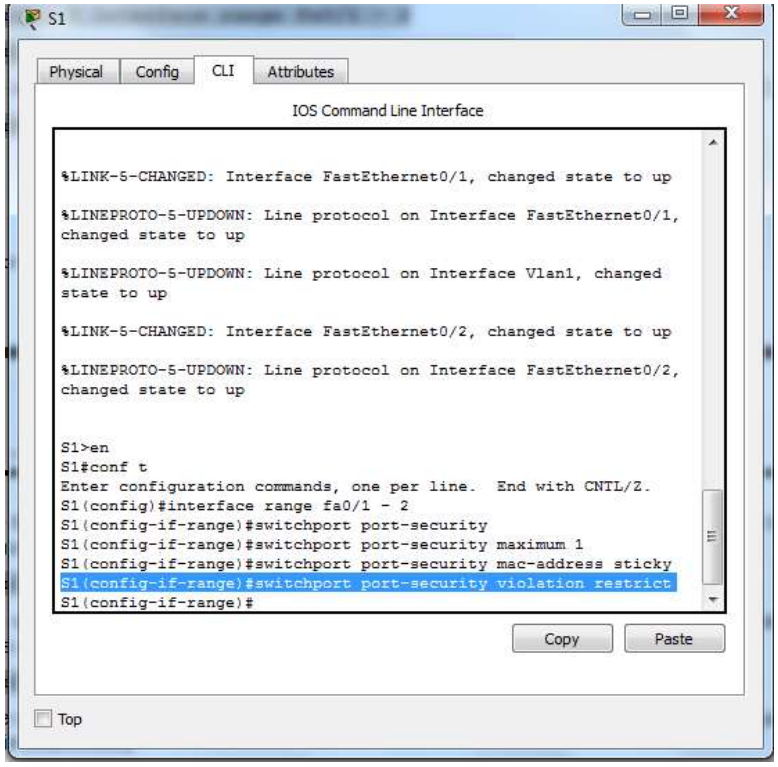
c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

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



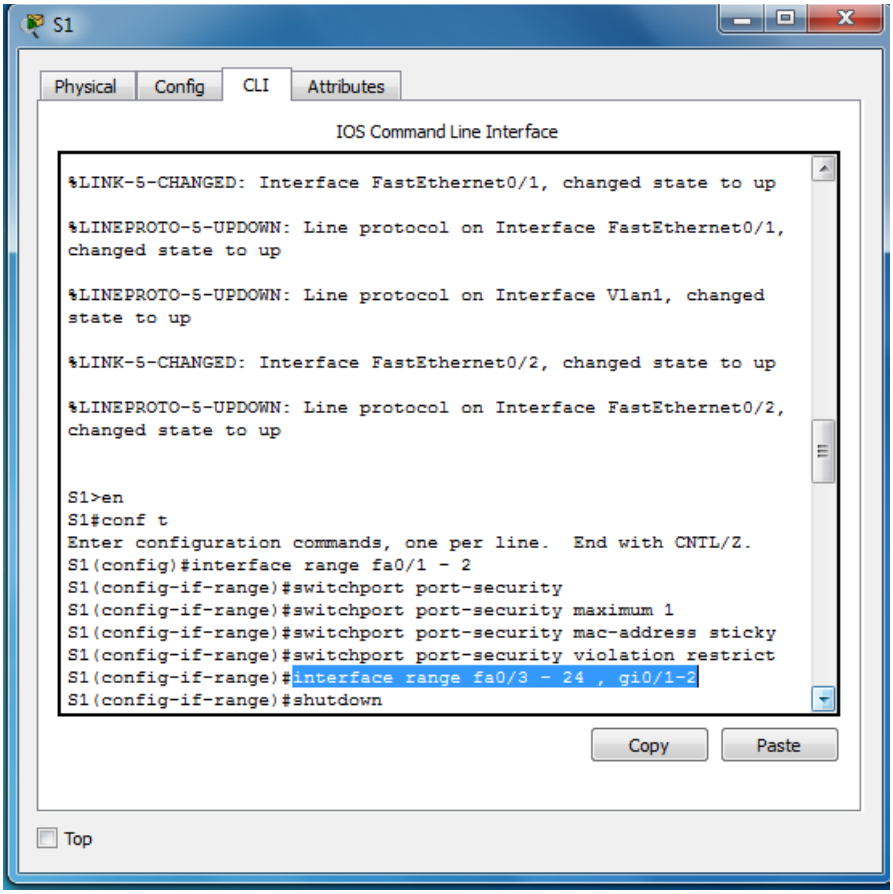
d. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but packets are dropped from an unknown source.

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

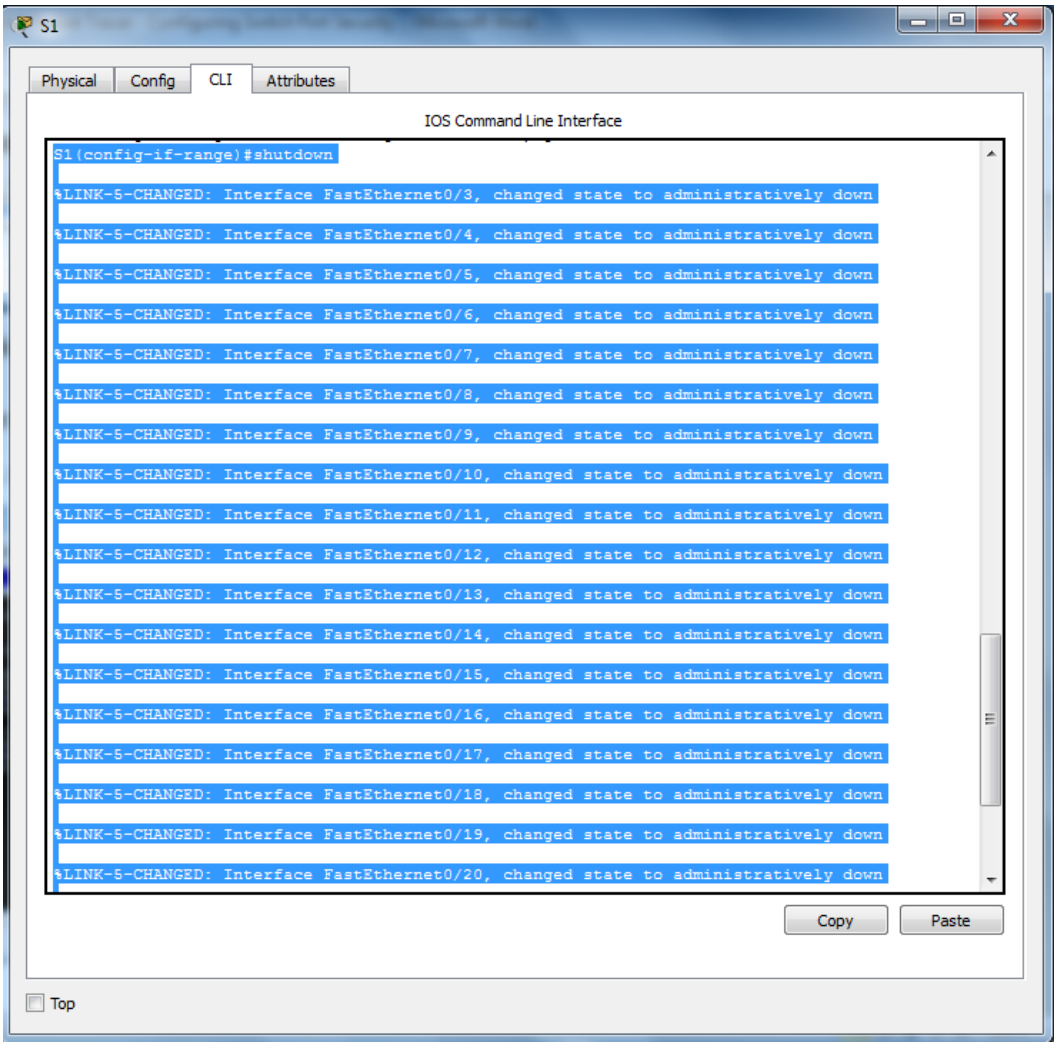


e. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

S1(config-if-range)# interface range fa0/3 - 24 , gi0/1 - 2

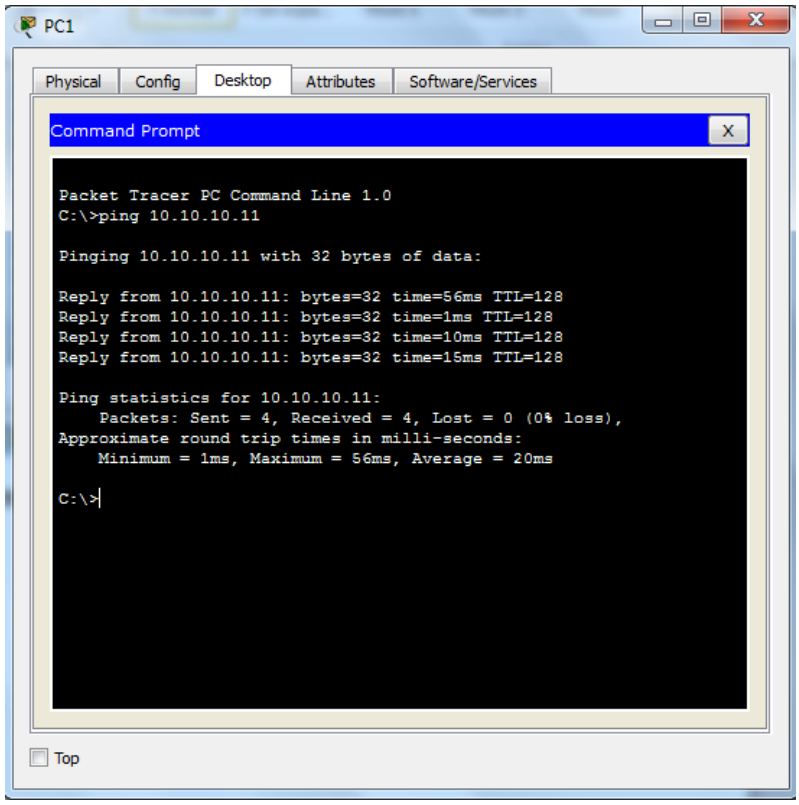


S1(config-if-range)# shutdown

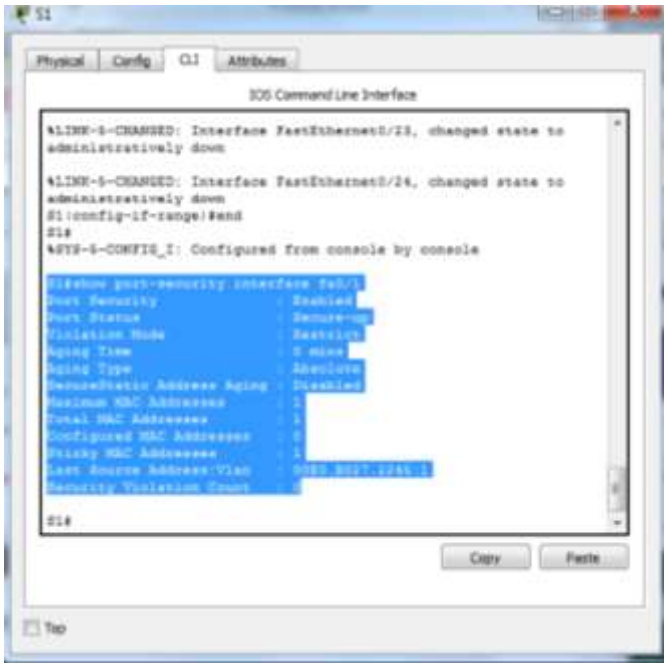


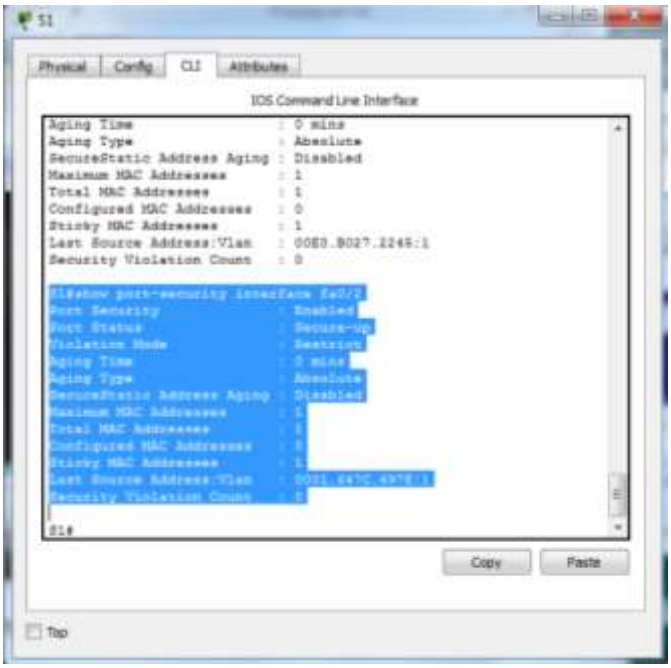
Part 2: Verify Port Security

a. From PC1, ping PC2.

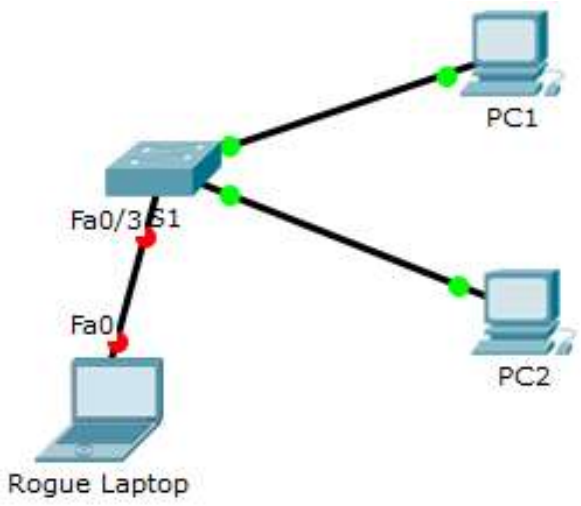


b. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

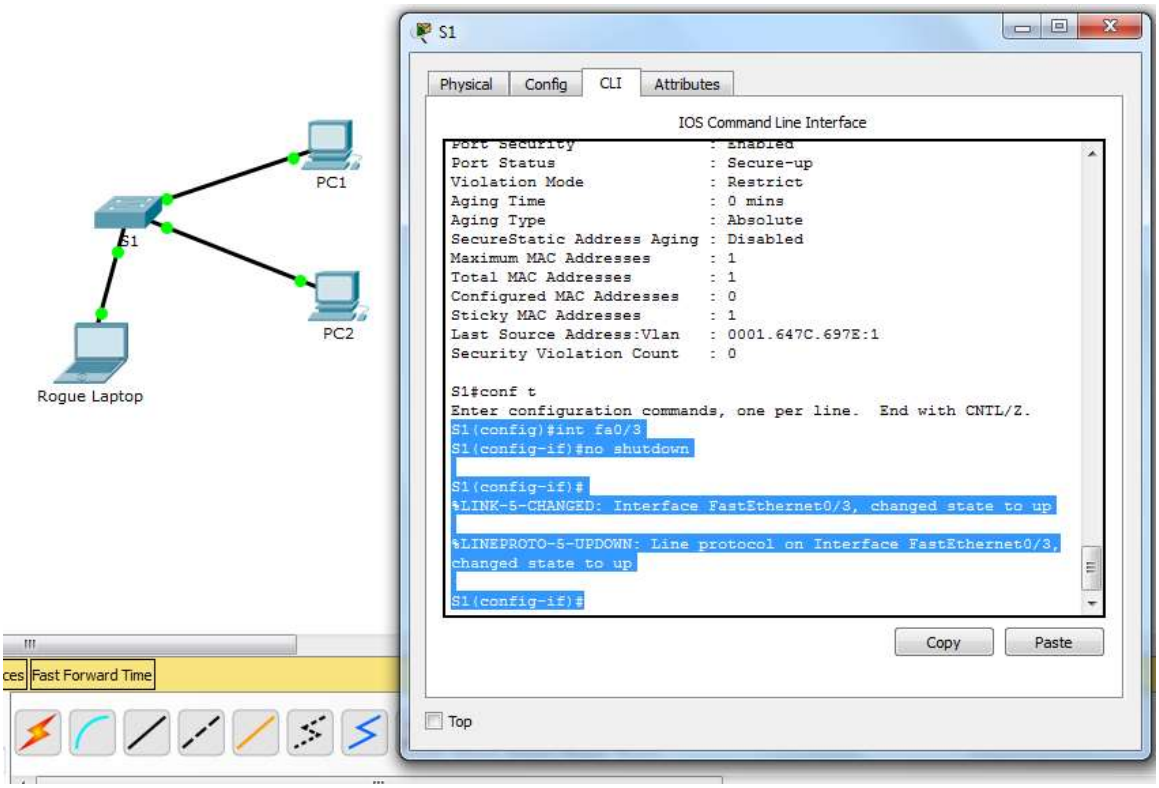




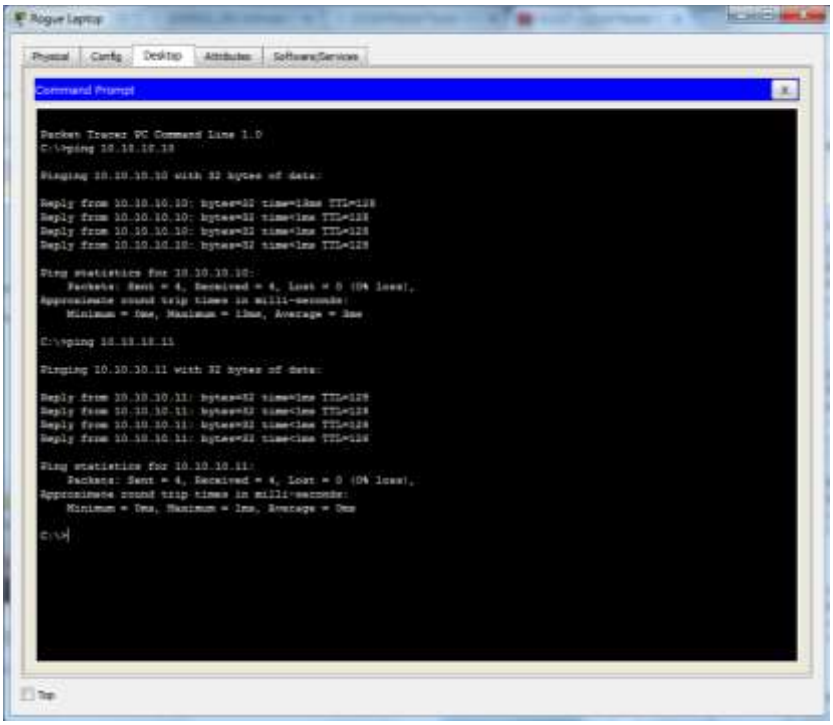
c. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.



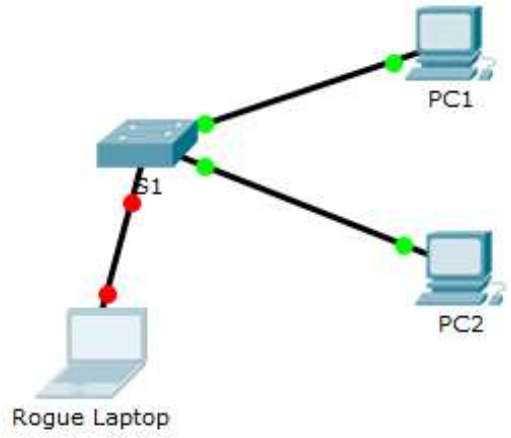
d. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**



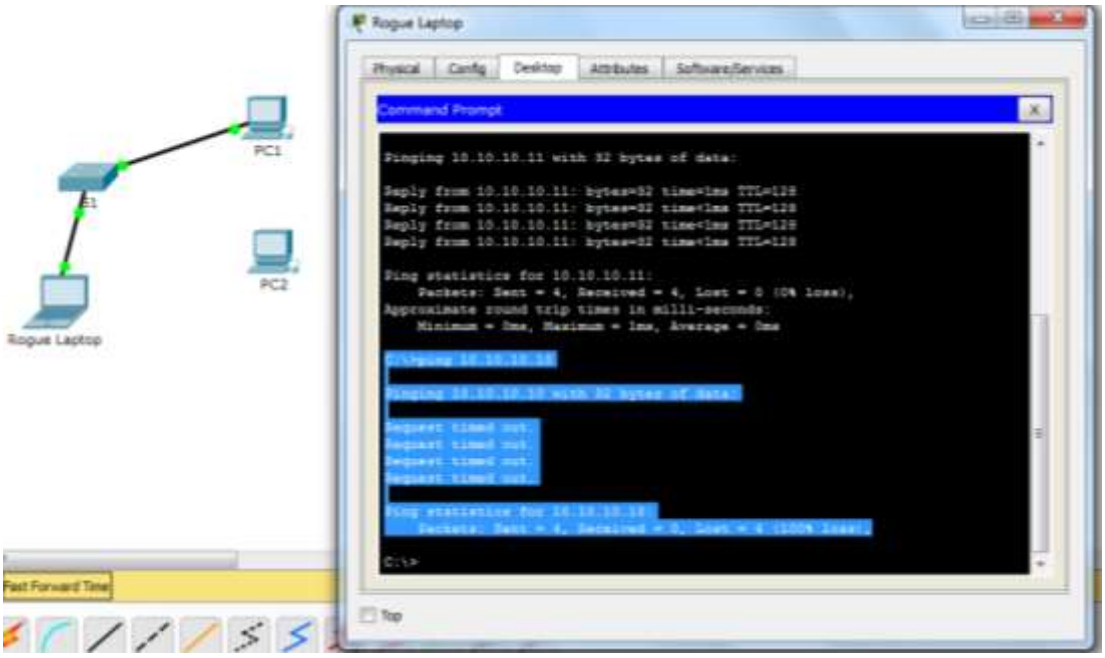
Rogue Laptop can ping **PC1** and **PC2**



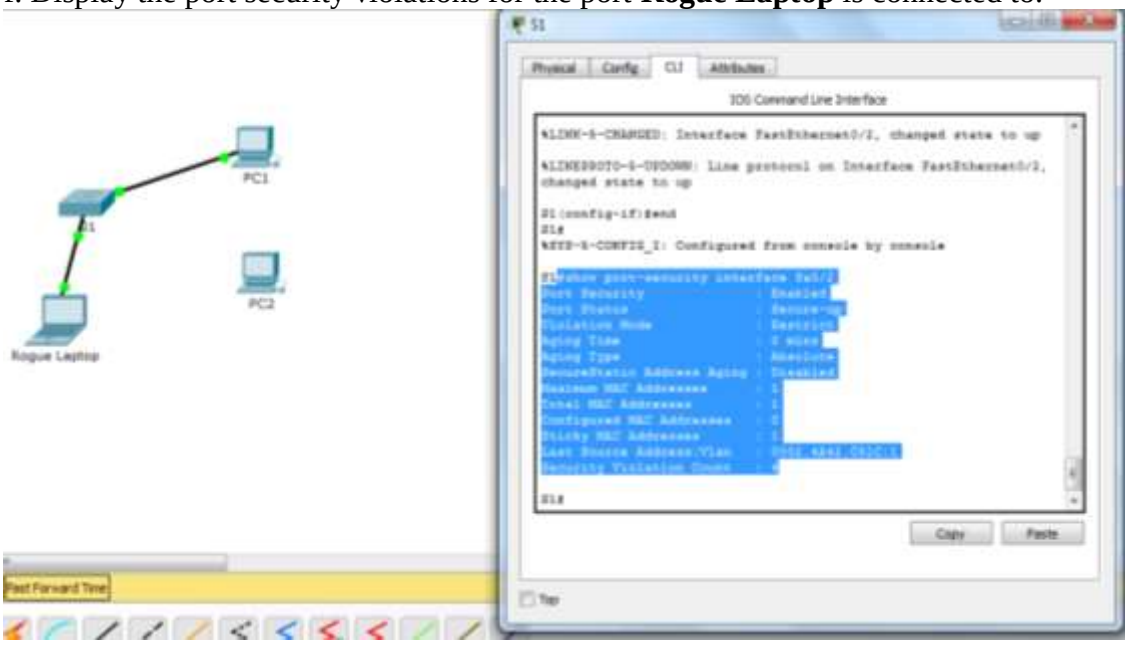
Shut down the port connected to **Rogue Laptop**



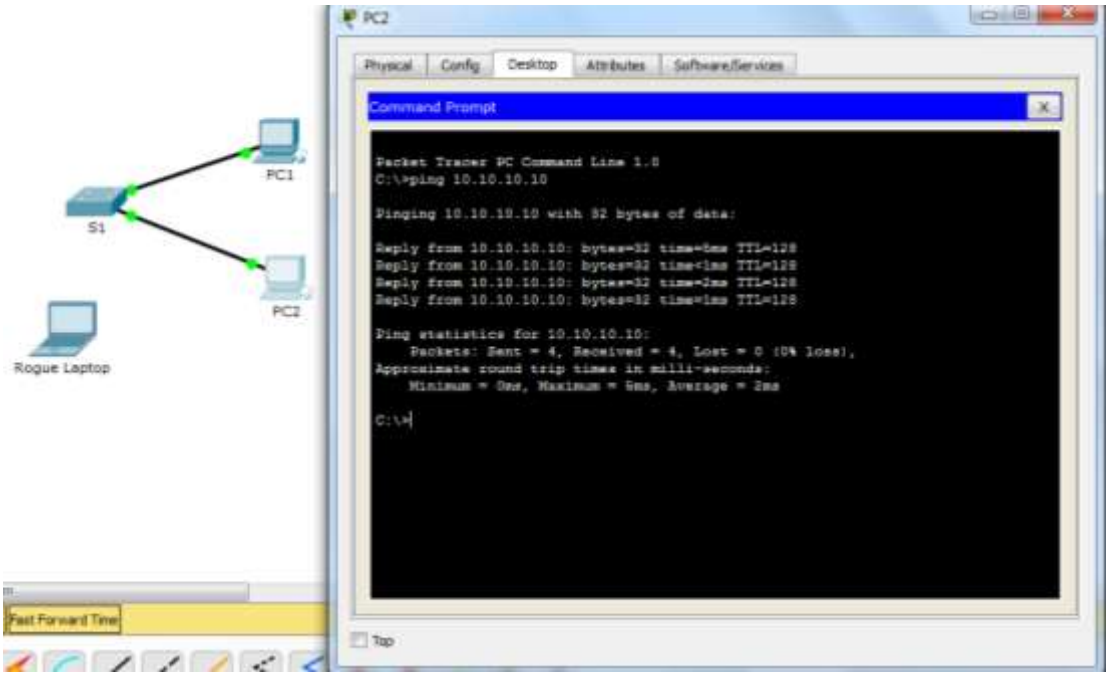
e) Disconnect **PC2** and connect **Rogue Laptop** to **PC2's** port. Verify that **Rogue Laptop** is unable to ping **PC1**.



f. Display the port security violations for the port **Rogue Laptop** is connected to.

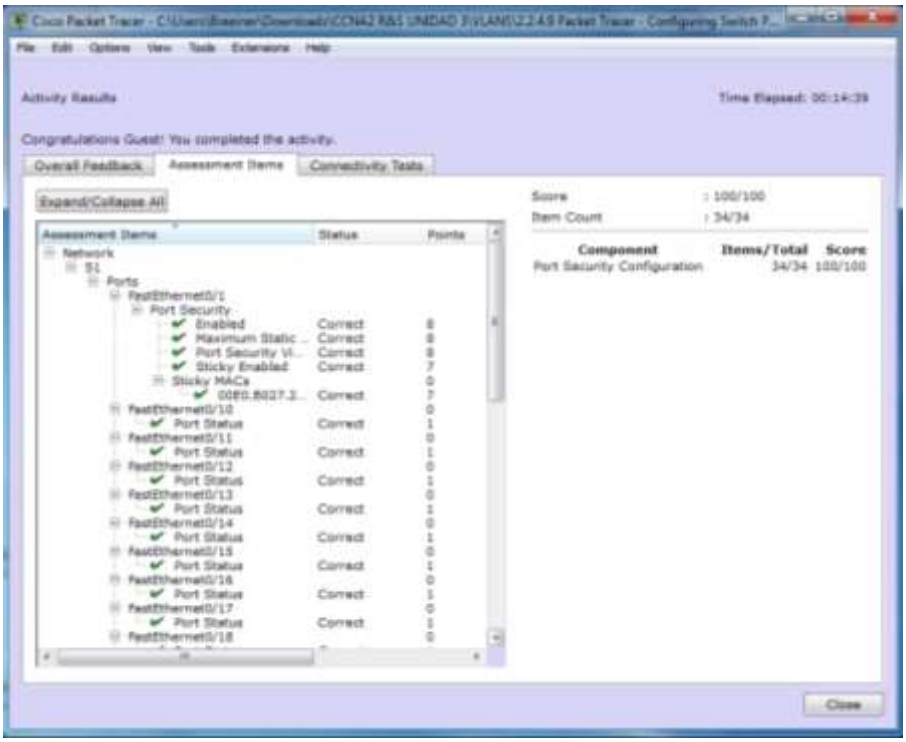


g. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.



h. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not? The port security that was enabled on the port only allowed the device, whose MAC was learned first, access to the port while preventing all other devices access.

"La seguridad del puerto que se habilitó en el puerto sólo permitió al dispositivo, cuyo MAC se aprendió primero, el acceso al puerto mientras se impide el acceso de todos los demás dispositivos."



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 1. Establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, si fuera necesario.

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

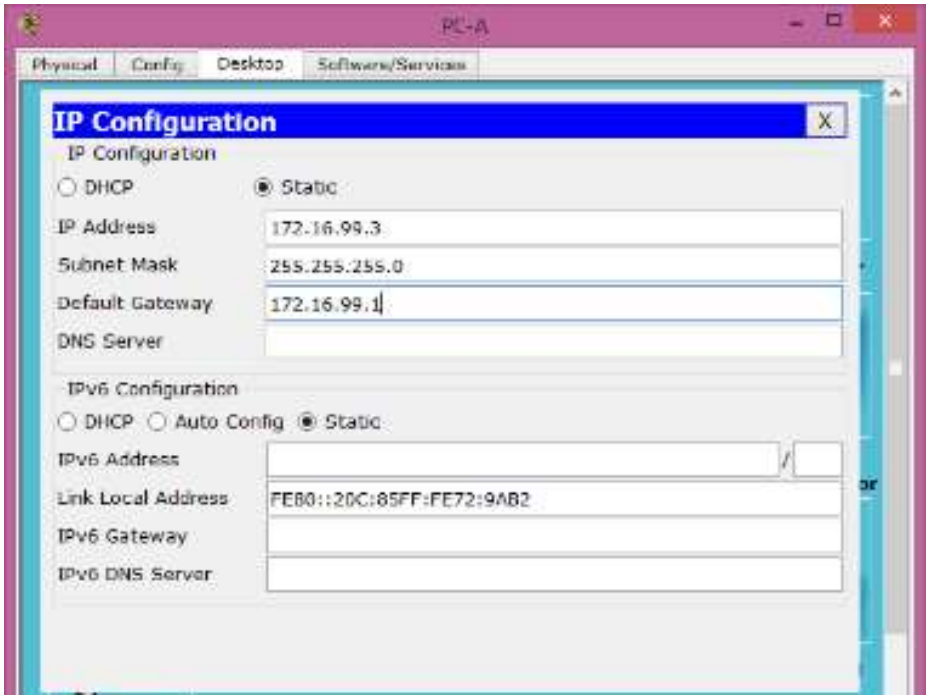
Paso 2. Inicializar y volver a cargar el router y el switch.

Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos.

Parte 2. Configurar los parámetros básicos de los dispositivos y verificar la conectividad

En la parte 2, configure los parámetros básicos en el router, el switch y la computadora. Consulte la topología y la tabla de direccionamiento incluidos al comienzo de esta práctica de laboratorio para conocer los nombres de los dispositivos y obtener información de direcciones.

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.

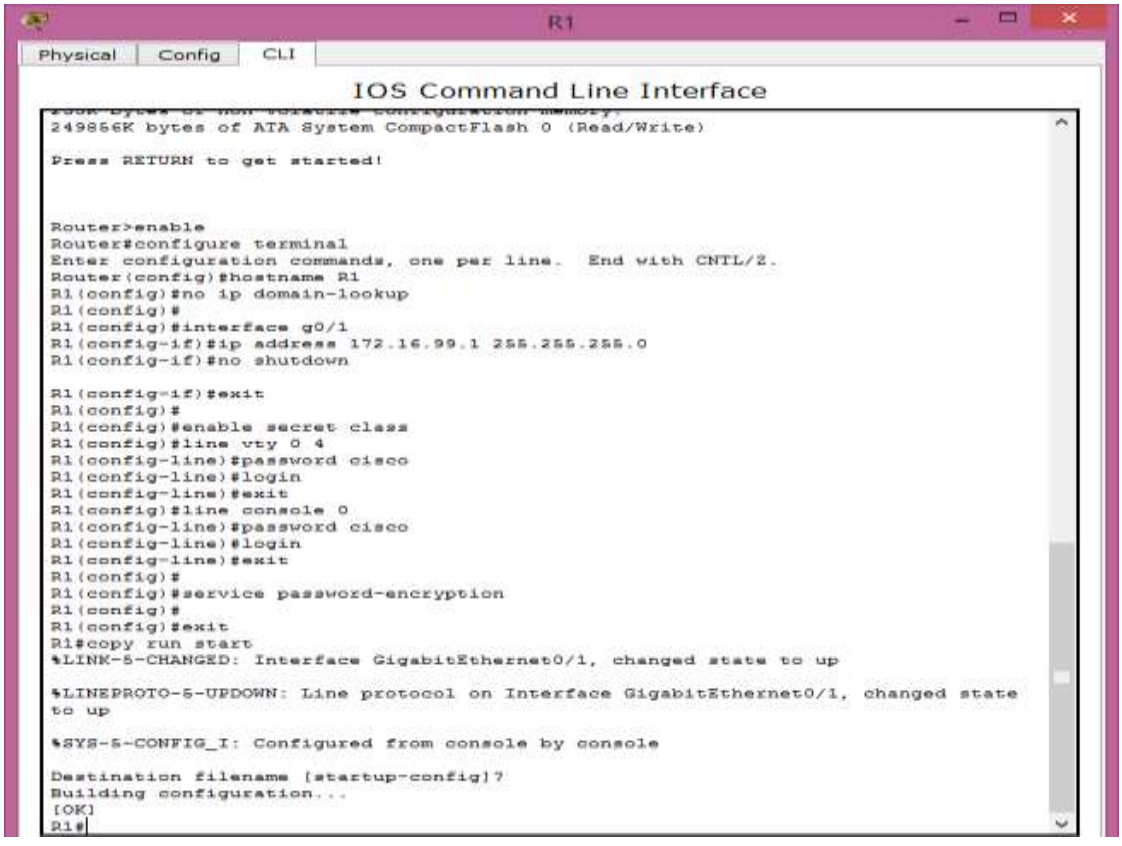
e. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

f. Cifre las contraseñas de texto no cifrado.

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

Comandos Ingresados:
enable
configure terminal
hostname R1
no ip domain-lookup

interface g0/1
ip address 172.16.99.1 255.255.255.0
no shutdown
exit
enable secret class
line vty 0 4
password cisco
login
exit
line console 0
password cisco
login
exit
service password-encryption
exit
copy run start



Paso 3. Configurar los parámetros básicos en el S1.

Una buena práctica de seguridad es asignar la dirección IP de administración del switch a una VLAN distinta de la VLAN 1 (o cualquier otra VLAN de datos con usuarios finales). En este paso, creará la VLAN 99 en el switch y le asignará una dirección IP.

a. Configure el nombre del dispositivo.

b. Desactive la búsqueda del DNS.

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

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

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

f. Cifre las contraseñas de texto no cifrado.

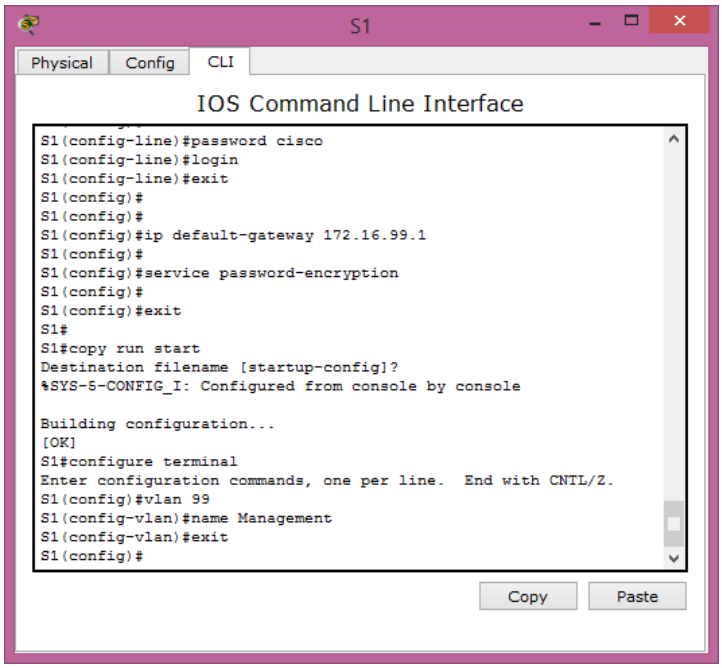
g. Guarde la configuración en ejecución en la configuración de inicio.

Comandos Usados:
enable
configure terminal
hostname S1
no ip domain-lookup
enable secret class
line vty 0 4
password cisco
login
exit
line console 0
password cisco
login
exit
ip default-gateway 172.16.99.1
service password-encryption
exit
copy run start

```
User Access Verification

Password:
Password:
Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#
S1(config)#enable secret class
S1(config)#
S1(config)#line vty 0 4
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)#login
S1(config-line)#exit
S1(config)#
S1(config)#
S1(config)#ip default-gateway 172.16.99.1
S1(config)#
S1(config)#service password-encryption
S1(config)#
S1(config)#exit
S1#
S1#copy run start
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
S1#
```

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

S1(config)# **vlan 99**
S1(config-vlan)# **name Management**
S1(config-vlan)# **exit**
S1(config)#



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

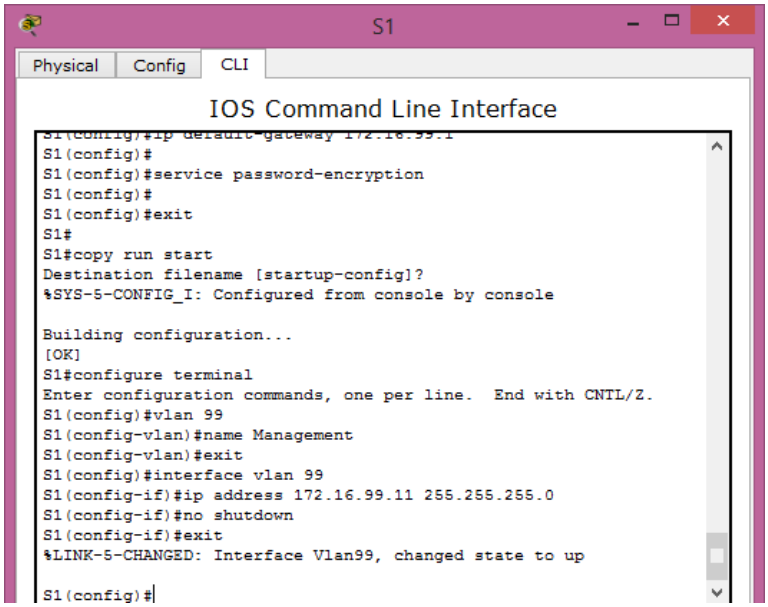
S1(config)# **interface vlan 99**

S1(config-if)# **ip address 172.16.99.11 255.255.255.0**

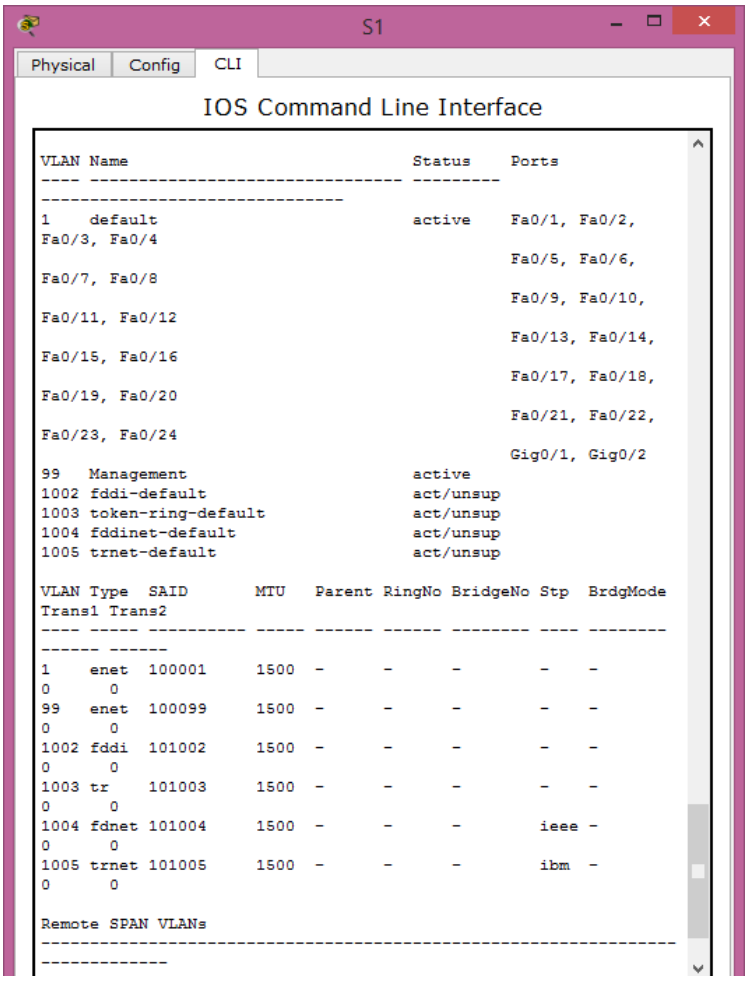
S1(config-if)# **no shutdown**

S1(config-if)# **end**

S1#



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



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

GigabitEthernet0/2 unassigned YES manual down down

Vlan1 unassigned YES manual administratively down down

Vlan99 172.16.99.11 YES manual up down

S1#

El estado es UP y el protocolo DOWN en la interface vlan99

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

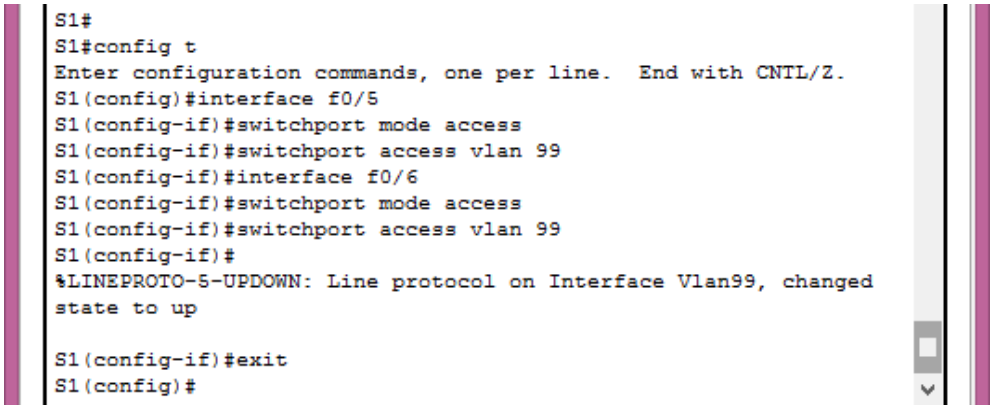
Porque VLAN 99 no tiene asignado ningúna interfaz FastEthernet

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

S1# **config t**

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 99**
S1(config-if)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 99**
S1(config-if)# **end**



m. 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 es UP y el protocolo UP en la interface vlan99

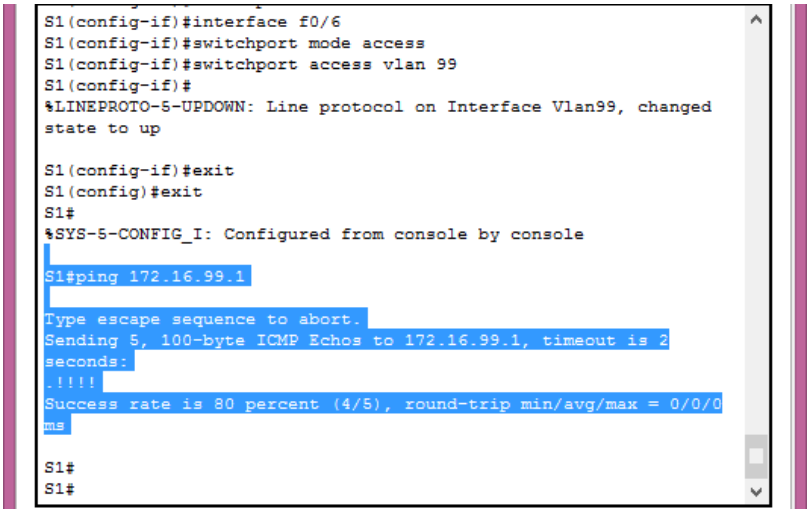
Nota: Puede haber una demora mientras convergen los estados de los puertos.

Paso 4. Verificar la conectividad entre los dispositivos.

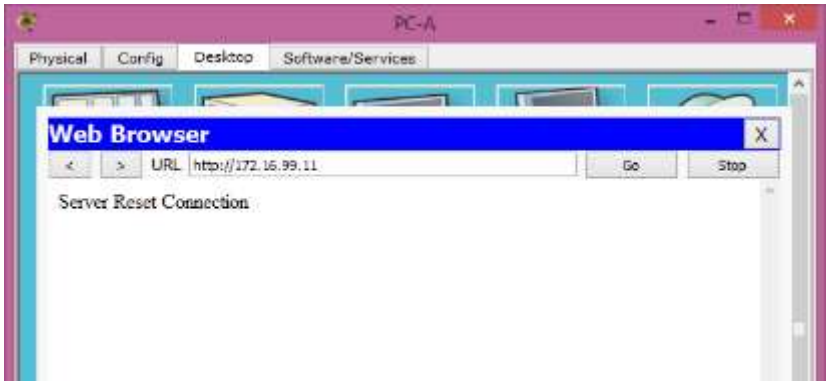
a. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? SI

b. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente? NO

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



d. 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



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

Nota: La interfaz web no segura (servidor HTTP) en un switch Cisco 2960 está habilitada de manera predeterminada. Una medida de seguridad frecuente es deshabilitar este servicio, tal como se describe en la parte 4.

Parte 3. 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**.

S1(config)# **ip domain-name 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.

Nota: La contraseña que se utiliza aquí NO es una contraseña segura. Simplemente se usa a los efectos de esta práctica de laboratorio.

S1(config)# **username admin privilege 15 secret sshadmin**

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.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

S1(config-line)# **login local**

S1(config-line)# **exit**

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

S1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 3 seconds)

S1(config)#

S1(config)# **end**

```
User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip domain-name CCNA-Lab.com
S1(config)#username admin privilege 15 secret sshadmin
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#crypto key generate rsa modulus 1024
                                  ^
% Invalid input detected at '^' marker.

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

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

S1(config)#
```

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

S1#show ip ssh

SSH Enabled - version 1.99

Authentication timeout: 120 secs; Authentication retries: 3

S1#

¿Qué versión de SSH usa el switch? 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.

S1# **config t**

S1(config)# **ip ssh time-out 75**

S1(config)# **ip ssh authentication-retries 2**

¿Cuántos intentos de autenticación permite SSH? 2

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

S1#show ip ssh

SSH Enabled - version 1.99

Authentication timeout: 75 secs; Authentication retries: 2

S1#

Paso 3. Verificar la configuración de SSH en el S1.

f. Mediante un software de cliente SSH en la PC-A (como Tera Term), abra una conexión SSH en el S1. Si recibe un mensaje en el cliente SSH con respecto a la clave de host, acéptela. Inicie sesión con el nombre de usuario **admin** y la contraseña **class**.

¿La conexión se realizó correctamente? SI

¿Qué petición de entrada se mostró en el S1? ¿Por qué?

Modo exec privilegiado.

Porque al usar la opción privilege 15 al crear el usuario se establecio de esta manera.

g. Escriba **exit** para finalizar la sesión de SSH en el S1.

Parte 4. Configurar y verificar las características de seguridad en el S1

En la parte 4, desactivará los puertos sin utilizar, desactivará determinados servicios que se ejecutan en el switch y configurará la seguridad de puertos según las direcciones MAC. Los switches pueden estar sujetos a ataques de desbordamiento de la tabla de direcciones MAC, a ataques de suplantación de direcciones MAC y a conexiones no autorizadas a los puertos

del switch. Configurará la seguridad de puertos para limitar la cantidad de direcciones MAC que se pueden detectar en un puerto del switch y para deshabilitar el puerto si se supera ese número.

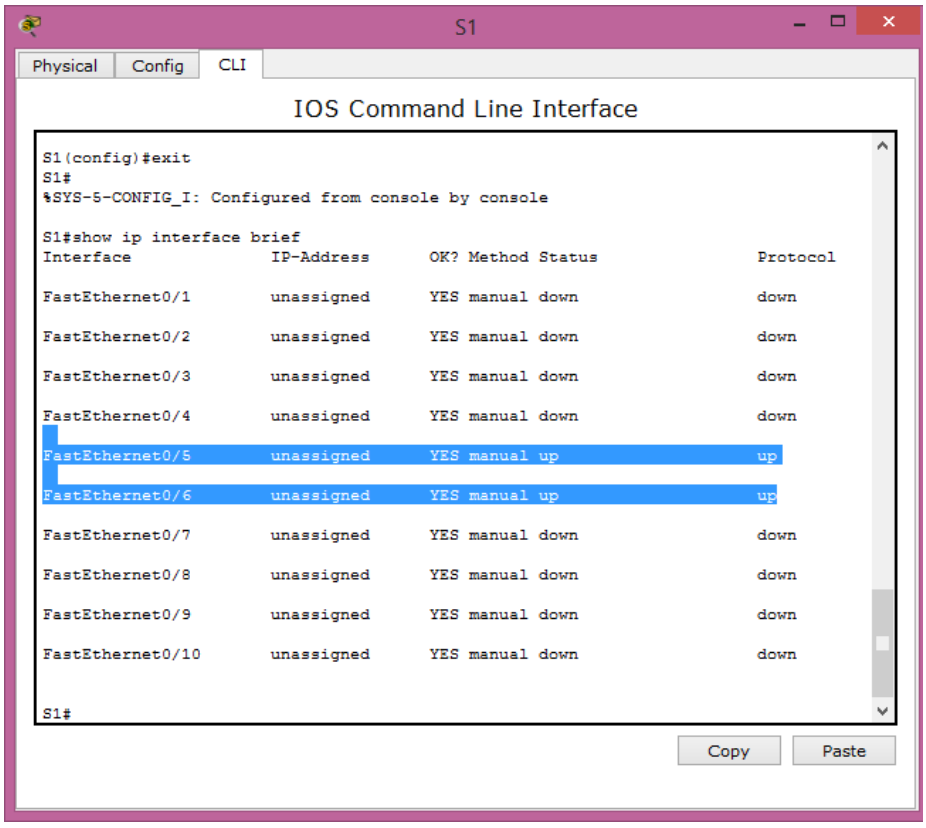
Paso 1. Configurar las características de seguridad general en el S1.

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

Banner motd "Solo Personal Autorizado"

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

Fa0/5 y Fa0/6



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

S1(config)# **interface range f0/1 – 4**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **interface range f0/7 – 24**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **interface range g0/1 – 2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

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**.

¿Cuál es el estado del servidor HTTP? Este comando no está soportado por packet tracer

¿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?

Server Reset Connection

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?

Server Reset Connection No puede conectarse

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.

R1# **show interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

¿Cuál es la dirección MAC de la interfaz G0/1 del R1?

GigabitEthernet0/1 is up, line protocol is up (connected)

Hardware is CN Gigabit Ethernet, address is 0060.702b.d902 (bia 0060.702b.d902)

Internet address is 172.16.99.1/24

0060.702b.d902

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: 0005.5e72.c805

Dirección MAC de F0/6: 0005.5e72.c806

l.Configure la seguridad básica de los puertos.

Nota: Normalmente, este procedimiento se realizaría en todos los puertos de acceso en el switch. Aquí se muestra F0/5 como ejemplo.

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

S1(config)# **interface f0/5**

2) Desactive el puerto.

S1(config-if)# **shutdown**

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

S1(config-if)# **switchport port-security**

Nota: La introducción del comando **switchport port-security** establece la cantidad máxima de direcciones MAC en 1 y la acción de violación en shutdown. Los comandos **switchport port-security maximum** y **switchport port-security violation** se pueden usar para cambiar el comportamiento predeterminado.

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

S1(config-if)# **switchport port-security mac-address xxxx.xxxx.xxxx**

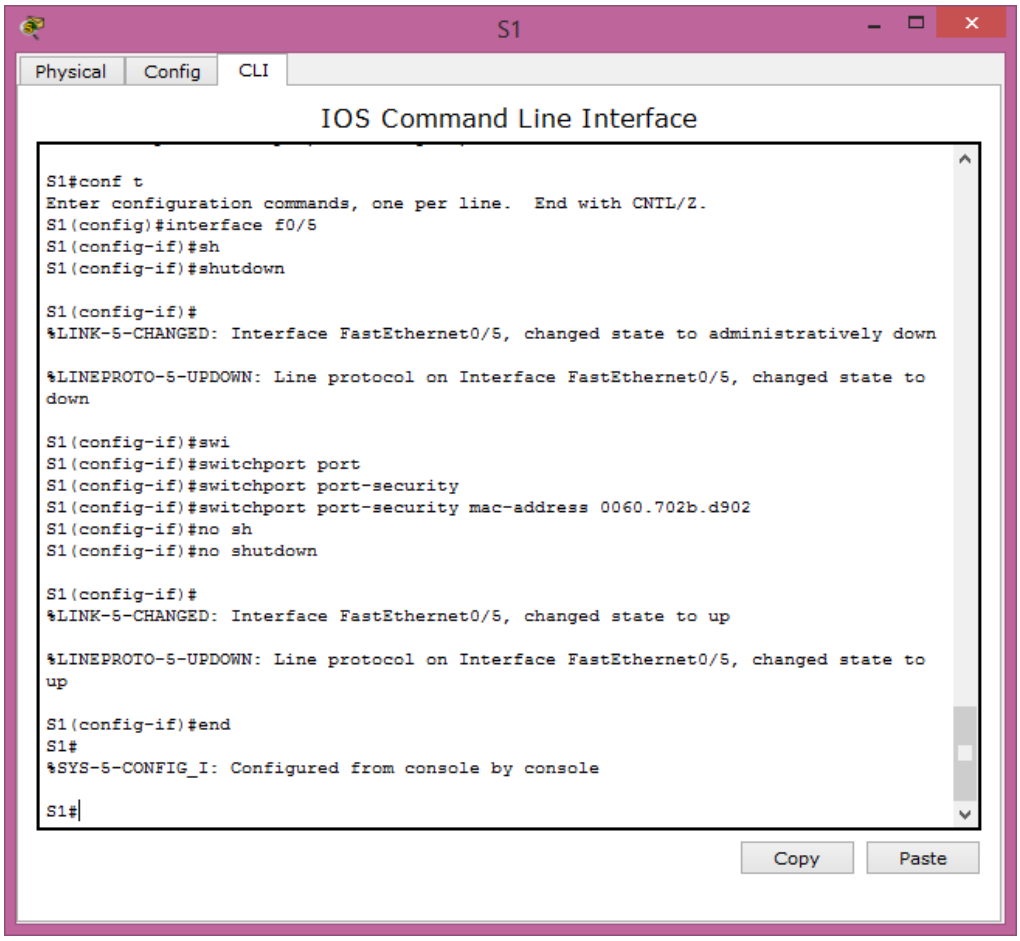
(xxxx.xxxx.xxxx es la dirección MAC real de la interfaz G0/1 del router)

Nota: De manera optativa, puede usar el comando **switchport port-security mac-address sticky** para agregar todas las direcciones MAC seguras que se detectan dinámicamente en un puerto (hasta el máximo establecido) a la configuración en ejecución del switch.

5) Habilite el puerto del switch.

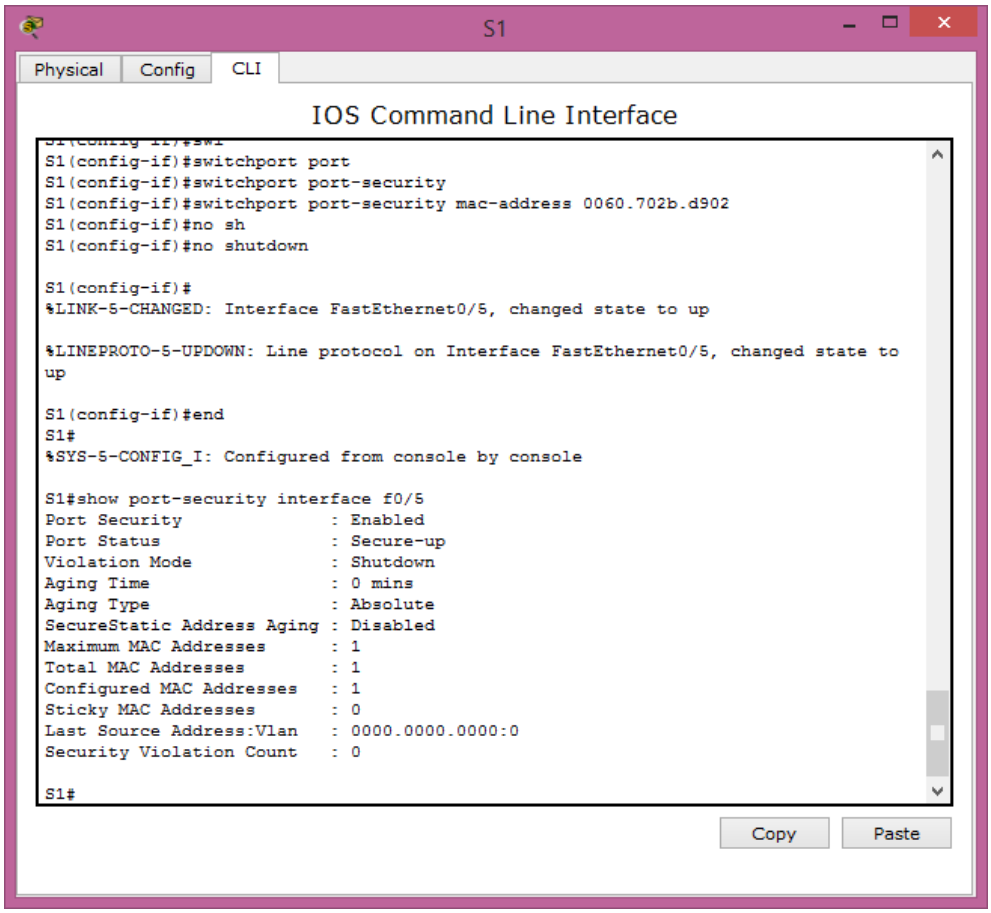
S1(config-if)# **no shutdown**

S1(config-if)# **end**



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

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 : 0000.0000.0000:0
Security Violation Count : 0



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

UP con Seguridad Abilitada

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

R1# **ping 172.16.99.3**

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 80 percent (4/5), round-trip min/avg/max = 0/1/3 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.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **shutdown**

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

R1(config-if)# **mac-address 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.

R1(config-if)# **no shutdown**

```
User Access Verification

Password:

R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down

R1(config-if)#mac-address aaaa.bbbb.cccc
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#
```

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, el puerto F0/5 en el S1 está desactivado debido a la violación de seguridad que hemos cometido al conectar un dispositivo con una MAC diferente

```
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
down
Solo Personal Autorizado

User Access Verification

Password:
Password:

S1>en
Password:
S1#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

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

S1#
```

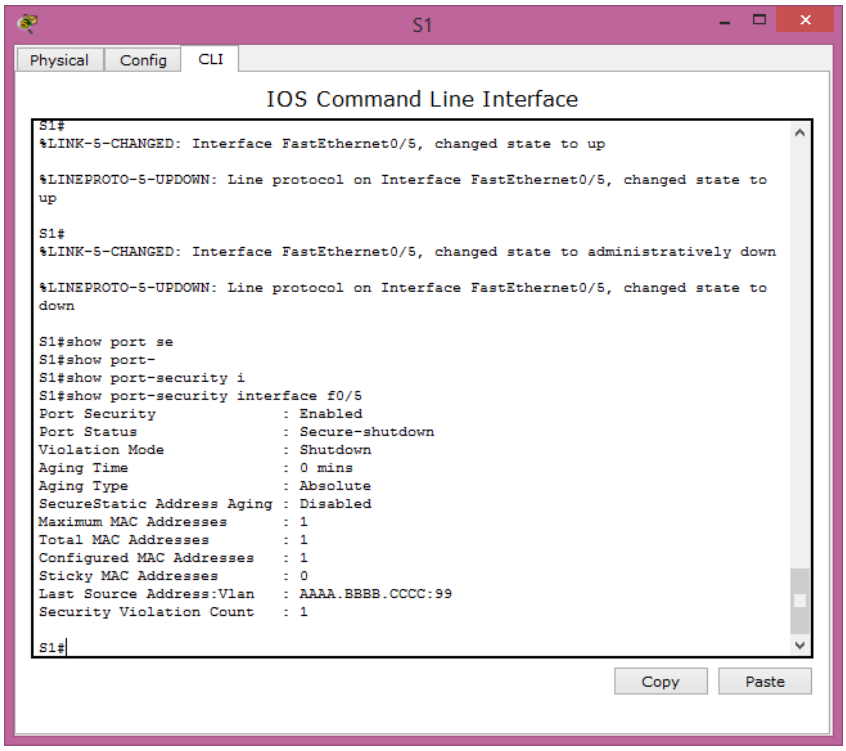
s. En el switch, verifique la seguridad de puertos con los comandos que se muestran a continuación.

S1# **show port-security**

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count)       (Count)       (Count)
---------------------------------------------------------------------
    Fa0/5          1          1              1        Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

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

```
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**

FastEthernet0/5 is down, line protocol is down (err-disabled)

Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

<output omitted>

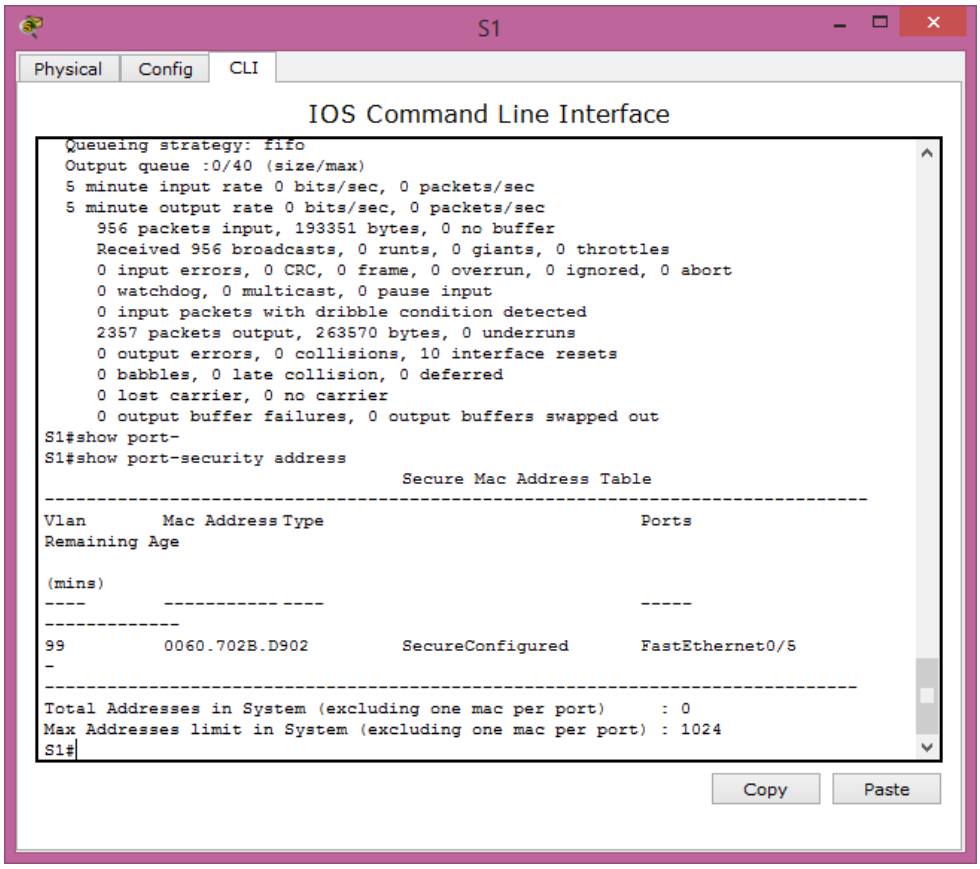
S1# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
99	30f7.0da3.1821	SecureConfigured	Fa0/5	-

Total Addresses in System (excluding one mac per port) :0

Max Addresses limit in System (excluding one mac per port) :8192



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.

R1(config-if)# **shutdown**

R1(config-if)# **no mac-address aaaa.bbbb.cccc**

R1(config-if)# **no shutdown**

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

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

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down
.....
Success rate is 0 percent (0/5)

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#shut
R1(config-if)#shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

R1(config-if)#no mac-a
R1(config-if)#no mac-address aaaa.bbbb.cccc
R1(config-if)#no shu
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

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 0 percent (0/5)

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 0 percent (0/5)

R1#
```

v. Emita el comando **show interface f0/5** para determinar la causa de la falla del ping. Registre sus conclusiones.

```
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0005.5e72.c805 (bia 0005.5e72.c805)
 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
S1#
```

A interface está deshabilitada a causa de la violación anterior cuando se usó una mac diferente para la conexión del puerto.

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

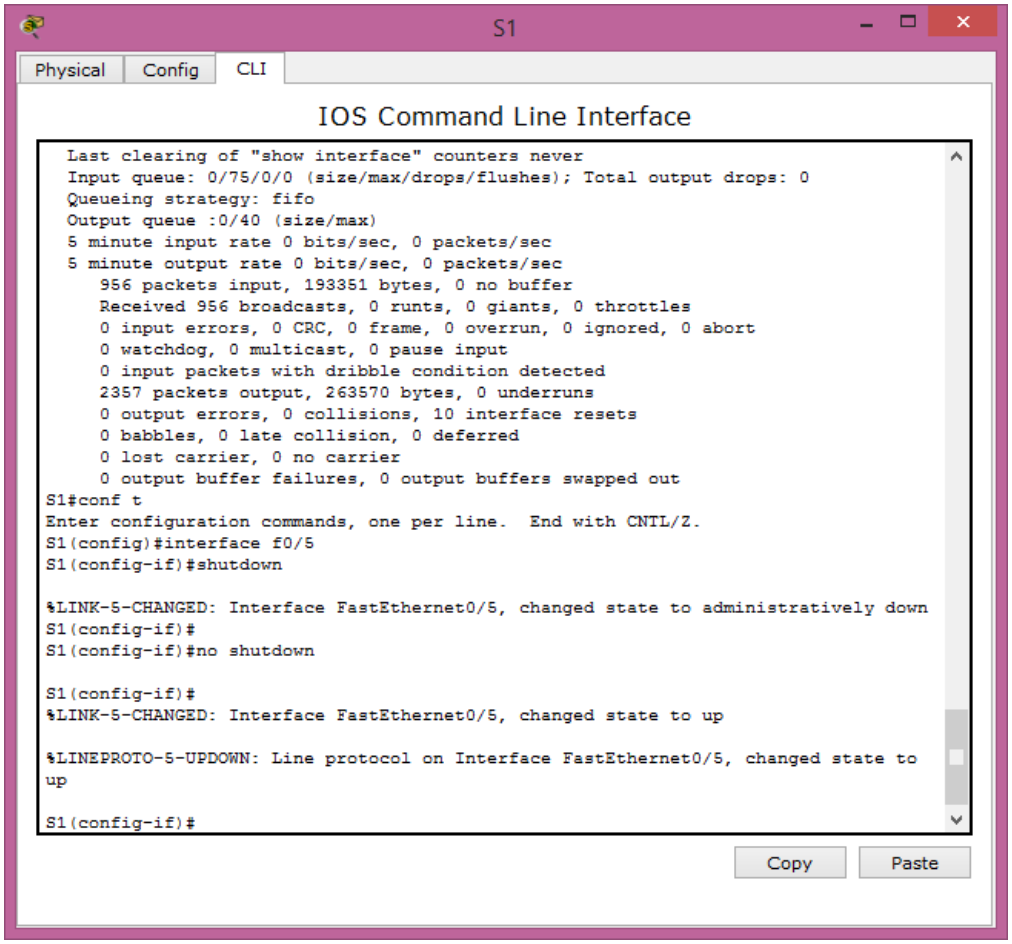
S1# **config t**

S1(config)# **interface f0/5**

S1(config-if)# **shutdown**

S1(config-if)# **no shutdown**

Nota: puede haber una demora mientras convergen los estados de los puertos.



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**

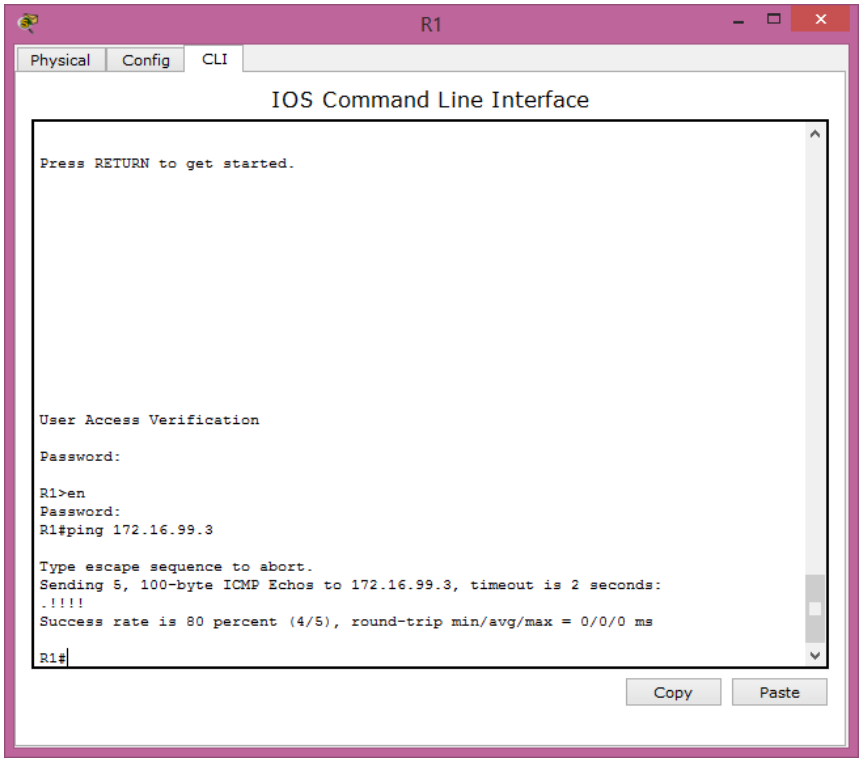
FastEthernet0/5 is up, line protocol is up (connected)

Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

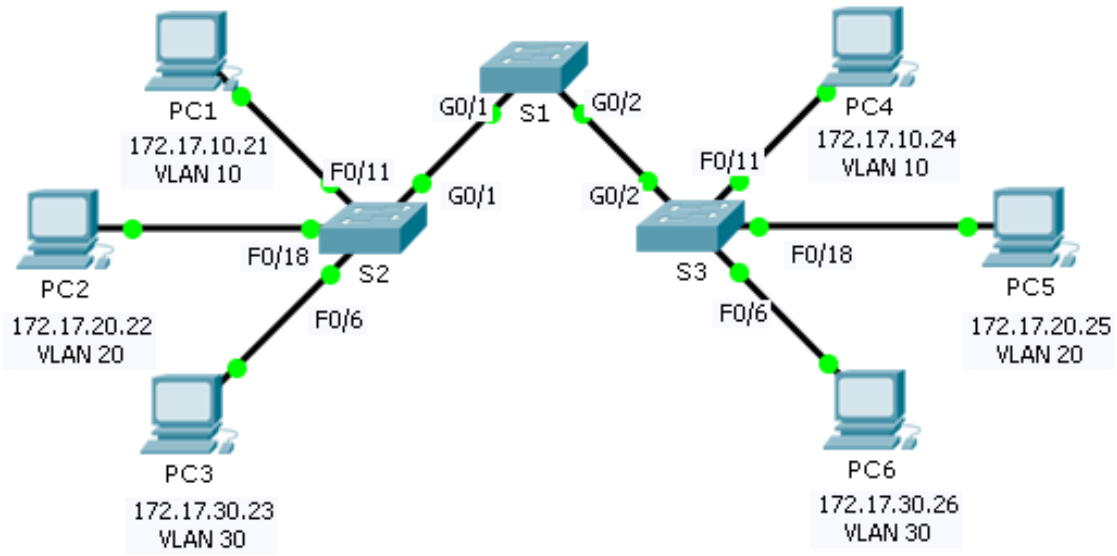
reliability 255/255, txload 1/255, rxload 1/255

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



3.2.1.7 Packet Tracer – Configuring VLANs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Objectives

Part 1: Verify the Default VLAN Configuration
Part 2: Configure VLANs
Part 3: Assign VLANs to Ports

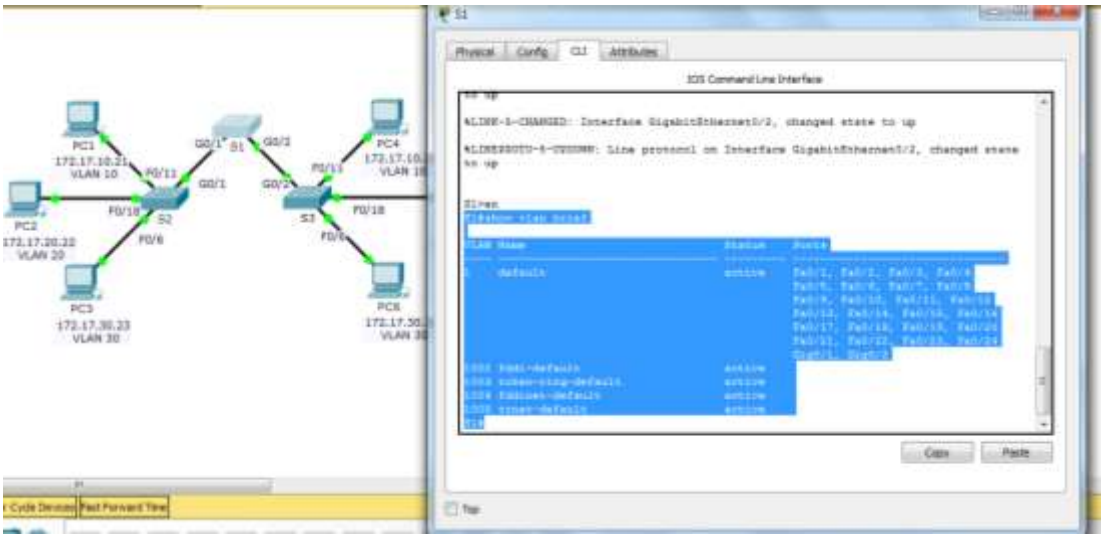
Background

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

Part 1: View the Default VLAN Configuration
Step 1: Display the current VLANs.

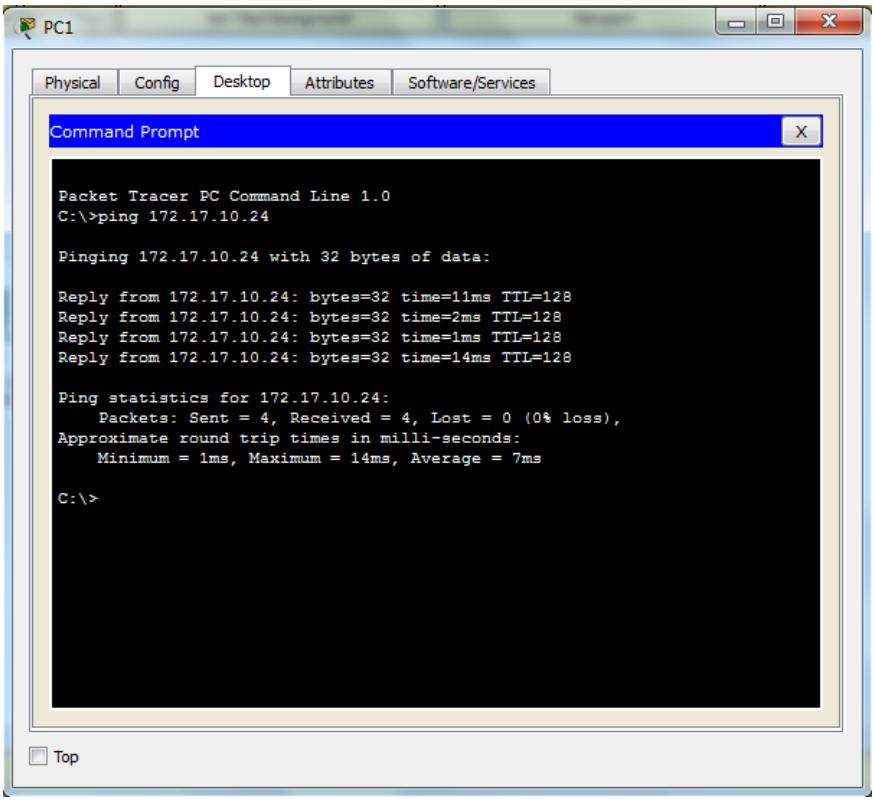
On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

S1# **show vlan brief**

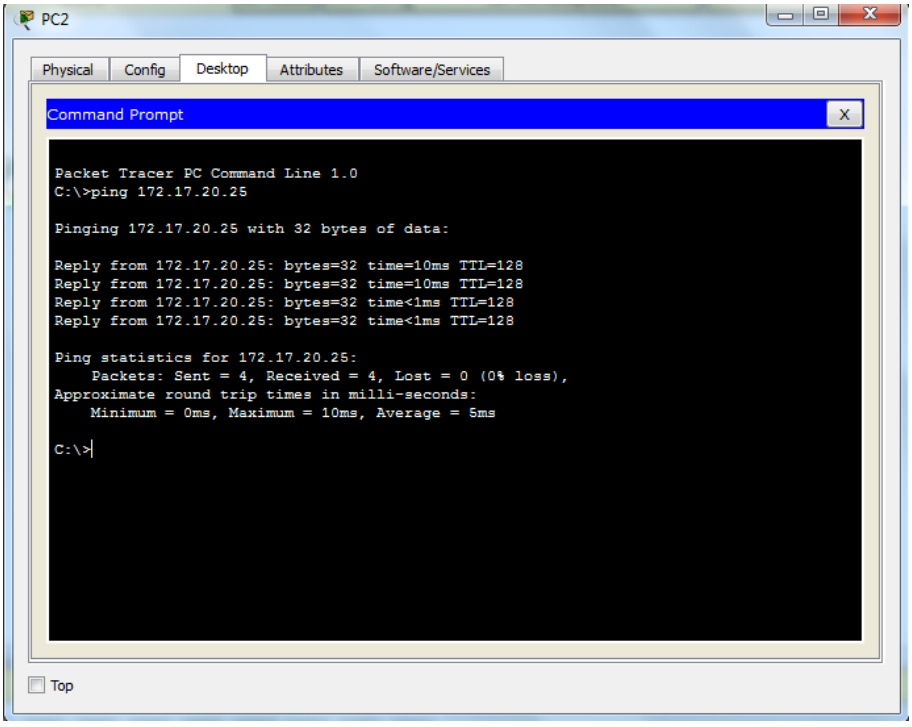


Step 2: Verify connectivity between PCs on the same network.
Notice that each PC can ping the other PC that shares the same network.

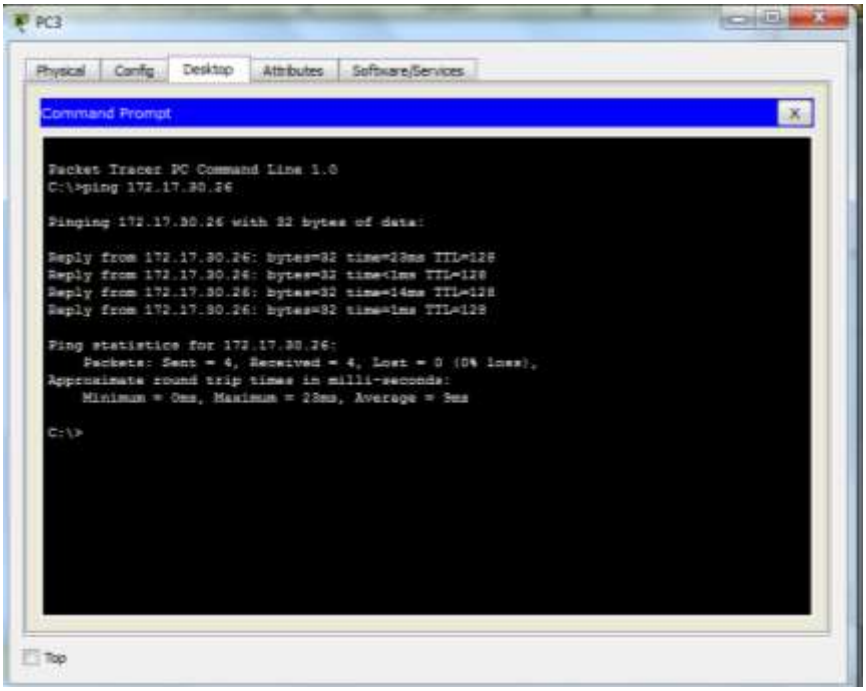
- PC1 can ping PC4



- PC2 can ping PC5



- PC3 can ping PC6



Pings to PCs in other networks fail.

What benefit will configuring VLANs provide to the current configuration? The primary benefits of using VLANs are as follows: security, cost reduction, higher performance, broadcast storm mitigation, improved IT staff efficiency, and simpler project and application management.

Part 2: Configure VLANs

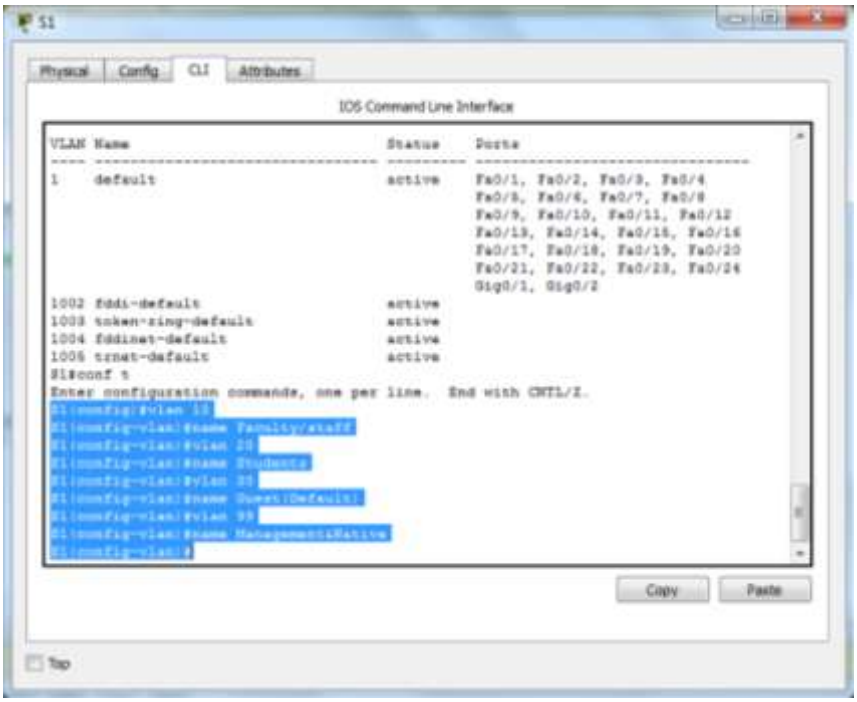
Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native

S1#(config)# **vlan 10**
S1#(config-vlan)# **name Faculty/Staff**
S1#(config-vlan)# **vlan 20**
S1#(config-vlan)# **name Students**
S1#(config-vlan)# **vlan 30**
S1#(config-vlan)# **name Guest(Default)**

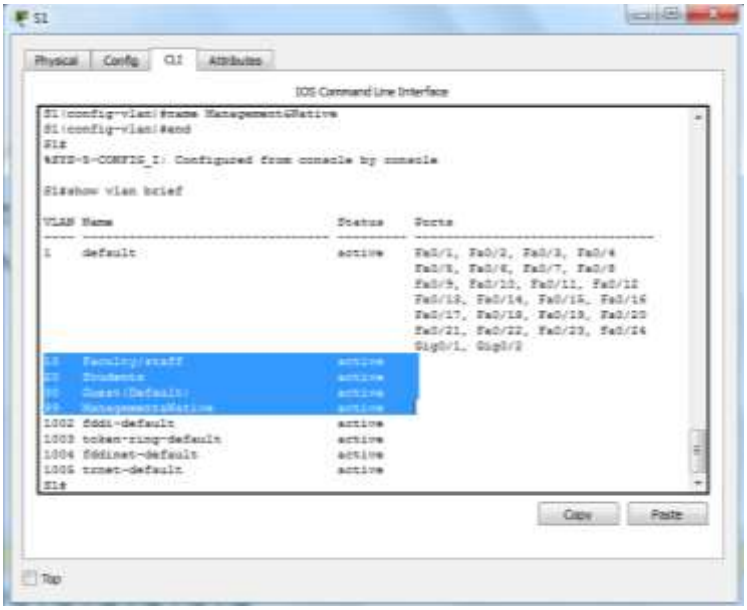
S1#(config-vlan)# **vlan 99**
S1#(config-vlan)# **name Management&Native**



Step 2: Verify the VLAN configuration.

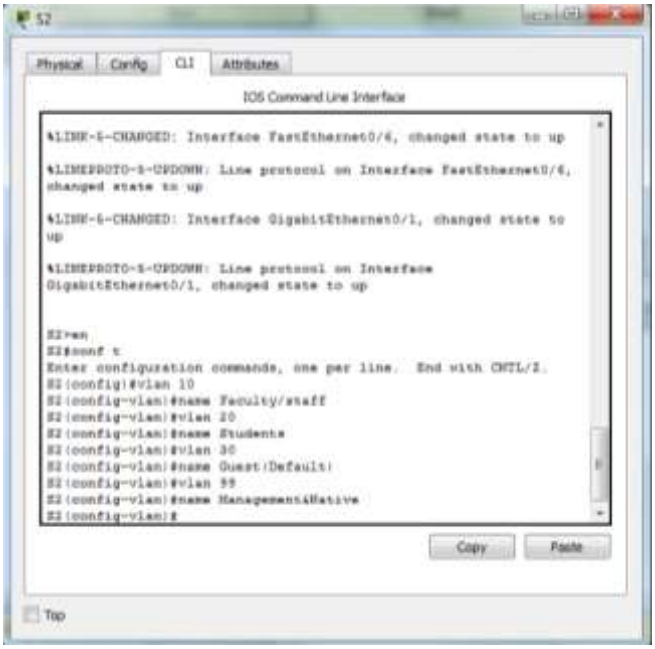
Which command will only display the VLAN name, status, and associated ports on a switch?

S1# **show vlan brief**

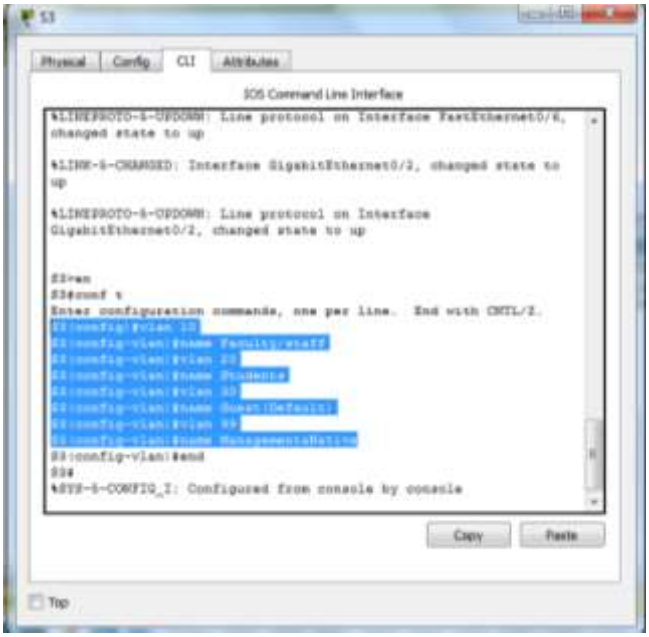


Step 3: Create the VLANs on S2 and S3.
Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

VLANs S2

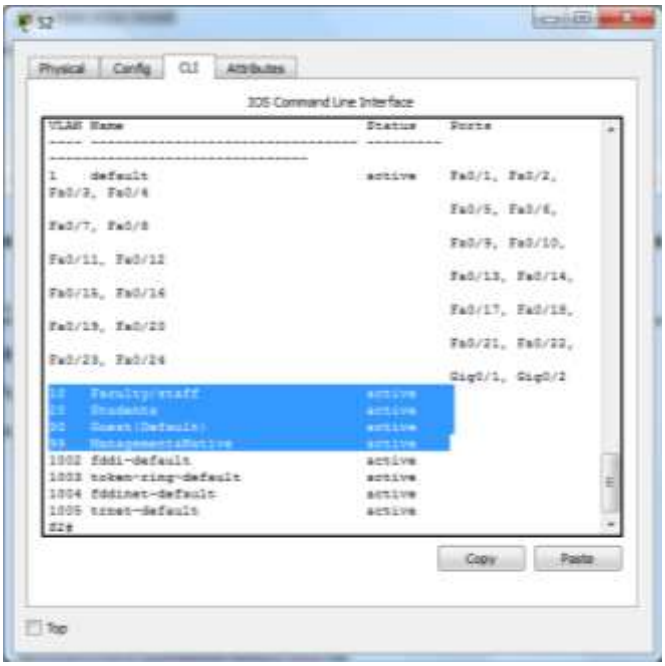


VLANs S3

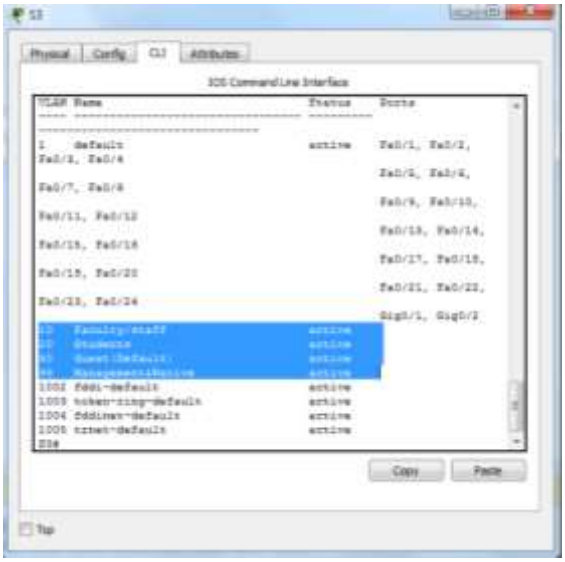


Step 4: Verify the VLAN configuration.

Verify the VLANs S2



Verify the VLANs S3



Part 3: Assign VLANs to Ports

Step 1: Assign VLANs to the active ports on S2.

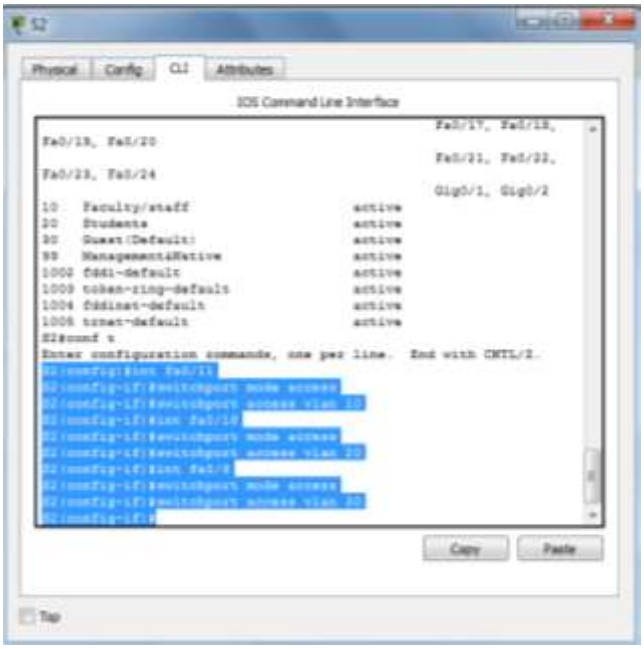
Assign the VLANs to the following ports:

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

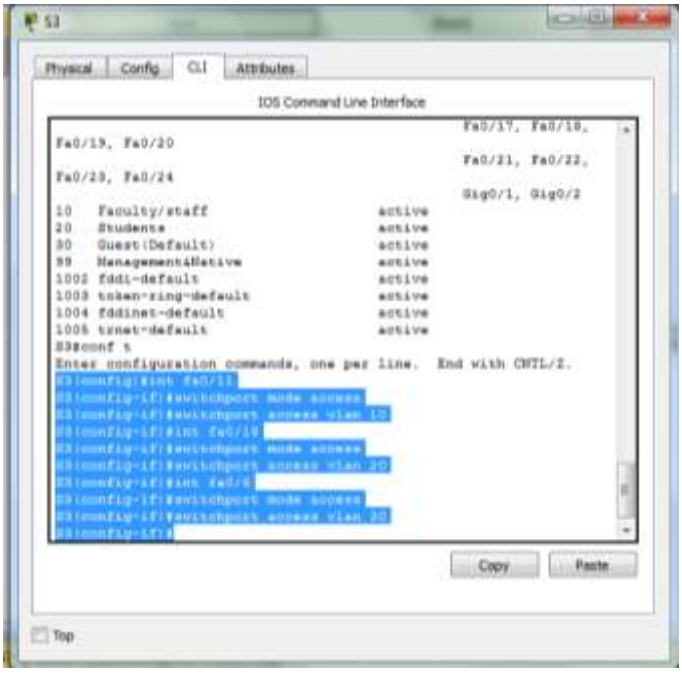
S2(config)# **interface fa0/11**

S2(config-if)# **switchport access vlan 10**

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



Step 2: Assign VLANs to the active ports on S3.
S3 uses the same VLAN access port assignments as S2.

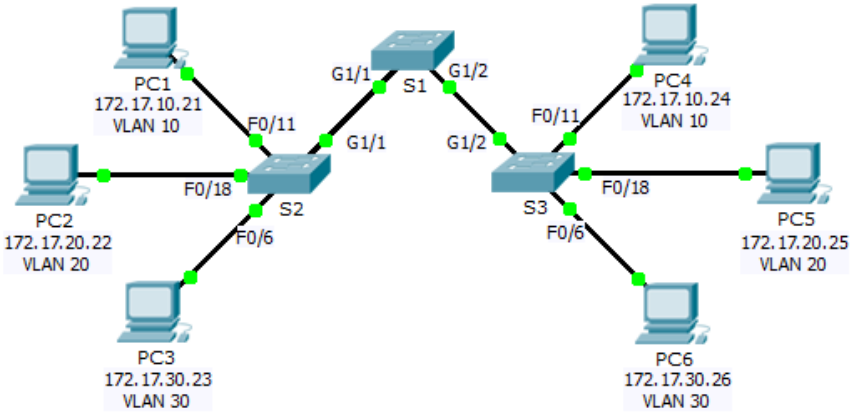


Step 3: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why?
No, the pings failed because the ports between the switches are in VLAN 1 and PC1 and PC4 are in VLAN 10.
What could be done to resolve this issue? Configure the ports between the switches as trunk ports.

3.2.2.4 Packet Tracer – Configuring Trunks

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Objectives

Part 1: Verify VLANs

Part 2: Configure Trunks

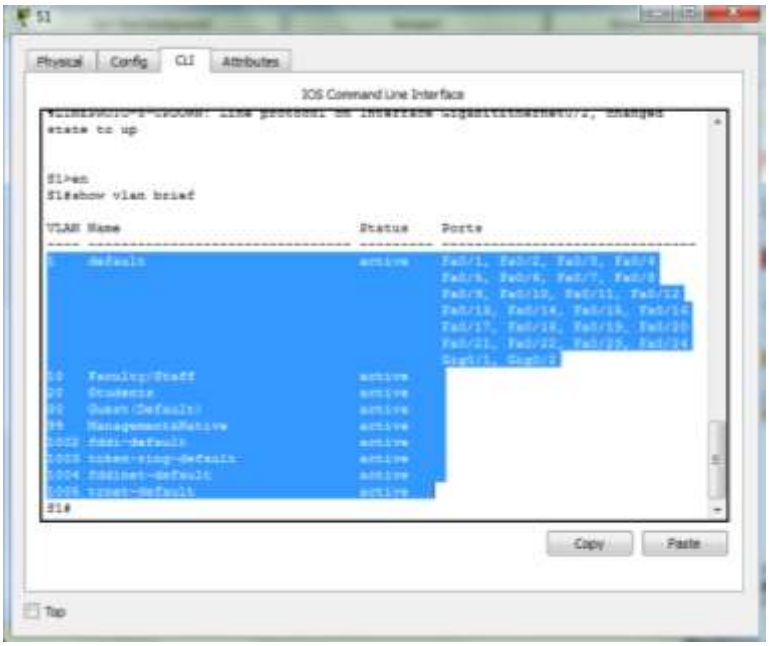
Background

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports, and assigning them to a native VLAN other than the default.

Part 1: Verify VLANs

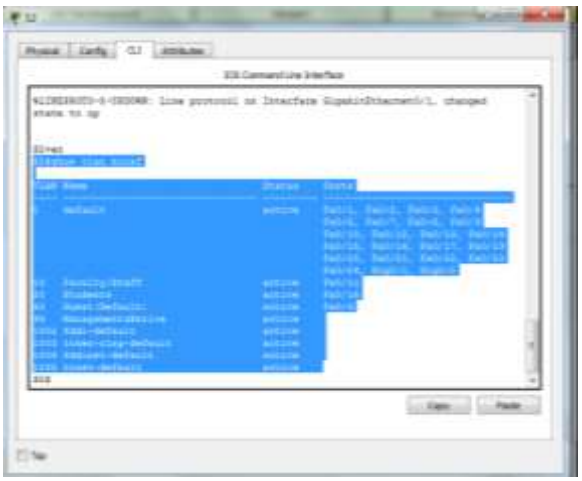
Step 1: Display the current VLANs.

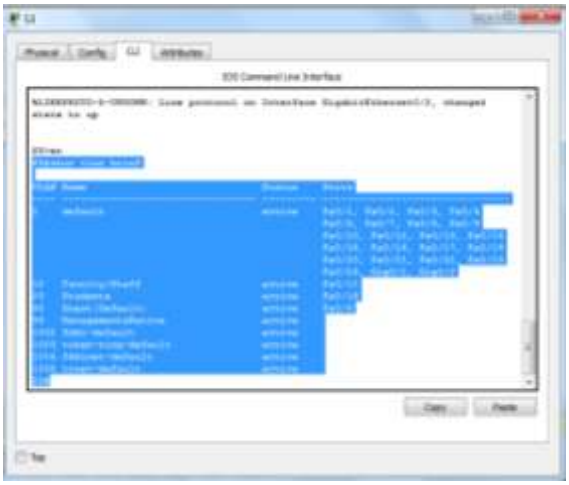
a. On **S1**, issue the command that will display all VLANs configured. There should be 9 VLANs in total. Notice how all 26 ports on the switch are assigned to one port or another.



b. On **S2** and **S3**, display and verify all the VLANs are configure and assigned to the correct switch ports according to the **Addressing Table**.

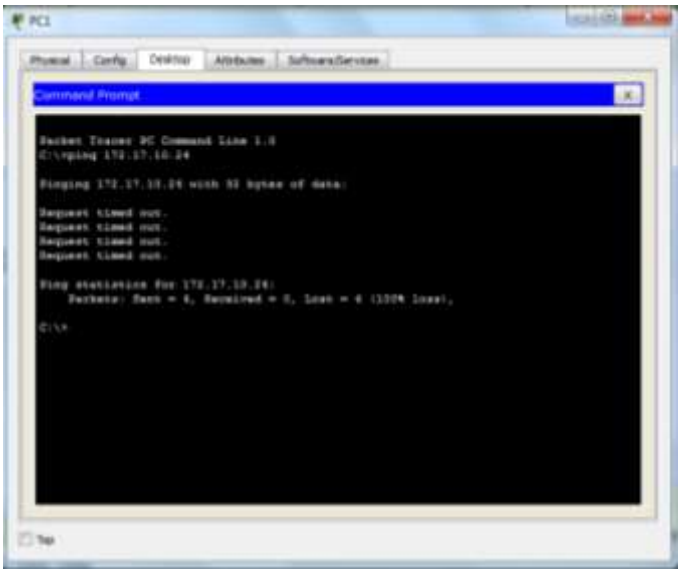
S2 **S3**





Step 2: Verify loss of connectivity between PCs on the same network.

Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

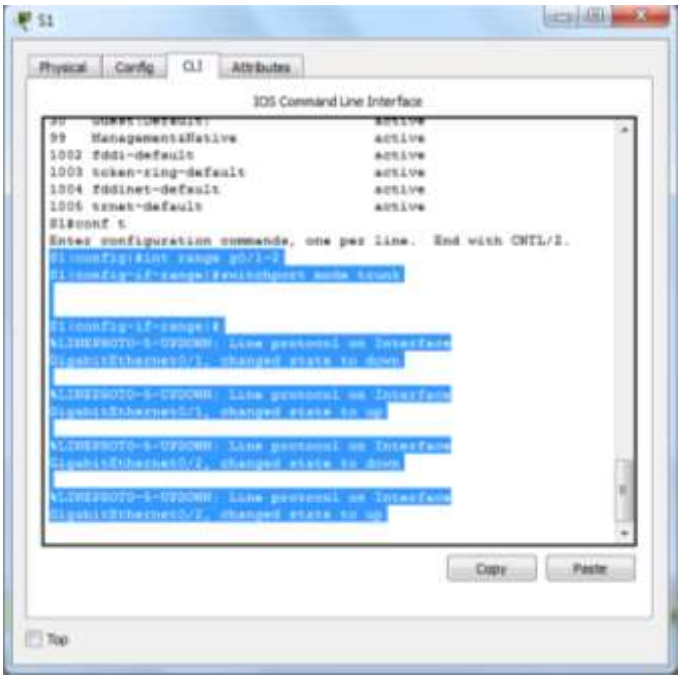


Part 2: Configure Trunks

Step 1: Configure trunking on S1 and use VLAN 99 as the native VLAN.

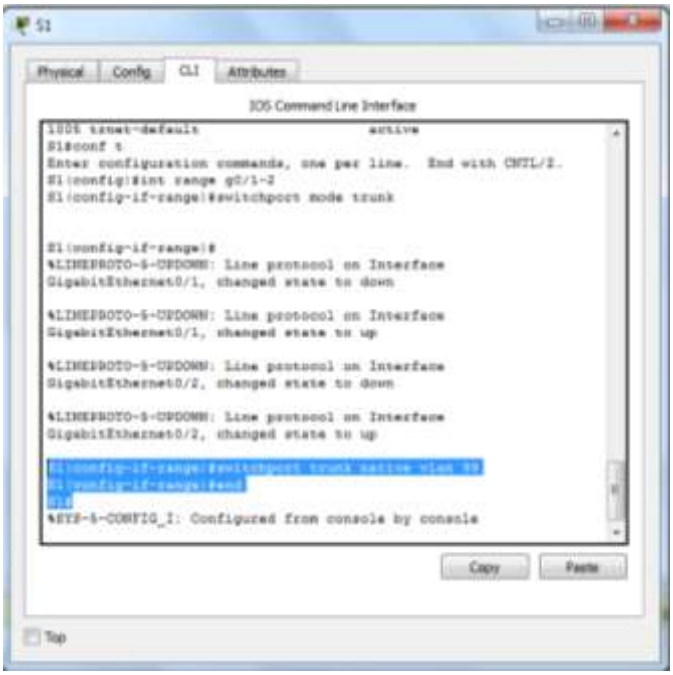
a. Configure G0/1 and G0/2 interfaces on S1 for trunking.

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



b. Configure VLAN 99 as the native VLAN for G1/1 and G1/2 interfaces on **S1**.

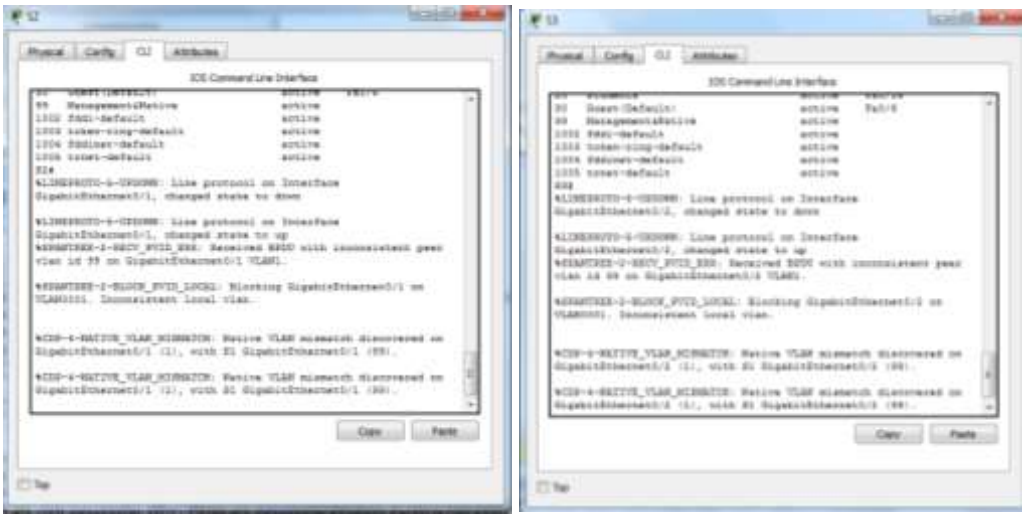
S1(config-if)# **switchport trunk native vlan 99**



The trunk port takes about a minute to become active due to Spanning Tree which you will learn in the proceeding chapters. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

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

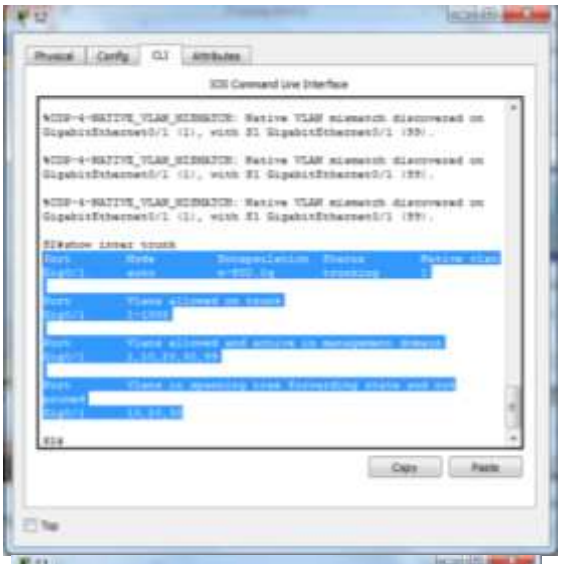
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(99), with S2 GigabitEthernet0/1 (1).

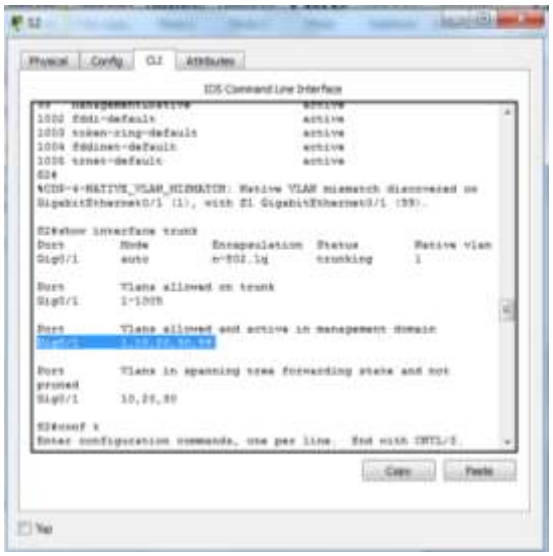


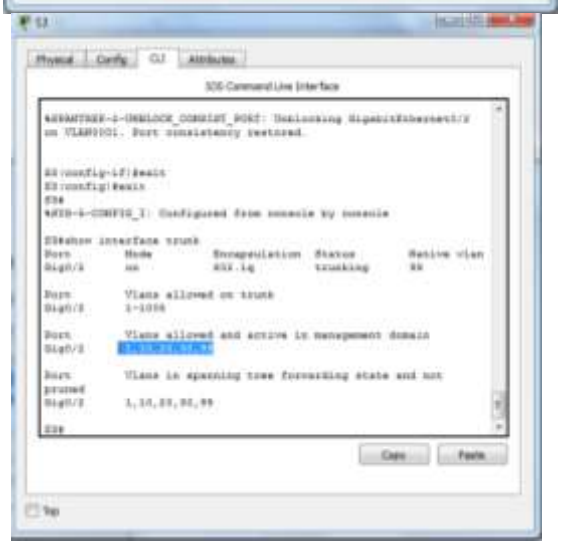
You configured VLAN 99 as the native VLAN on S1. However, the S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.
Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why? Pings are successful because trunking has been enabled on S1. Dynamic Trunking Protocol (DTP) has automatically negotiated the other side of the trunk links. In this case, S2 and S3 have now automatically configured the ports attached to S1 as trunking ports.

Step 2: Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.
Which active VLANs are allowed to across the trunk? 1, 10, 20, 30, and 99.

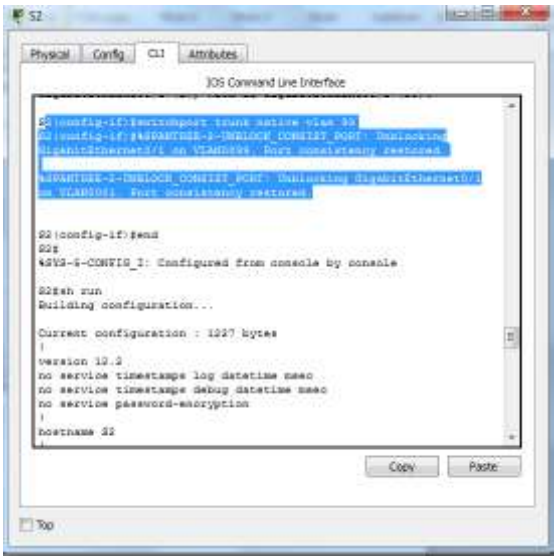


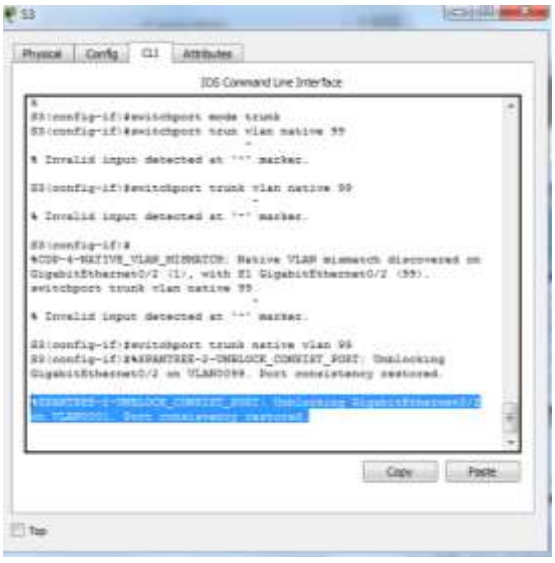




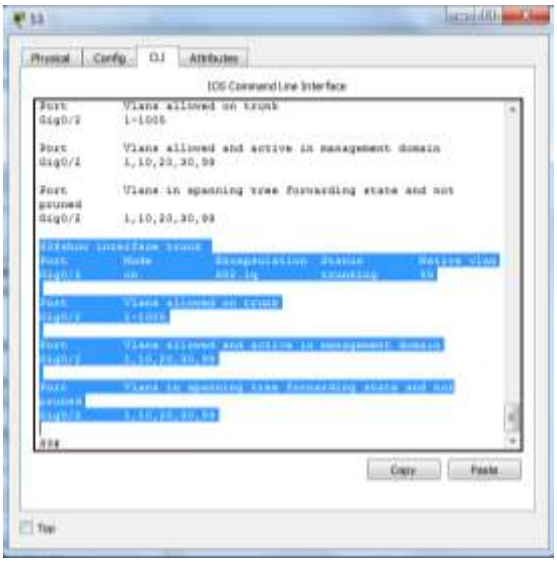
Step 3: Correct the native VLAN mismatch on S2 and S3.

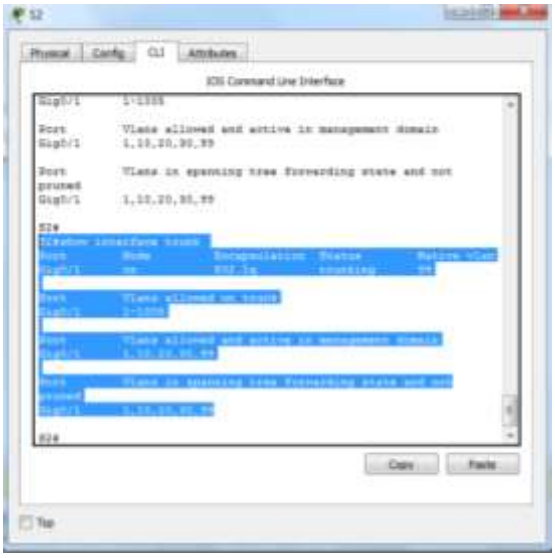
a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.





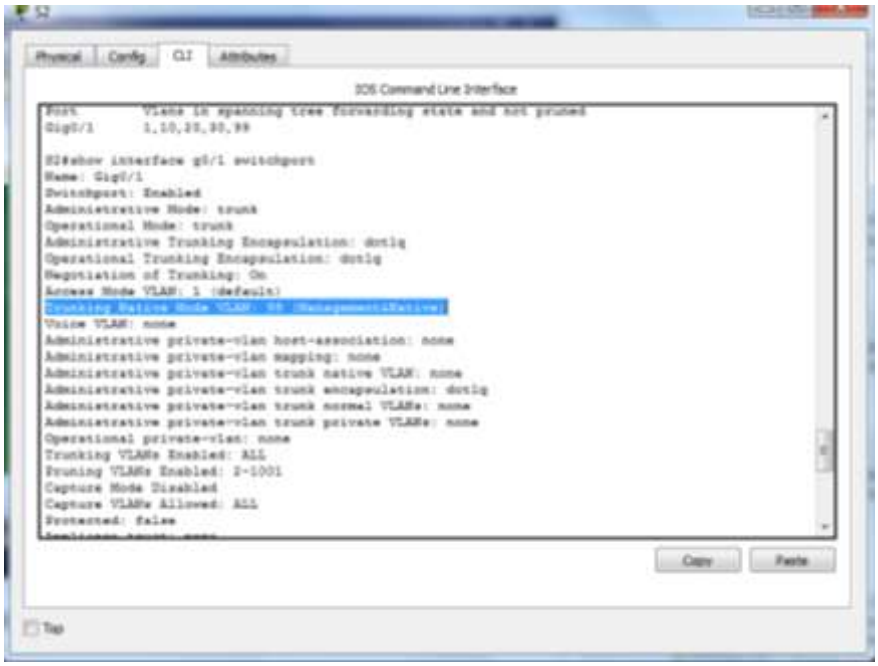
b. Issue **show interface trunk** command to verify the correct native VLAN configuration.

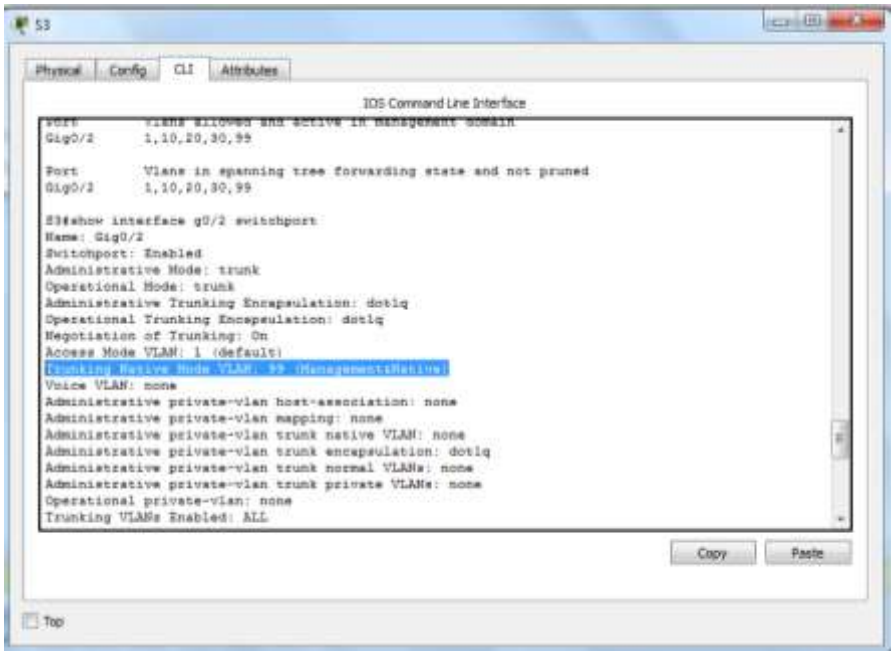




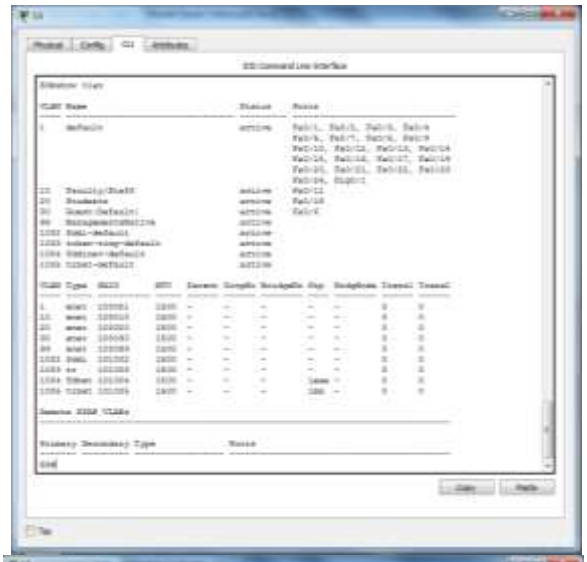
Step 4: Verify configurations on S2 and S3.

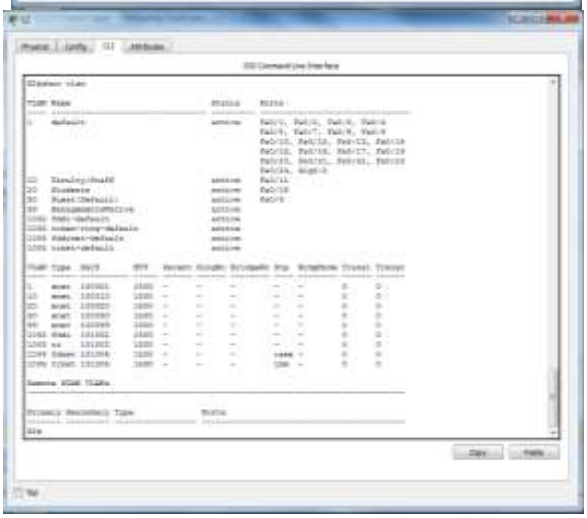
a. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.



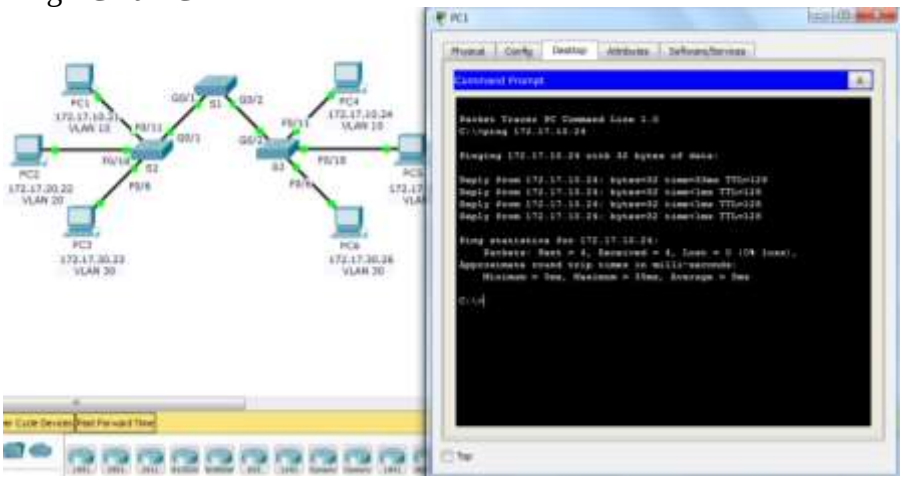


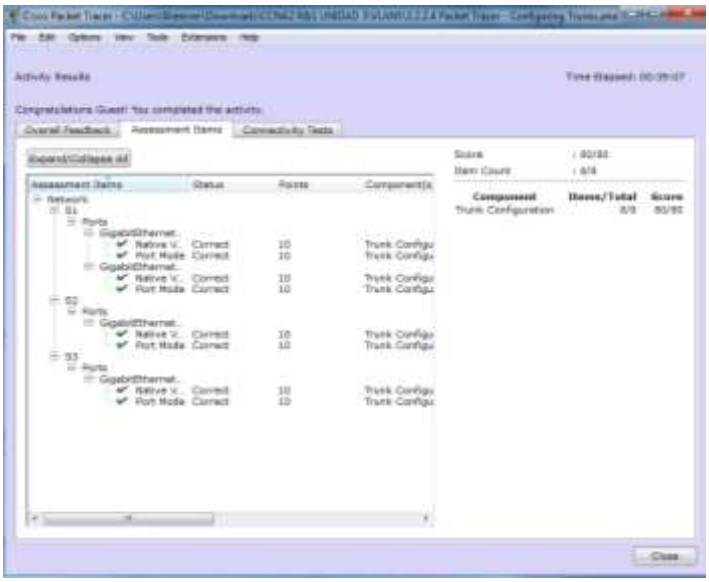
b. Use the **show vlan** command to display information regarding configured VLANs. Why is port G0/1 on S2 no longer assigned to VLAN 1? Port G0/1 is a trunk port and trunks ports are not displayed.





Ping PC1 a PC4





3.2.2.5 Práctica de laboratorio: configuración de redes VLAN y enlaces troncales

Topología

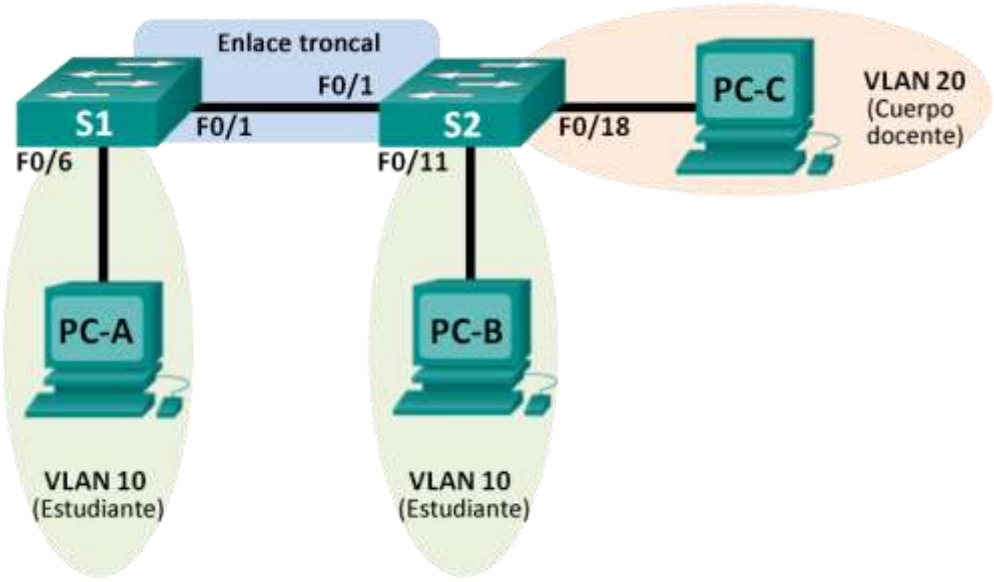


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objetivos

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

Parte 2: Crear redes VLAN y asignar puertos de switch

Parte 3: Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

Parte 4: Configurar un enlace troncal 802.1Q entre los switches

Parte 5: Eliminar la base de datos de VLAN

Información básica/situación

Los switches modernos usan redes de área local virtuales (VLAN) para mejorar el rendimiento de la red mediante la división de grandes dominios de difusión de capa 2 en otros más pequeños. Las VLAN también se pueden usar como medida de seguridad al controlar qué hosts se pueden comunicar. Por lo general, las redes VLAN facilitan el diseño de una red para respaldar los objetivos de una organización.

Los enlaces troncales de VLAN se usan para abarcar redes VLAN a través de varios dispositivos. Los enlaces troncales permiten transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN.

En esta práctica de laboratorio, creará redes VLAN en los dos switches de la topología, asignará las VLAN a los puertos de acceso de los switches, verificará que las VLAN funcionen como se espera y, a continuación, creará un enlace troncal de VLAN entre los dos switches para permitir que los hosts en la misma VLAN se comuniquen a través del enlace troncal, independientemente del switch al que está conectado el host.

Nota: Los switches que se utilizan 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

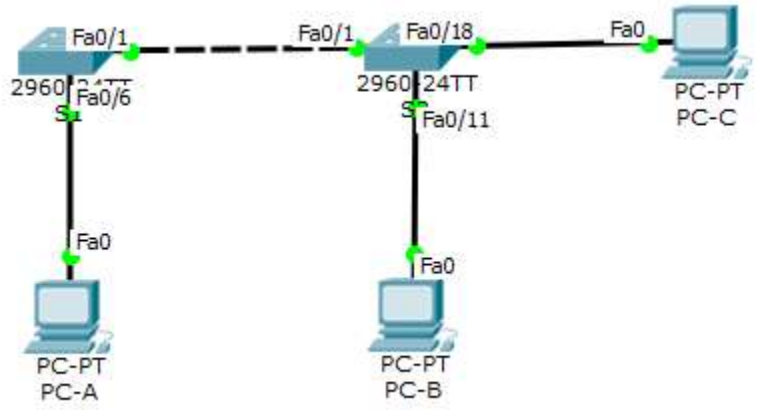
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 5. Armar la red y configurar los parámetros básicos de los dispositivos

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

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

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



Paso 2. Inicializar y volver a cargar los switches según sea necesario.

Paso 3. Configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

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

d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

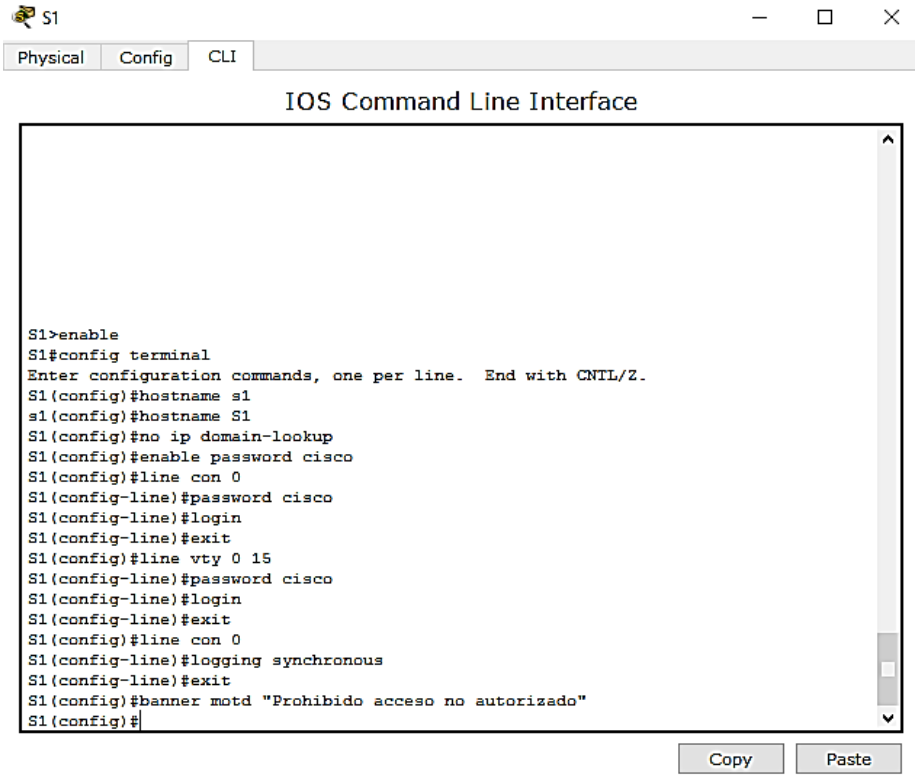
e. Configure **logging synchronous** para la línea de consola.

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

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

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

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




```
S1>enable
Password:
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password class
S1(config)#
```

```
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#int range fa0/2-5, fa0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

S2

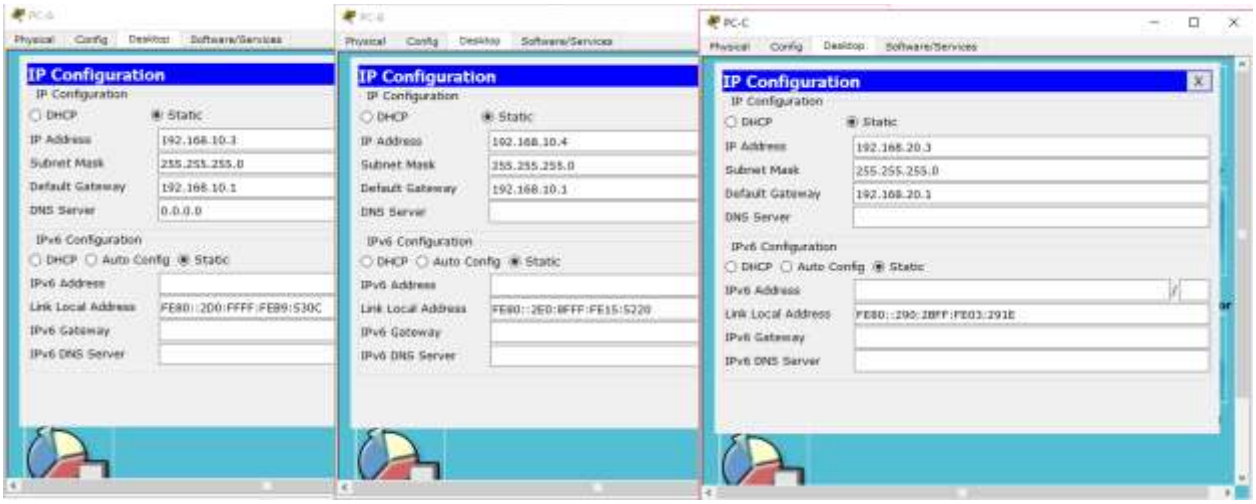
```
S2>enable
S2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable password class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#banner motd "Prohibido acceso no autorizado"

S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

```
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.1.12 255.255.255.0
S2(config-if)#no sh

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#
```

```
S2(config)#int range fa0/2-10, fa0/12-17, fa0/19-24, g0/1-2
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down

%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
```

Paso 4. Configurar los equipos host.

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



Paso 5. Probar la conectividad.

Verifique que los equipos host puedan hacer ping entre sí.

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

¿Se puede hacer ping de la PC-A a la PC-B? ____si_____

¿Se puede hacer ping de la PC-A a la PC-C? ____no_____

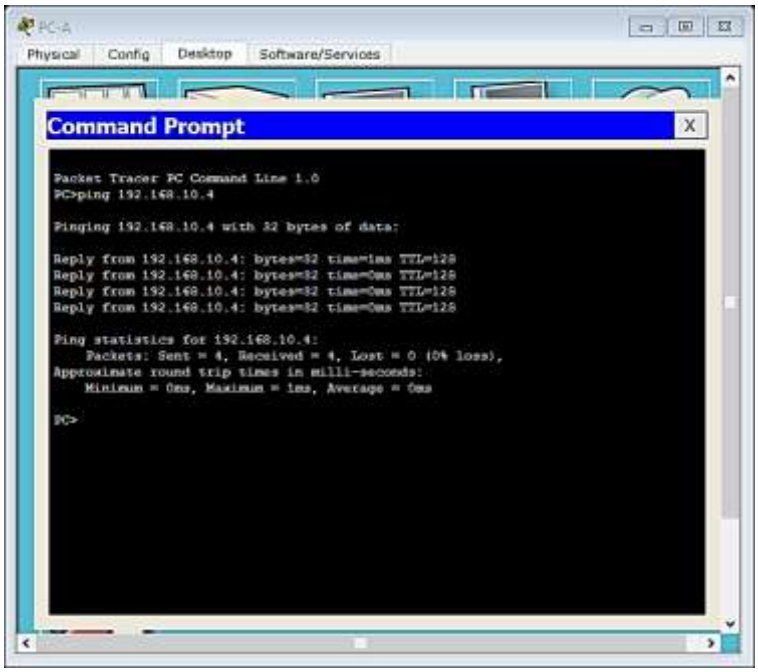
¿Se puede hacer ping de la PC-A al S1? ____no_____

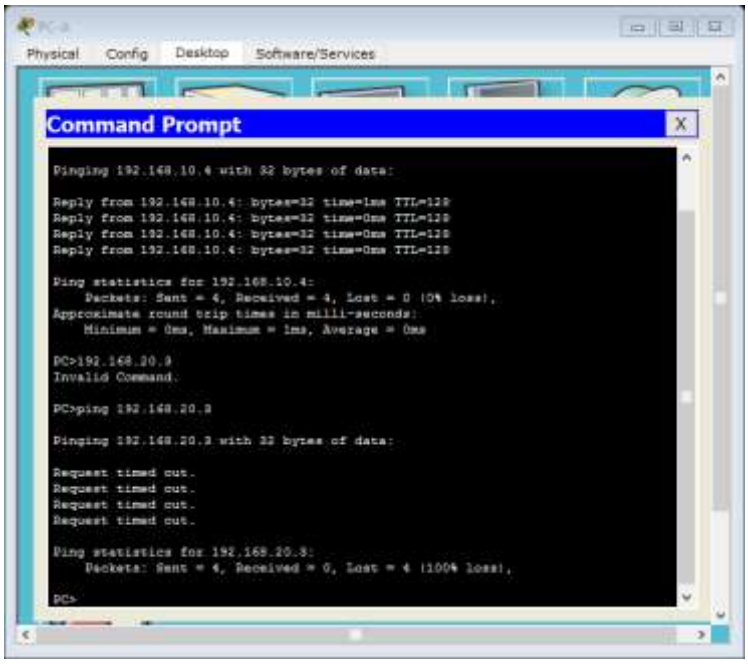
¿Se puede hacer ping de la PC-B a la PC-C? ____no_____

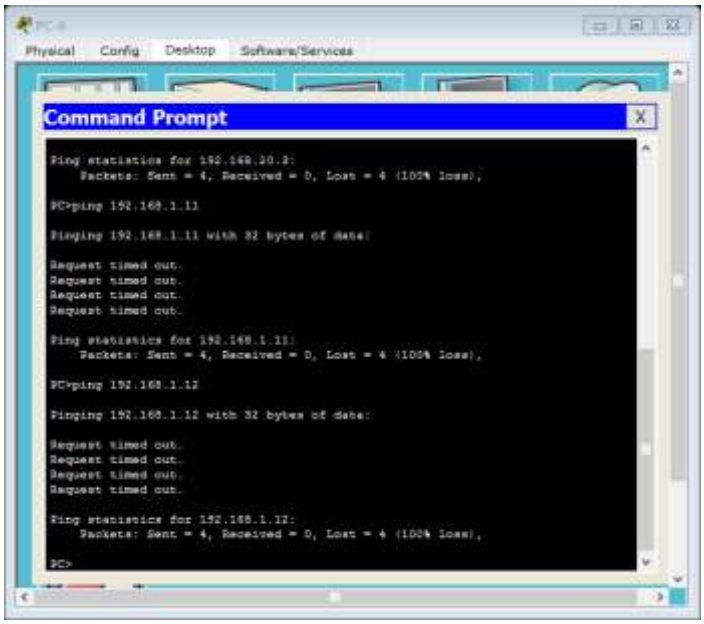
¿Se puede hacer ping de la PC-B al S2? ____no_____

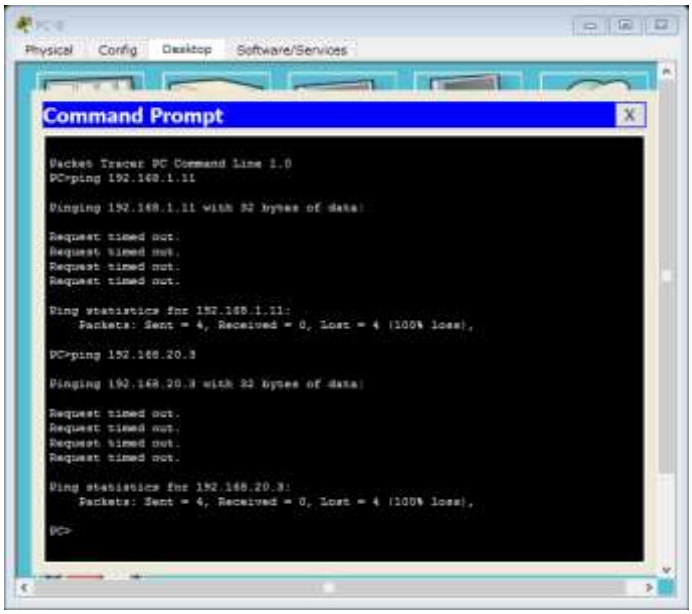
¿Se puede hacer ping de la PC-C al S2? ____no_____

¿Se puede hacer ping del S1 al S2? ____si_____

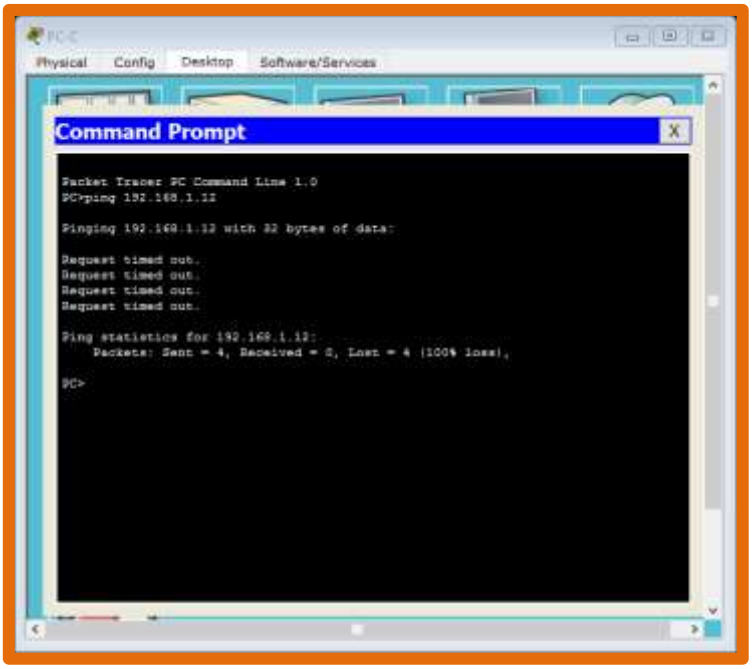

PC-A
Physical
Config
Desktop
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.4
Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.10.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>


Physical
Config
Desktop
Software/Services
Command Prompt
X
Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Reply from 192.168.10.4: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.10.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>192.168.20.3
Invalid Command.
PC>ping 192.168.20.3
Pinging 192.168.20.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.20.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>






```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

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

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```




```
S1#ping 192.168.1.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.1.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

Parte 6. Crear redes VLAN y asignar puertos de switch

En la parte 2, creará redes VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

Paso 1. Crear las VLAN en los switches.

a. Cree las VLAN en S1.

S1(config)# **vlan 10**
S1(config-vlan)# **name Student**
S1(config-vlan)# **vlan 20**
S1(config-vlan)# **name Faculty**
S1(config-vlan)# **vlan 99**
S1(config-vlan)# **name Management**
S1(config-vlan)# **end**

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Student
S1(config-vlan)#vlan 20
S1(config-vlan)#name Faculty
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

b. Cree las mismas VLAN en el S2.

```
S2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Student
S2(config-vlan)#vlan 20
S2(config-vlan)#name Faculty
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management
S2(config-vlan)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```

c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.

S1# **show vlan**

Physical Config CLI

IOS Command Line Interface

```
S2#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   Student                           active
20   Faculty                           active
99   Management                        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
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
------- --------- ----------------- ------------------------------------------
S2#
```

Copy Paste

¿Cuál es la VLAN predeterminada? ___**vlan 1**_____

¿Qué puertos se asignan a la VLAN predeterminada?

Todos los puertos

Paso 2. Asignar las VLAN a las interfaces del switch correctas.

a. Asigne las VLAN a las interfaces en el S1.

1) Asigne la PC-A a la VLAN Estudiantes.

S1(config)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 10**

2) Transfiera la dirección IP del switch a la VLAN 99.

S1(config)# **interface vlan 1**
S1(config-if)# **no ip address**
S1(config-if)# **interface vlan 99**
S1(config-if)# **ip address 192.168.1.11 255.255.255.0**
S1(config-if)# **end**

```
S1#confi terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#int vlan 1
S1(config-if)#no ip address
S1(config-if)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.1.11 255.
                                        ^
% Invalid input detected at '^' marker.

S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

b. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

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, Fa0/7, 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   Student                           active    Fa0/6
20   Faculty                           active
99   Management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

c. Emita el comando **show ip interface brief**.

```
FastEthernet0/24       unassigned      YES manual administratively down down

GigabitEthernet0/1     unassigned      YES manual administratively down down

GigabitEthernet0/2     unassigned      YES manual administratively down down

Vlan1                  unassigned      YES manual up                    up

Vlan99                 192.168.1.11    YES manual up                    down
S1#
```

¿Cuál es el estado de la VLAN 99? ¿Por qué?

Esta activo pero el protocolo esta desactivado pues no ha sido asignado aun puerto activo aun.

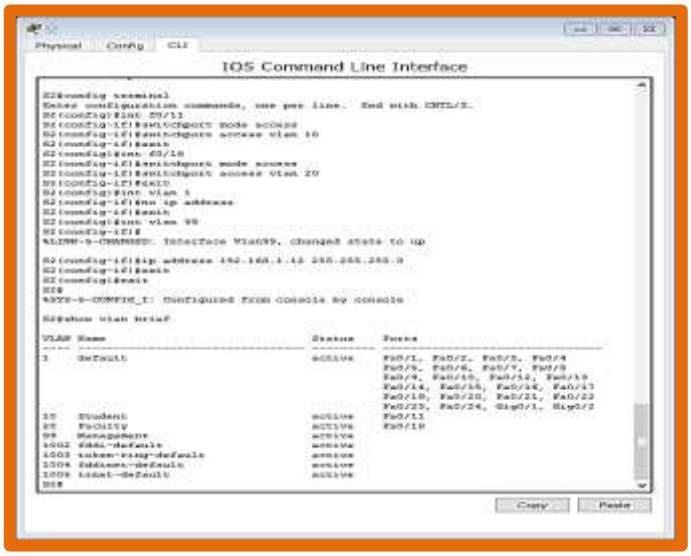
d. Use la topología para asignar las VLAN a los puertos correspondientes en el S2.

e. Elimine la dirección IP para la VLAN 1 en el S2.

f. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.

g. Use el comando **show vlan brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.

S2# **show vlan brief**



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

No porque la interface f0/1 no está signada a la vlan 10 por tanto no puede enviar datos por ese puerto

¿Es posible hacer ping del S1 al S2? ¿Por qué?

No porque las direcciones ip de los switches están asignadas a la vlan 99, por esto no puede enviar por la interface f0/1

Parte 7. Mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

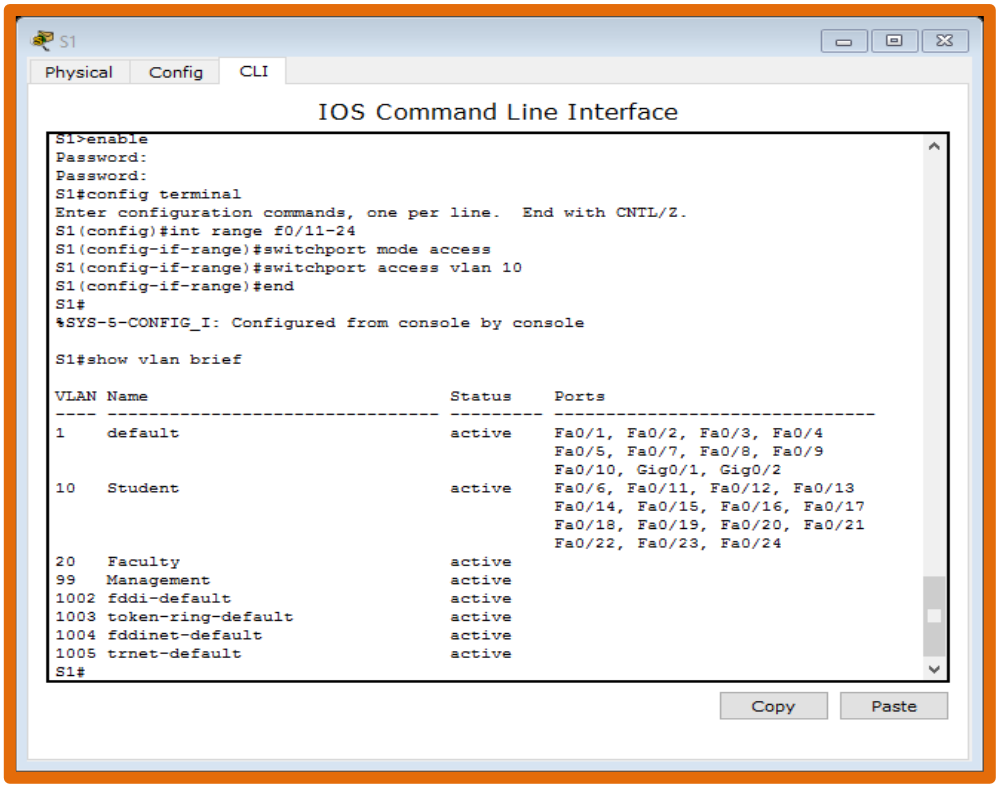
En la parte 3, cambiará las asignaciones de VLAN a los puertos y eliminará las VLAN de la base de datos de VLAN.

Paso 1. Asignar una VLAN a varias interfaces.

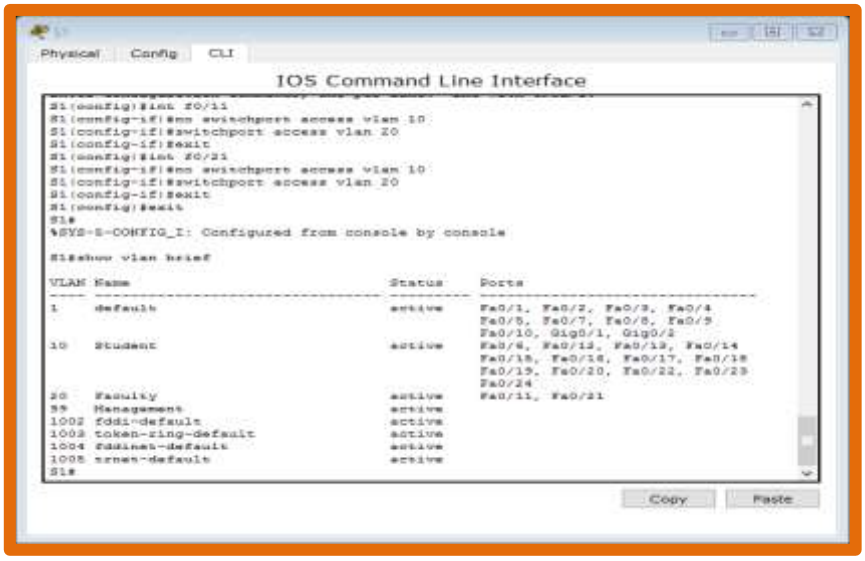
a. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 10.

S1(config)# **interface range f0/11-24**
S1(config-if-range)# **switchport mode access**
S1(config-if-range)# **switchport access vlan 10**
S1(config-if-range)# **end**

b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.



c. Reasigne F0/11 y F0/21 a la VLAN 20.



d. Verifique que las asignaciones de VLAN sean las correctas.

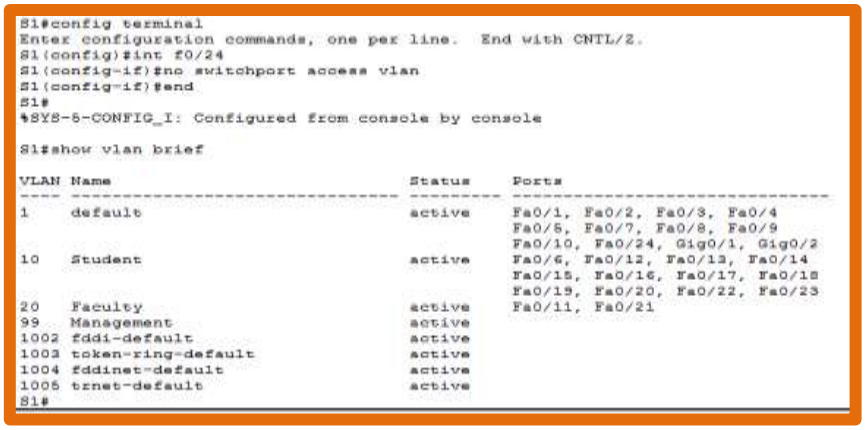
Paso 2. Eliminar una asignación de VLAN de una interfaz.

a. Use el comando **no switchport access vlan** para eliminar la asignación de la VLAN 10 a F0/24.

S1(config)# **interface f0/24**

S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**



b. Verifique que se haya realizado el cambio de VLAN.

¿A qué VLAN está asociada ahora F0/24?

Está asociada la interface f0/24 a la vlan 1.

Paso 3. Eliminar una ID de VLAN de la base de datos de VLAN.

a. Agregue la VLAN 30 a la interfaz F0/24 sin emitir el comando VLAN.

S1(config)# **interface f0/24**

S1(config-if)# **switchport access vlan 30**

% Access VLAN does not exist. Creating vlan 30

Nota: La tecnología de switches actual ya no requiere la emisión del comando **vlan** para agregar una VLAN a la base de datos. Al asignar una VLAN desconocida a un puerto, la VLAN se agrega a la base de datos de VLAN.

b. Verifique que la nueva VLAN se muestre en la tabla de VLAN.

S1# **show vlan brief**

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/24
S1(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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, Gig0/1, Gig0/2
10   Student                          active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
30   VLAN0030                         active    Fa0/24
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

¿Cuál es el nombre predeterminado de la VLAN 30?

____VLAN0030_____

___

c. Use el comando **no vlan 30** para eliminar la VLAN 30 de la base de datos de VLAN.

S1(config)# **no vlan 30**

S1(config)# **end**

d. Emita el comando **show vlan brief**. F0/24 se asignó a la VLAN 30.

Una vez que se elimina la VLAN 30, ¿a qué VLAN se asigna el puerto F0/24? ¿Qué sucede con el tráfico destinado al host conectado a F0/24?

La interface no está asignada a ninguna vlan, por lo tanto no podrá transferir ningún tráfico.

S1# **show vlan brief**

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no vlan 30
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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, Gig0/1, Gig0/2
10   Student                           active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
99   Management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

e. Emita el comando **no switchport access vlan** en la interfaz F0/24.

f. Emita el comando **show vlan brief** para determinar la asignación de VLAN para F0/24. ¿A qué VLAN se asignó F0/24?

___vlan 1_____

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/24
S1(config-if)#no switchport access vlan
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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, Fa0/24, Gig0/1, Gig0/2
10   Student                           active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
99   Management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Nota: Antes de eliminar una VLAN de la base de datos, se recomienda reasignar todos los puertos asignados a esa VLAN.

¿Por qué debe reasignar un puerto a otra VLAN antes de eliminar la VLAN de la base de datos de VLAN?

La interface queda deshabilitada hasta que se reasigne, lo que puede ocasionar perdida de información y traumatismos en la red.

Parte 8. Configurar un enlace troncal 802.1Q entre los switches

En la parte 4, configurará la interfaz F0/1 para que use el protocolo de enlace troncal dinámico (DTP) y permitir que negocie el modo de enlace troncal. Después de lograr y

verificar esto, desactivará DTP en la interfaz F0/1 y la configurará manualmente como enlace troncal.

Paso 1. Usar DTP para iniciar el enlace troncal en F0/1.

El modo de DTP predeterminado de un puerto en un switch 2960 es dinámico automático. Esto permite que la interfaz convierta el enlace en un enlace troncal si la interfaz vecina se establece en modo de enlace troncal o dinámico deseado.

a. Establezca F0/1 en el S1 en modo de enlace troncal.

```
S1>enable
Password:
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport mode dynamic desirable

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#
```

b. Emita el comando **show vlan brief** en el S1 y el S2. La interfaz F0/1 ya no está asignada a la VLAN 1. Las interfaces de enlace troncal no se incluyen en la tabla de VLAN.

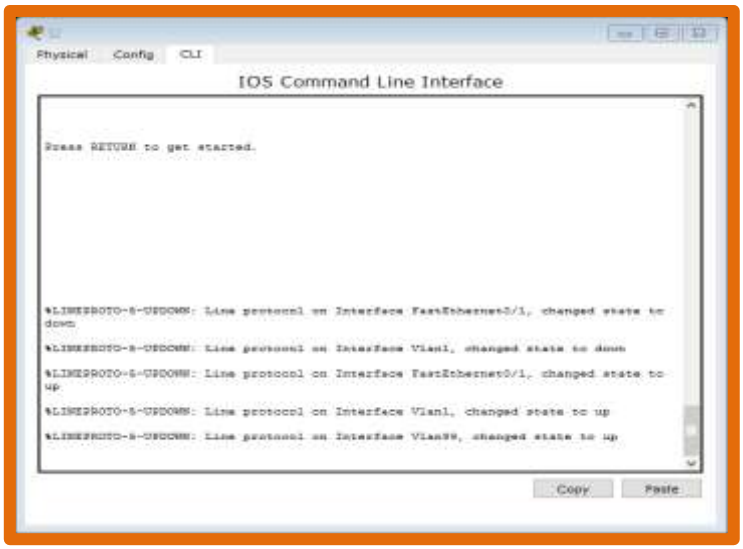
S1# **show vlan brief**

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/24, Gig0/1, Gig0/2
10   Student                          active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

c. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

S1# **show interfaces trunk**

```
S1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```



S2# **show interfaces trunk**

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S2#
```

Nota: De manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

d. Verifique que el tráfico de VLAN se transfiera a través de la interfaz de enlace troncal F0/1.

¿Se puede hacer ping del S1 al S2? ___si_____

¿Se puede hacer ping de la PC-A a la PC-B? ___si_____

¿Se puede hacer ping de la PC-A a la PC-C? ___no_____

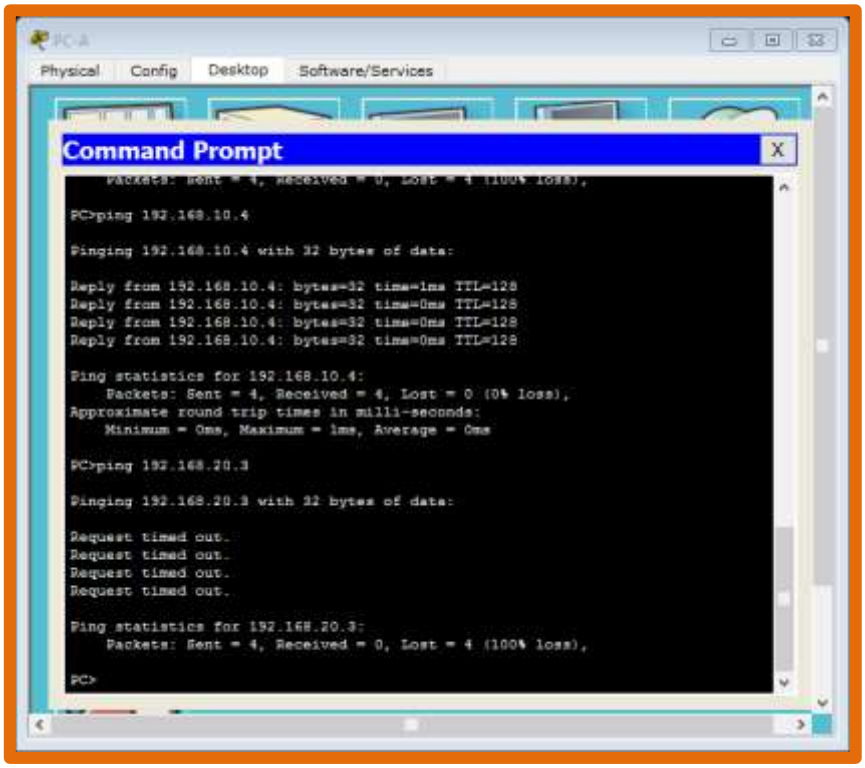
¿Se puede hacer ping de la PC-B a la PC-C? ____no_____

¿Se puede hacer ping de la PC-A al S1? _____no_____

¿Se puede hacer ping de la PC-B al S2? _____no_____

¿Se puede hacer ping de la PC-C al S2? _____no_____

```
S1#ping 192.168.1.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```



Si la respuesta a cualquiera de las preguntas anteriores es no, justifíquela a continuación.

PC-C está en una VLAN diferente a PC-A y PC-B. igualmente S1 Y S2 están en unas VLAN diferente a las de PC´S.

Paso 2. Configurar manualmente la interfaz de enlace troncal F0/1.

El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

a. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switches.

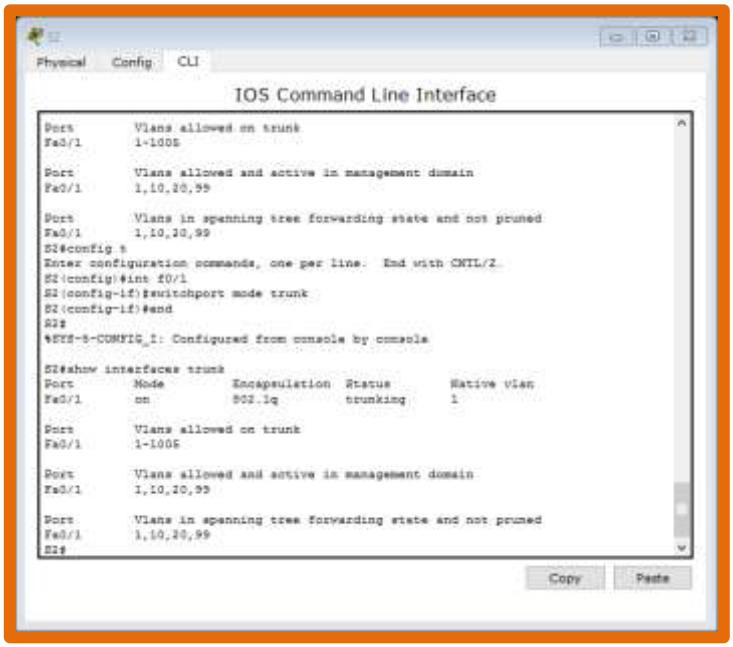
S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

b. Emita el comando **show interfaces trunk** para ver el modo de enlace troncal. Observe que el modo cambió de **desirable** a **on**.

S2# **show interfaces trunk**

```
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces 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       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```



¿Por qué desearía configurar una interfaz en modo de enlace troncal de forma manual en lugar de usar DTP?

NO todos los equipos usan DTP por lo que configurarlo manualmente brinda mayor confiabilidad.

Parte 9. Eliminar la base de datos de VLAN

En la parte 5, eliminará la base de datos de VLAN del switch. Es necesario hacer esto al inicializar un switch para que vuelva a la configuración predeterminada.

Paso 1. Determinar si existe la base de datos de VLAN.

Emita el comando **show flash** para determinar si existe el archivo **vlan.dat** en la memoria flash.

S1# **show flash**

```
S1#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-         736          <no date>  vlan.dat

64016384 bytes total (59600727 bytes free)
S1#
```

Nota: Si hay un archivo **vlan.dat** en la memoria flash, la base de datos de VLAN no contiene la configuración predeterminada.

Paso 2. Eliminar la base de datos de VLAN.

a. Emita el comando **delete vlan.dat** para eliminar el archivo vlan.dat de la memoria flash y restablecer la base de datos de VLAN a la configuración predeterminada. Se le solicitará dos veces que confirme que desea eliminar el archivo vlan.dat. Presione Enter ambas veces.

S1# delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

S1#

b. Emita el comando **show flash** para verificar que se haya eliminado el archivo vlan.dat.

S1# **show flash**

```
S1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

S1#show flash
Directory of flash:/

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

64016384 bytes total (59601463 bytes free)
S1#
```

Para inicializar un switch para que vuelva a la configuración predeterminada, ¿cuáles son los otros comandos que se necesitan?

Erase startup-config

Reload

Delete vlan.dat

Reflexión

1. ¿Qué se necesita para permitir que los hosts en la VLAN 10 se comuniquen con los hosts en la VLAN 20?

Es necesario un equipo de capa 3 como un switch o un router.

2. ¿Cuáles son algunos de los beneficios principales que una organización puede obtener mediante el uso eficaz de las VLAN?

   - **Se ahorran costos**
   - **Se mejora la seguridad**
   - **Se mejora el rendimiento**

3.3.2.2Práctica de laboratorio: implementación de seguridad de VLAN

Topología

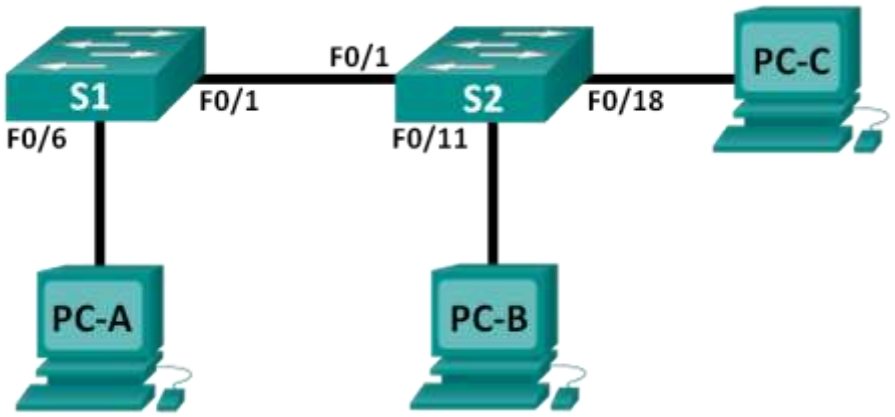


Tabla de direccionamiento

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.

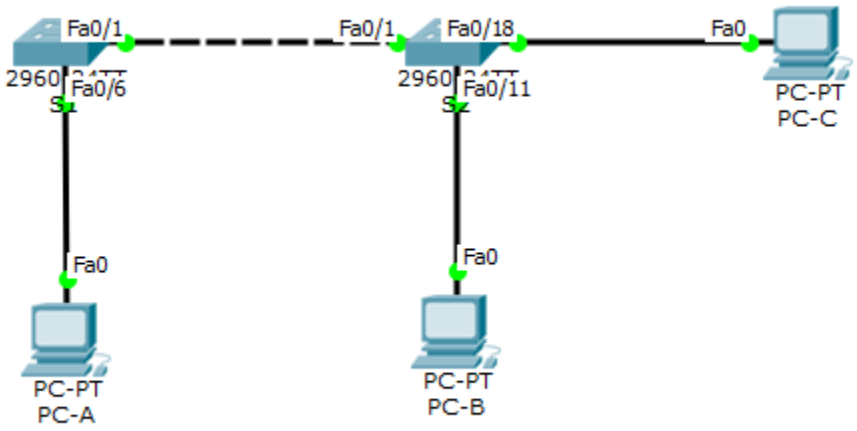
Recursos necesarios

- 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 10. 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.

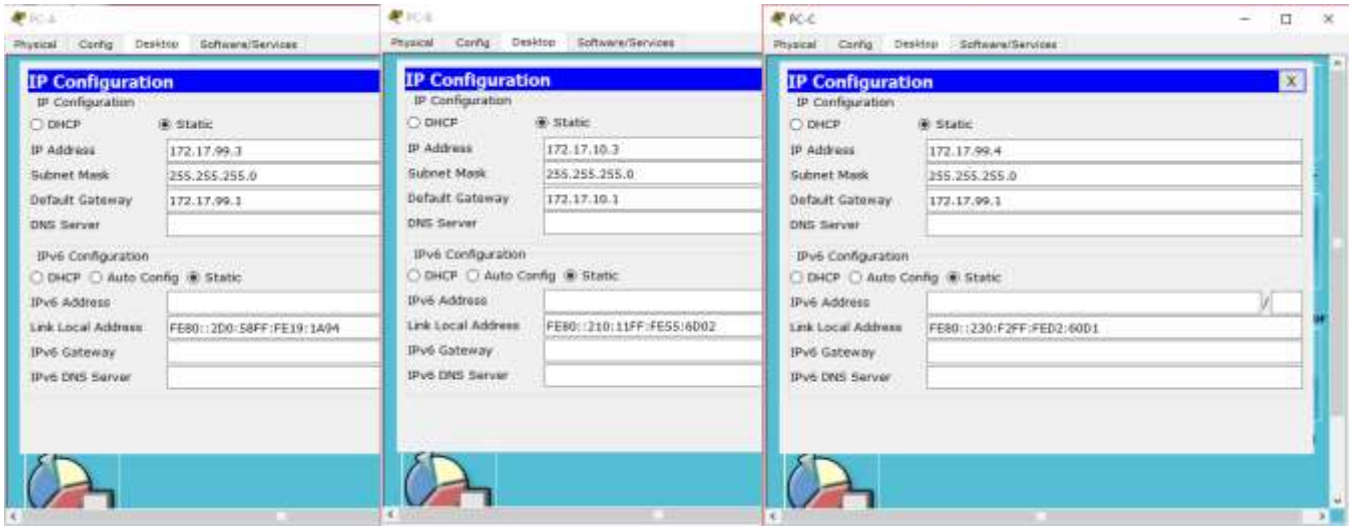
Paso 1. Realizar el cableado de red tal como se muestra en la topología.



Paso 2. Inicializar y volver a cargar los switches.

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.

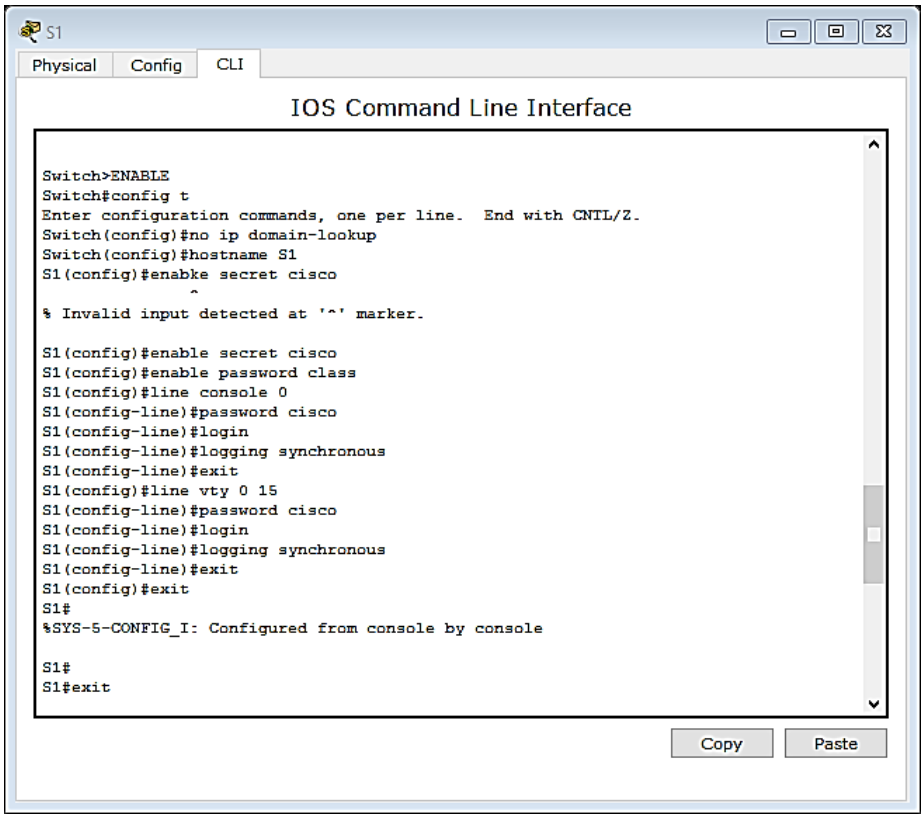
a. Desactive la búsqueda del DNS.

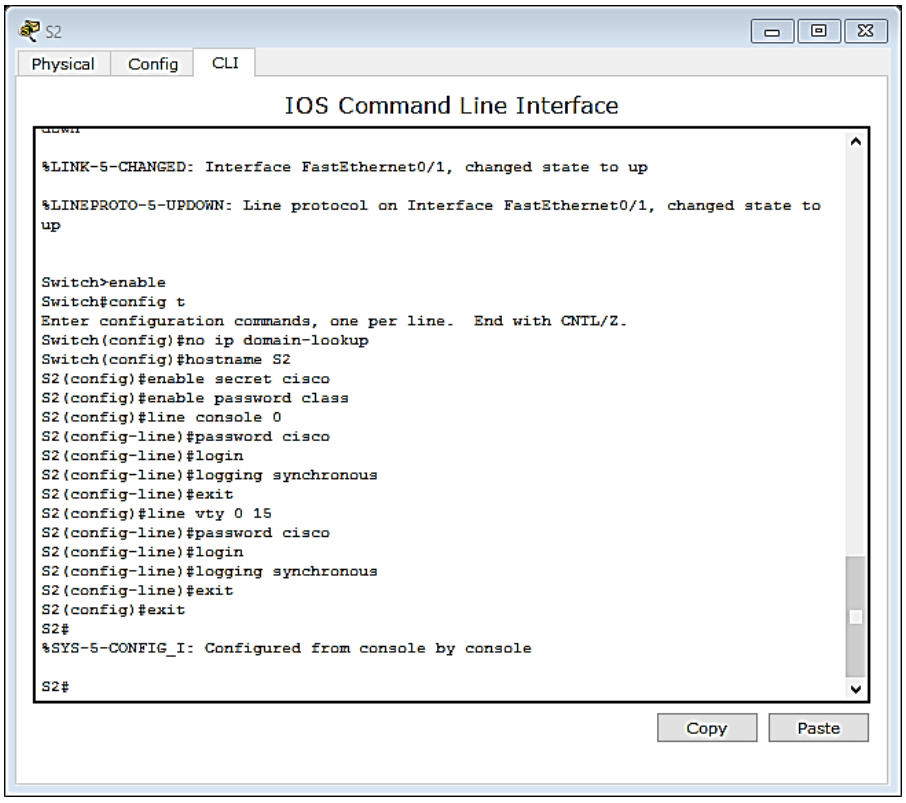
b. Configure los nombres de los dispositivos como se muestra en la topología.

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.





Paso 5. Configurar las VLAN en cada switch.

a. Cree las VLAN y asígneles nombres según la tabla de asignaciones de VLAN.


```
User Access Verification

Password:

S2>enable
Password:
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Datos
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management&Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name BlackHole
S2(config-vlan)#
```

b. Configure la dirección IP que se indica para la VLAN 99 en la tabla de direccionamiento en ambos switches.

```
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#exit
S1(config)#ip default-gateway 172.17.99.1
S1(config)#
```

```
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 sh
S2(config-if)#exit
S2(config)#ip default-gateway 172.17.99.1
S2(config)#
```

c. Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.

```
S1(config)#int fa0/6
S1(config-if)#switchport mode access
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)#int fa0/11
S2(config-if)#switchport mode access
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-if)#int fa0/18
S2(config-if)#switchport mode access
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.

```
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   Datos                            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?

En 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.

```
S1(config)#banner motd "ACCESO NO AUTORIZADO ESTA PROHIBIDO"
```

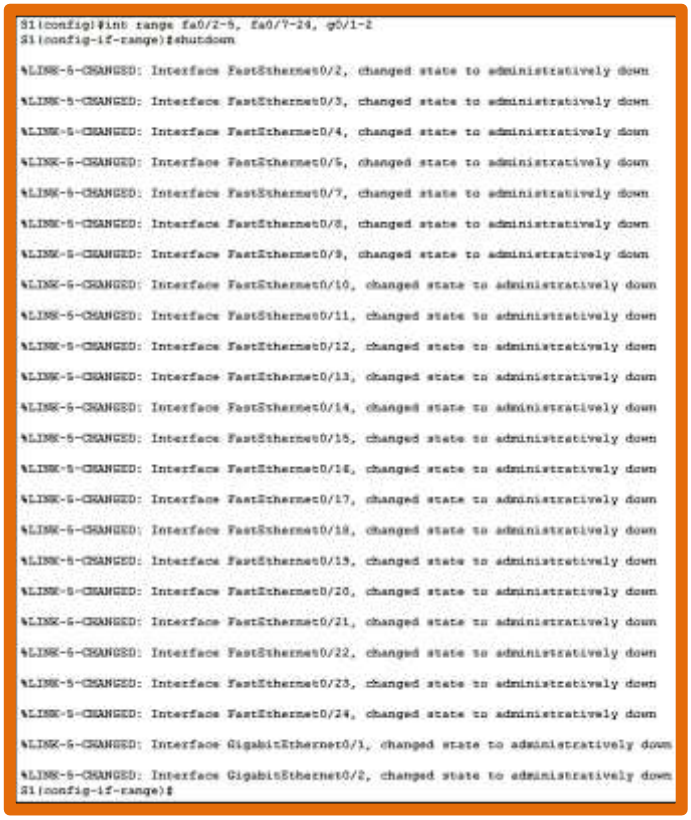
```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#banner motd "ACCESO NO AUTORIZADO ESTA PROHIBIDO"
S2(config)#
```

b. Encripte todas las contraseñas.

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

```
S2(config)#service password-encryption
S2(config)#
```

c. Desactive todos los puertos físicos sin utilizar.



d. Deshabilite el servicio web básico en ejecución.

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

```
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.
```

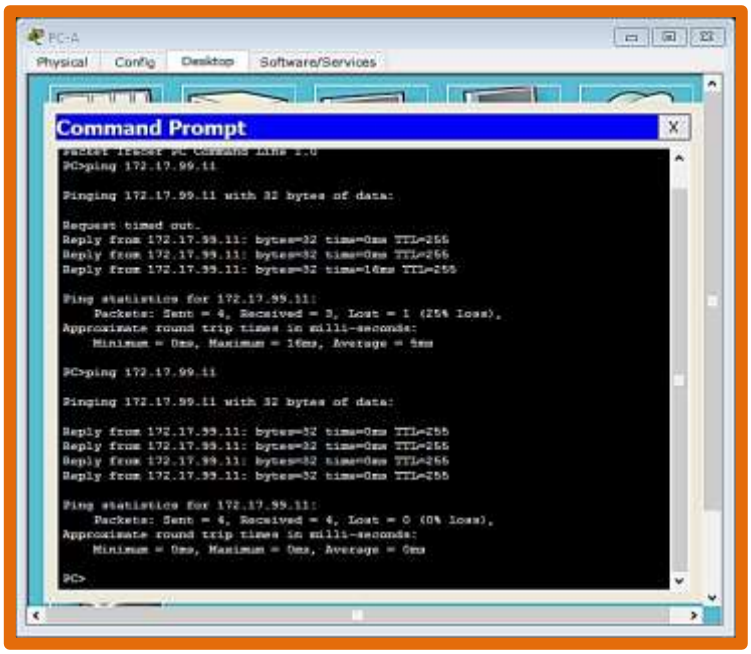
e. Copie la configuración en ejecución en la configuración de inicio.

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

```
S2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

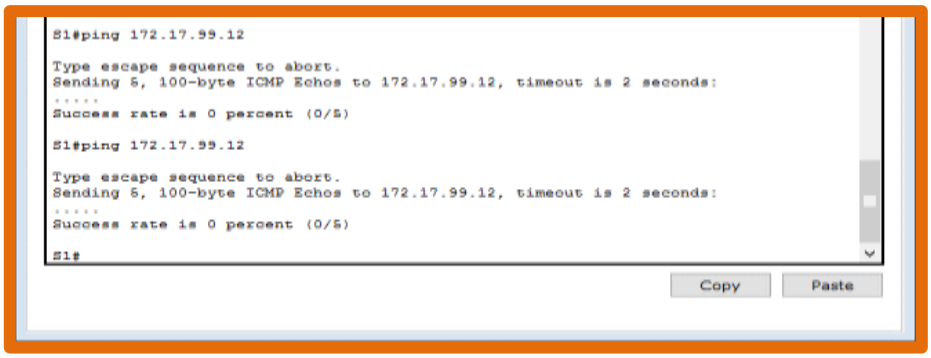
Paso 7. Verificar la conectividad entre la información de VLAN y los dispositivos.

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?



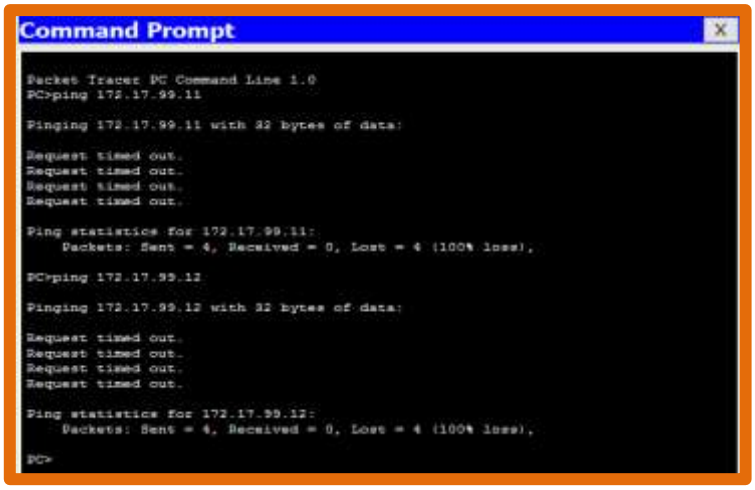
El comando ping es satisfactorio. El PC-A esta en la misma VLAN administrativa que el SWITCH.

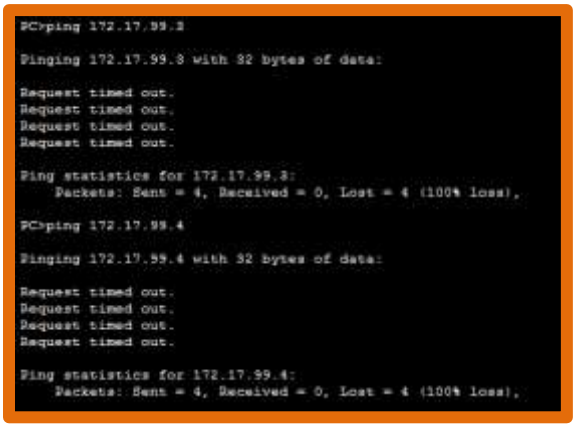
b. Desde el S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?



El PIN no es satisfactorio. Aunque las direcciones de S1 Y S2 están en la misma VLAN, las interfaces F0/1 no están configuradas como troncal.

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?





Todos los pin no se dan de manera satisfactoria. Porque PC-B está en la VLAN 10 y el resto está en la VLAN 99.

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

PC>
```

Es posible hacer PIN a S2 pero no a S1. Aunque están en la misma VLAN PC-C no es capaz de hacer PIN con S1, pues el enlace troncal entre S1 Y S2 no está activo.

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

Parte 11. Implementar seguridad de VLAN en los switches

Paso 1. Configurar puertos de enlace troncal en el S1 y el S2.

a. 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)#int f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

S1(config-if)#
```

b. 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 t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#
```

c. 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#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
S1#
```

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?

__VLAN 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**

```
S1(config)#int fa0/1
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
```

c. 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)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(99), with S2 FastEthernet0/1 (1).

S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(99), with S2 FastEthernet0/1 (1).

S1(config-if)#
```

__Este mensaje se presenta porque S1 Y S2 tienen VLAN distintas.____

d. 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-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.


S2(config-if)#
```

e. Verifique que ahora la VLAN nativa sea la 99 en ambos switches. A continuación, se muestra el resultado del S1.

S1# **show interface trunk**

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

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#
```

```
S2#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
S2#
```

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>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

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
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 = 0ms, Average = 0ms

PC>
```

El comando ping es satisfactorio. El PC-A esta en la misma VLAN administrativa que el SWITCH.

b. En la sesión de consola del 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 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

El PING es satisfactorio, ya está creada la troncal entre ambos SWITCH 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?

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

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

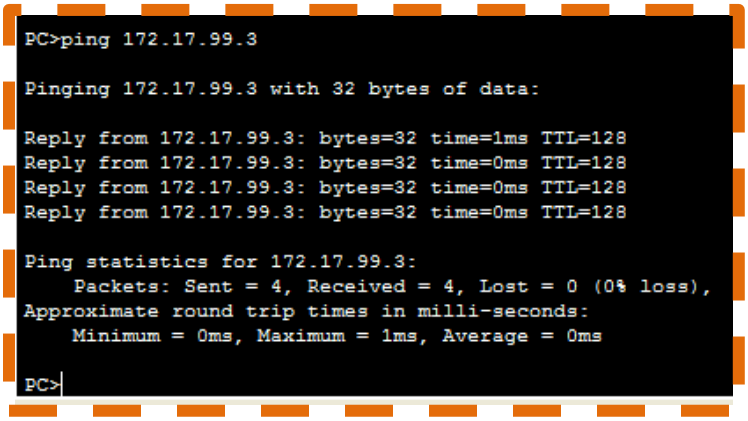
```
PC>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

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

Ping statistics for 172.17.99.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 172.17.99.4

Pinging 172.17.99.4 with 32 bytes of data:

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

Ping statistics for 172.17.99.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Todos los PIN no se dan de manera satisfactoria. Porque PC-B está en la VLAN 10 y el resto está en la VLAN 99.

---

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?

```
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

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>
```



Todos los PINES son satisfactorios. PC-C está en la misma VLAN de S1 S2 y PC-A. Además la troncal ya está creada.

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#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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
S1#
```

a. Desactive la negociación en el S1.

S1(config)# **interface f0/1**

S1(config-if)# **switchport nonegotiate**

```
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Desactive la negociación en el S2.

S2(config)# **interface f0/1**

S2(config-if)# **switchport nonegotiate**

```
S2(config)#int f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#end
S2#
```

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

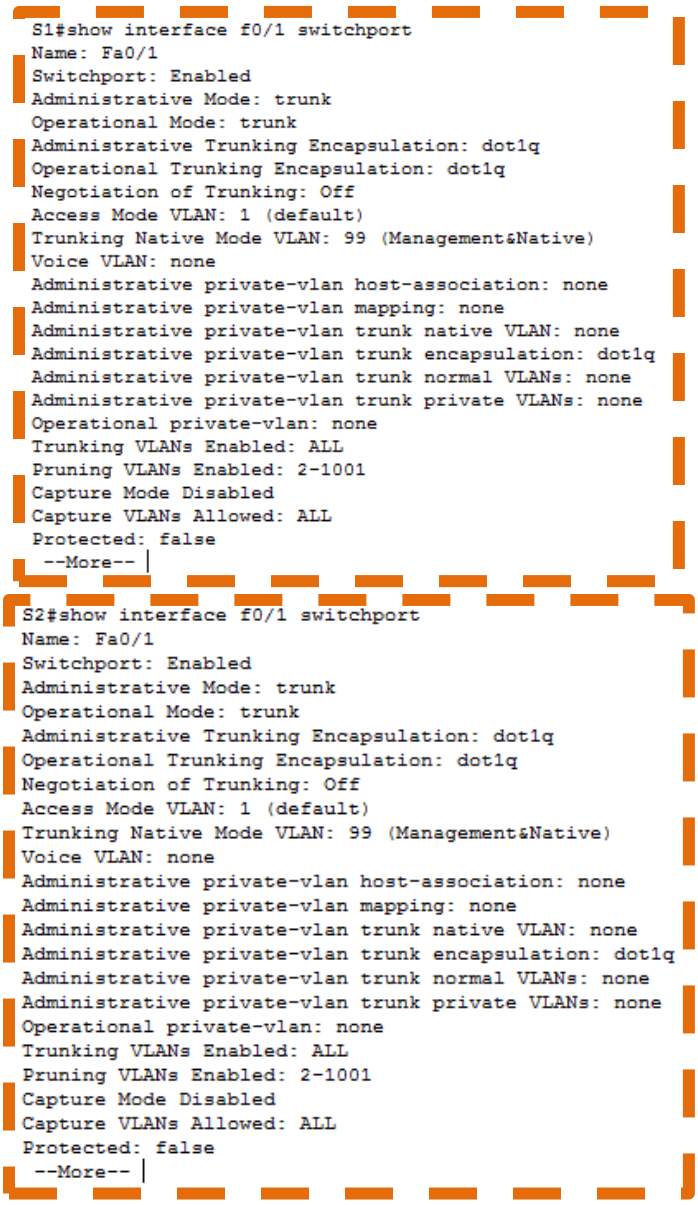
Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: Off

<Output Omitted>



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#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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
 --More--
```

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 t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/2-5
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#
```

c. Deshabilite los enlaces troncales en los puertos de acceso del S2.

```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int range f0/2-5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#
```

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#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
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
 --More--
```

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#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, Gig0/1, Gig0/2
10   Datos                            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#
```

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 t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport trunk allowed vlan 10,99
S1(config-if)#
```

g. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10 y 99.

```
S2(config)#int f0/1
S2(config-if)#switchport trunk allowed vlan 10,99
S2(config-if)#
```

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**

```
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#
```

```
S2#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
S2#
```

¿Cuál es el resultado?

Solo están permitidas las VLAN 10 Y 99 por la troncal entre S1 Y S2

Reflexión

¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco?

1. **Todos los puertos por defecto están asignados a la misma vlan.**
2. **Los enlaces troncales están por defecto en auto negociación.**
3. **Que las contraseñas estén en texto plano.**
4. **Servidor http está activado por defecto.**

4.1.4.6 Práctica de laboratorio: configuración de los parámetros básicos del router con la CLI del IOS

Topología

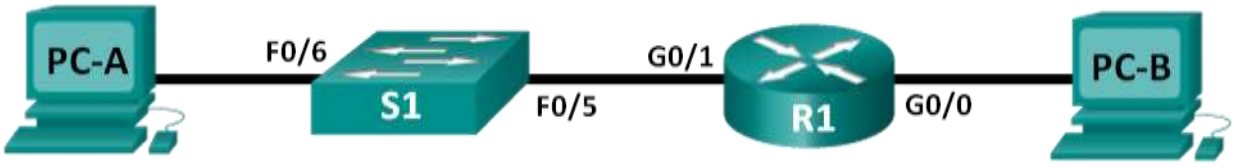


Tabla de direccionamiento

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
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

- Realizar el cableado de los equipos para que coincidan con la topología de la red.
- Inicializar y reiniciar el router y el switch.

Parte 2: Configurar los dispositivos y verificar la conectividad

- Asignar información de IPv4 estática a las interfaces de la computadora.
- Configurar los parámetros básicos del router.
- Verificar la conectividad de la red
- Configurar el router para el acceso por SSH.

Parte 3: Mostrar la información del router

- Recuperar información del hardware y del software del router.
- Interpretar el resultado de la configuración de inicio.
- Interpretar el resultado de la tabla de routing.
- Verificar el estado de las interfaces.

Parte 4: Configurar IPv6 y verificar la conectividad

Información básica/situación

Esta es una práctica de laboratorio integral para revisar comandos de router de IOS que se abarcaron anteriormente. En las partes 1 y 2, realizará el cableado de los equipos y completará las configuraciones básicas y las configuraciones de las interfaces IPv4 en el router.

En la parte 3, utilizará SSH para conectarse de manera remota al router y usará comandos de IOS para recuperar la información del dispositivo para responder preguntas sobre el router. En la parte 4, configurará IPv6 en el router de modo que la PC-B pueda adquirir una dirección IP y luego verificará la conectividad.

Para fines de revisión, esta práctica de laboratorio proporciona los comandos necesarios para las configuraciones de router específicas.

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 2960 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. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

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: 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 1: Establecer la topología e inicializar los dispositivos

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

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

j. Encienda todos los dispositivos de la topología.

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

Nota: En el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

Parte 2: Configurar dispositivos y verificar la conectividad

Paso 1. Configure las interfaces de la PC.

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

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

Paso 2. Configurar el router.

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

Router> **enable**
Router#

b. Ingrese al modo de configuración global.

Router# **config terminal**
Router(config)#

c. Asigne un nombre de dispositivo al router.

Router(config)# **hostname R1**

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

R1(config)# **no ip domain-lookup**

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

R1(config)# **security passwords min-length 10**

Además de configurar una longitud mínima, enumere otras formas de aportar seguridad a las contraseñas.

_____
_____

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

R1(config)# **enable secret cisco12345**

g. Asigne **ciscoconpass** como la contraseña de consola, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**. El comando **logging synchronous** sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.

R1(config)# **line con 0**
R1(config-line)# **password ciscoconpass**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**

R1(config-line)# **logging synchronous**
R1(config-line)# **exit**
R1(config)#

Para el comando **exec-timeout**, ¿qué representan el **5** y el **0**?

_____
_____

h. Asigne **ciscovtypass** como la contraseña de vty, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**.

R1(config)# **line vty 0 4**
R1(config-line)# **password ciscovtypass**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **logging synchronous**
R1(config-line)# **exit**
R1(config)#

i. Cifre las contraseñas de texto no cifrado.

R1(config)# **service password-encryption**

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

R1(config)# **banner motd #Unauthorized access prohibited!#**

k. Configure una dirección IP y una descripción de interfaz. Active las dos interfaces en el router.

R1(config)# **int g0/0**
R1(config-if)# **description Connection to PC-B**
R1(config-if)# **ip address 192.168.0.1 255.255.255.0**
R1(config-if)# **no shutdown**
R1(config-if)# **int g0/1**
R1(config-if)# **description Connection to S1**
R1(config-if)# **ip address 192.168.1.1 255.255.255.0**
R1(config-if)# **no shutdown**
R1(config-if)# **exit**
R1(config)# **exit**
R1#

l. Configure el reloj en el router, por ejemplo:

R1# **clock set 17:00:00 18 Feb 2013**

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

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

¿Qué resultado obtendría al volver a cargar el router antes de completar el comando **copy running-config startup-config**?

_____

_____

_____

_____

Paso 3. Verificar la conectividad de la red

a. Haga ping a la PC-B en un símbolo del sistema en la PC-A.

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

¿Tuvieron éxito los pings? ____

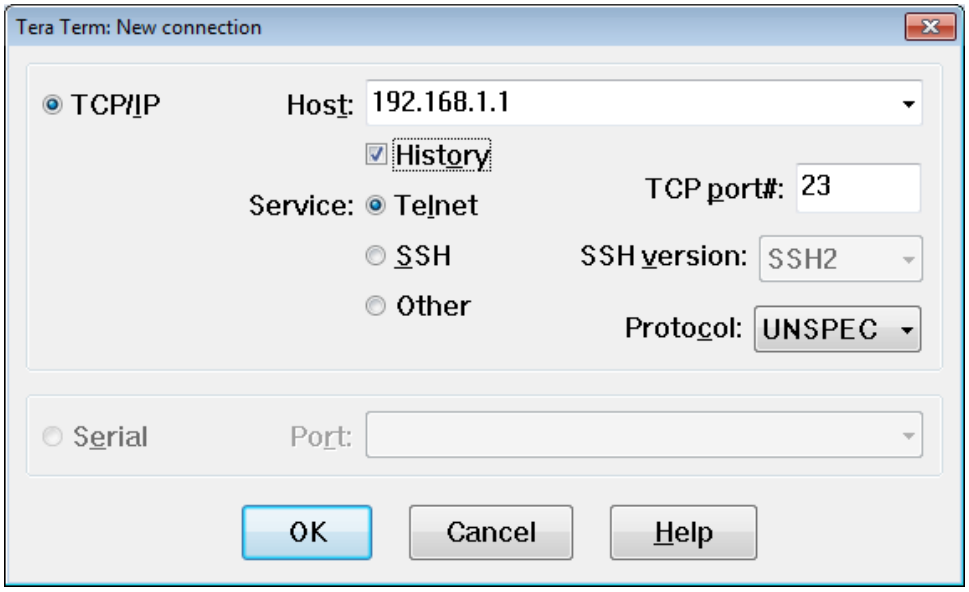
Después de completar esta serie de comandos, ¿qué tipo de acceso remoto podría usarse para acceder al R1?

_____

_____

b. Acceda de forma remota al R1 desde la PC-A mediante el cliente de Telnet de Tera Term.

Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: nueva conexión). Asegúrese de que el botón de opción **Telnet** esté seleccionado y después haga clic en **OK** (Aceptar) para conectarse al router.



¿Pudo conectarse remotamente? ____

¿Por qué el protocolo Telnet es considerado un riesgo de seguridad?

_____
_____

_____
_____

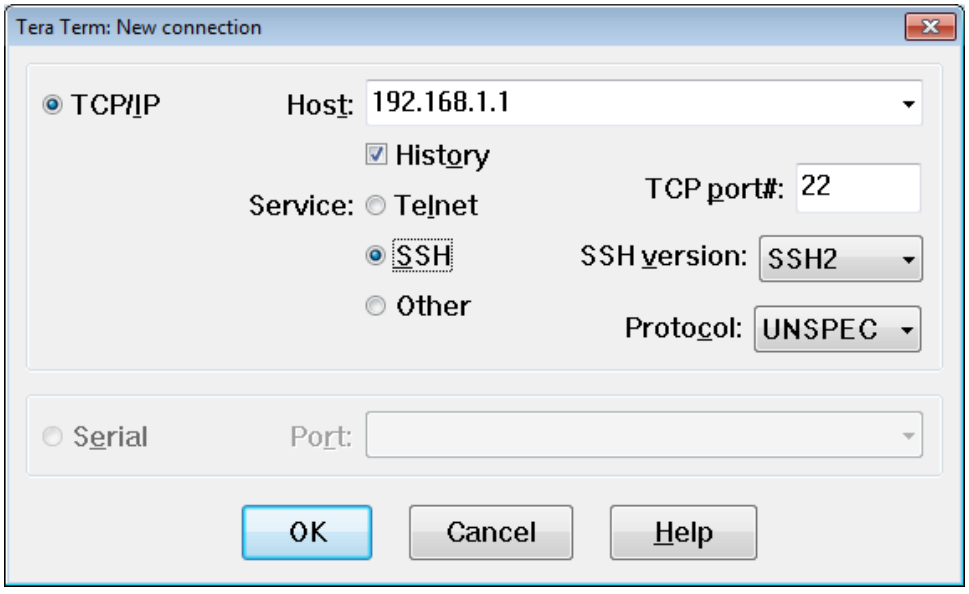
Paso 4. configurar el router para el acceso por SSH.

a. Habilite las conexiones SSH y cree un usuario en la base de datos local del router.

R1# **configure terminal**
R1(config)# **ip domain-name CCNA-lab.com**
R1(config)# **username admin privilege 15 secret adminpass1**
R1(config)# **line vty 0 4**
R1(config-line)# **transport input ssh**
R1(config-line)# **login local**
R1(config-line)# **exit**
R1(config)# **crypto key generate rsa modulus 1024**
R1(config)# **exit**

b. Acceda remotamente al R1 desde la PC-A con el cliente SSH de Tera Term.

Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: nueva conexión). Asegúrese de que el botón de opción **SSH** esté seleccionado y después haga clic en **OK** para conectarse al router.



¿Pudo conectarse remotamente? ____

Parte 3: Mostrar la información del router

En la parte 3, utilizará comandos **show** en una sesión SSH para recuperar información del router.

Paso 1. Establecer una sesión SSH para el R1.

Mediante Tera Term en la PC-B, abra una sesión SSH para el R1 en la dirección IP 192.168.0.1 e inicie sesión como **admin** y use la contraseña **adminpass1**.

Paso 2. Recuperar información importante del hardware y el software.

a. Use el comando **show version** para responder preguntas sobre el router.

¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router?

¿Cuánta memoria flash tiene el router?

b. Con frecuencia, los comandos **show** proporcionan varias pantallas de resultados. Filtrar el resultado permite que un usuario visualice determinadas secciones del resultado. Para habilitar el comando de filtrado, introduzca una barra vertical (|) después de un comando **show**, seguido de un parámetro de filtrado y una expresión de filtrado. Para que el resultado coincida con la instrucción de filtrado, puede usar la palabra clave **include** para ver todas las líneas del resultado que contienen la expresión de filtrado. Filtre el comando **show version** mediante **show version | include register** para responder la siguiente pregunta.

¿Cuál es el proceso de arranque para el router en la siguiente recarga?

Paso 3. Mostrar la configuración de inicio.

Use el comando **show startup-config** en el router para responder las siguientes preguntas.

¿De qué forma figuran las contraseñas en el resultado?

Use el comando **show startup-config | begin vty**.

¿Qué resultado se obtiene al usar este comando?

Paso 4. Mostrar la tabla de routing en el router.

Use el comando **show ip route** en el router para responder las siguientes preguntas.

¿Qué código se utiliza en la tabla de routing para indicar una red conectada directamente?

¿Cuántas entradas de ruta están cifradas con un código C en la tabla de routing? _____

Paso 5. Mostrar una lista de resumen de las interfaces del router.

Use el comando **show ip interface brief** en el router para responder la siguiente pregunta.

¿Qué comando cambió el estado de los puertos Gigabit Ethernet de administrativamente inactivo a activo?

Parte 4: Configurar IPv6 y verificar la conectividad

Paso 1. Asignar direcciones IPv6 a la G0/0 del R1 y habilitar el routing IPv6.

Nota: La asignación de una dirección IPv6, además de una dirección IPv4, en una interfaz se conoce como "dual stacking", debido a que las pilas de protocolos IPv4 e IPv6 están activas. Al habilitar el routing de unidifusión IPv6 en el R1, la PC-B recibe el prefijo de red IPv6 de G0/0 del R1 y puede configurar automáticamente la dirección IPv6 y el gateway predeterminado.

a. Asigne una dirección de unidifusión global IPv6 a la interfaz G0/0; asigne la dirección link-local en la interfaz, además de la dirección de unidifusión; y habilite el routing IPv6.

R1# **configure terminal**
R1(config)# **interface g0/0**
R1(config-if)# **ipv6 address 2001:db8:acad:a::1/64**
R1(config-if)# **ipv6 address fe80::1 link-local**
R1(config-if)# **no shutdown**
R1(config-if)# **exit**
R1(config)# **ipv6 unicast-routing**
R1(config)# **exit**

b. Use el comando **show ipv6 int brief** para verificar la configuración de IPv6 en el R1.

Si no se asignó una dirección IPv6 a la G0/1, ¿por qué se indica como [up/up]?

c. Emita el comando **ipconfig** en la PC-B para examinar la configuración de IPv6.

¿Cuál es la dirección IPv6 asignada a la PC-B?

FE80::2E0:A3FF:FEB9:9E50

¿Cuál es el gateway predeterminado asignado a la PC-B? FE80::2E0:A3FF:FEB9:9E50

En la PC-B, haga ping a la dirección link-local del gateway predeterminado del R1. ¿Tuvo éxito? si

En la PC-B, haga ping a la dirección IPv6 de unidifusión del R1 2001:db8:acad:a::1. ¿Tuvo éxito? No

Reflexión

1. Durante la investigación de un problema de conectividad de red, un técnico sospecha que no se habilitó una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?

show ip route_, show ipv int brief

2. Durante la investigación de un problema de conectividad de red, un técnico sospecha que se asignó una máscara de subred incorrecta a una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?

   Show ip route- show startup config

3. Después de configurar IPv6 en la LAN de la PC-B en la interfaz G0/0 del R1, si hiciera ping de la PC-A a la dirección IPv6 de la PC-B, ¿el ping sería correcto? ¿Por qué o por qué no?

   Se presume incorrecto por que el router presenta seguridad ssh.

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: Inicialización y recarga de un router y un switch

Paso 1. Inicializar y volver a cargar el router.

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

   Router> **enable**

   Router#

b. Escriba el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM.

Router# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Router#

c. Emita el comando **reload** para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje **Proceed with reload** (Continuar con la recarga), presione Enter para confirmar. (Si presiona cualquier otra tecla, se cancela la recarga).

Router# **reload**

Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

Nota: Es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el router. Escriba **no** y presione Enter.

System configuration has been modified. Save? [yes/no]: **no**

d. Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Enter.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

e. Se le solicita finalizar la instalación automática. Escriba **yes** (sí) y, luego, presione Enter.

Would you like to terminate autoinstall? [yes]: **yes**

Paso 2. Inicializar y volver a cargar el switch.

a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

Switch> **enable**

Switch#

b. Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

Switch# **show flash**

Directory of flash:/

2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text
3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text
4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs

5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)

Switch#

c. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

d. Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Enter si introdujo el nombre de manera correcta.

e. Se le solicitará que confirme que desea eliminar este archivo. Presione Enter para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

Delete flash:/vlan.dat? [confirm]

Switch#

f. Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicitará que confirme la eliminación del archivo de configuración. Presione Enter para confirmar que desea borrar este archivo. (Al pulsar cualquier otra tecla, se cancela la operación).

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

g. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Se le solicitará que confirme la recarga del switch. Presione Enter para seguir con la recarga. (Si presiona cualquier otra tecla, se cancela la recarga).

Switch# **reload**

Proceed with reload? [confirm]

Nota: Es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Enter.

System configuration has been modified. Save? [yes/no]: **no**

h. Una vez que se vuelve a cargar el switch, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Enter.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Switch>

Desarrollo Laboratorio

```
Router>ena
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

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

IOS Image Load Test
_____
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################
# [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
Onboard devices &
buffer pools 0x01E8F000
-----------------------------------------
TOTAL: 0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
```

Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport

Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

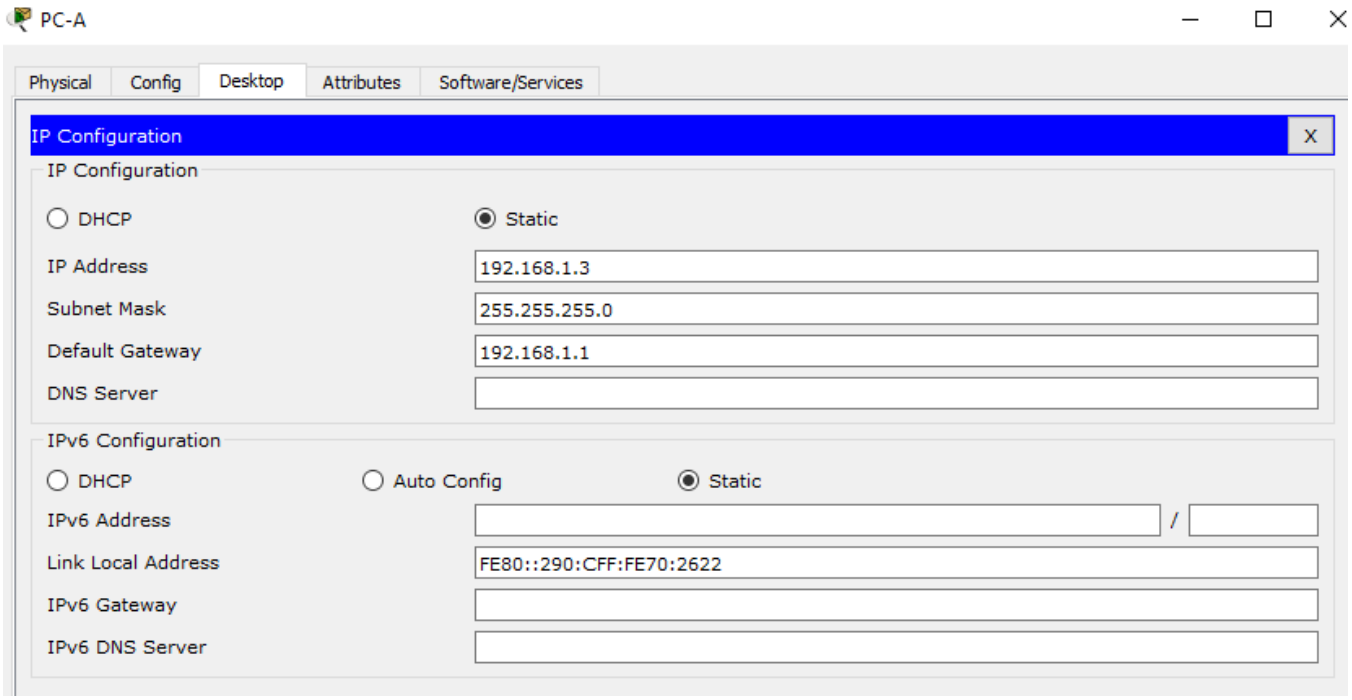
Press RETURN to get started!

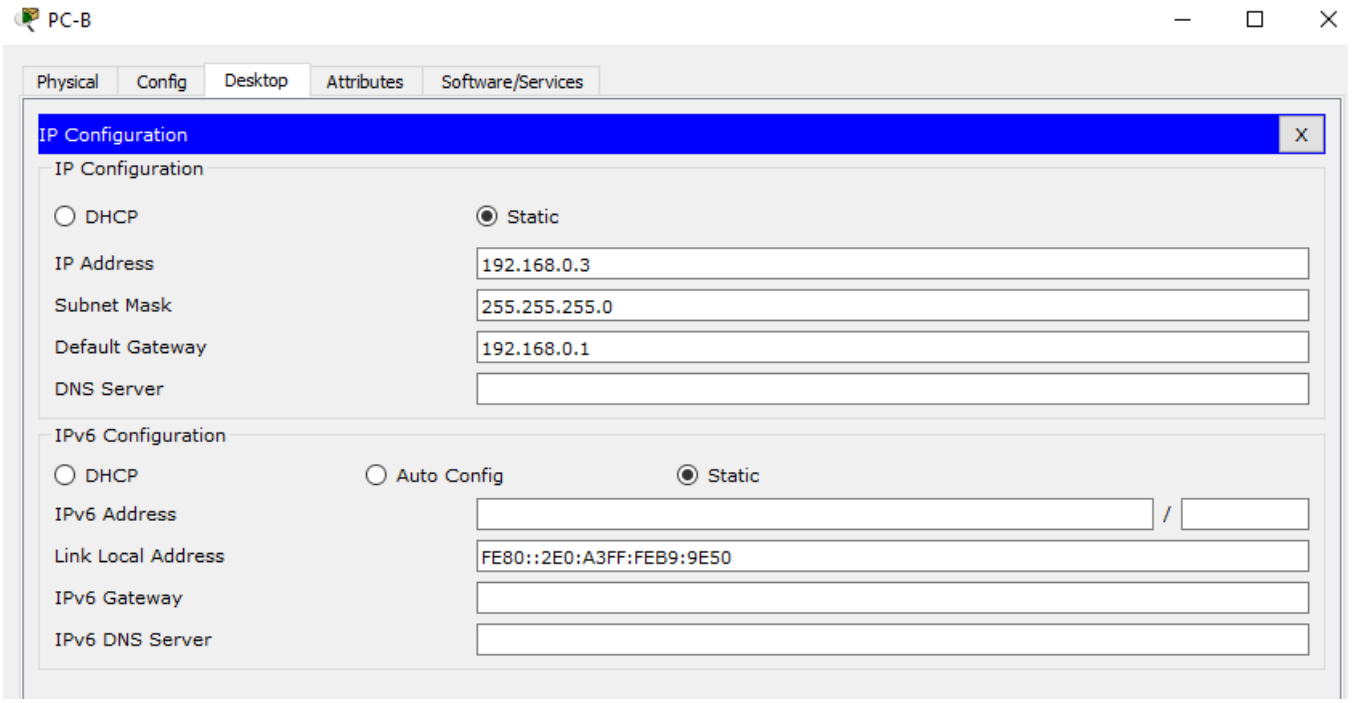
Router>

Switch>ena
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#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]n
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]n
Switch#
Switch#



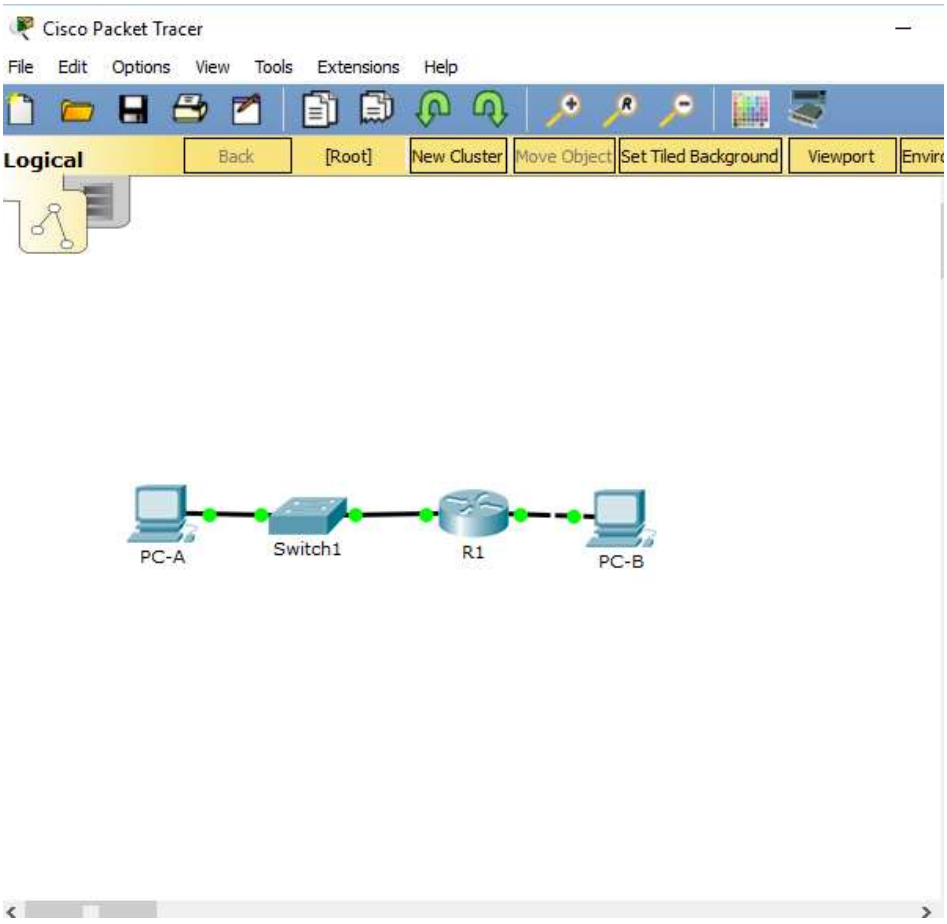


Configuración Router

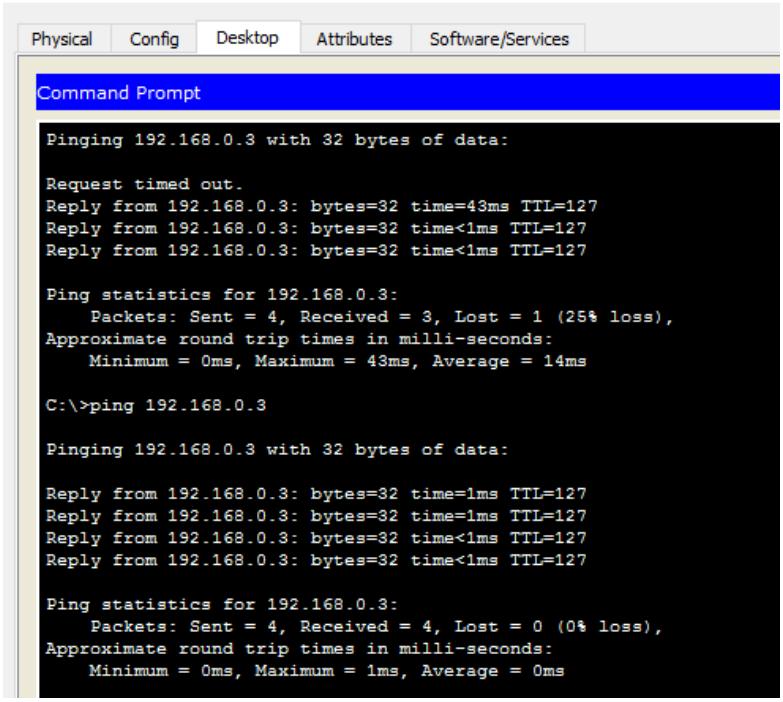
Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1

```
R1(config)#no ip domain-lookup
R1(config)#security password min-length 10
R1(config)#enable secret cisco12345
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#loggin synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#loggin synchronous
R1(config-line)#exit
R1(config)#servide password-encryption
^
% Invalid input detected at '^' marker.
R1(config)#service password-encryption
R1(config)#banner motd #Unauthorized access prohibited!#
R1(config)#int g0/0
R1(config-if)#description Connection to PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#
R1(config-if)#int g0/1
R1(config-if)#description Connection to S1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)#
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 20:02:00 02 nov 2016
```

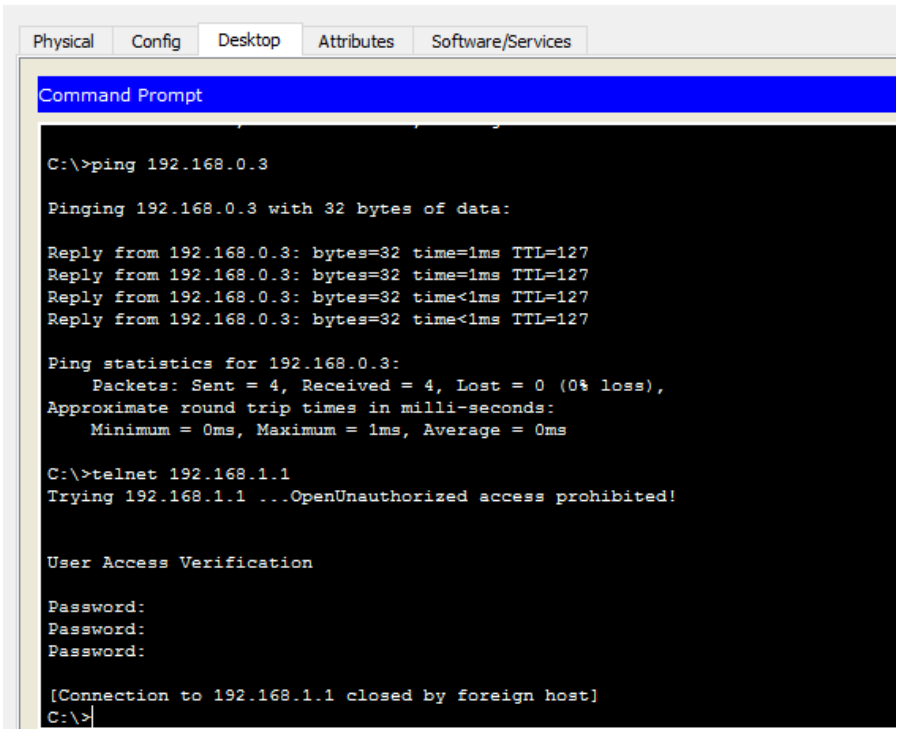
R1#copy running-config startup-config



PC-A



PC-A



R1>ena
Password:
R1#conf t

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name CCNA-lab.com
R1(config)#username admin privilege 15 secret adminpass1
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#cryto key generate rsa modulus 1024
R1(config)#crypto key generate rsa
The name for the keys will be: R1.CCNA-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R1(config)#exit
*Nov. 2 21:58:40.572: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#


R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 2 hours, 30 minutes, 2 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

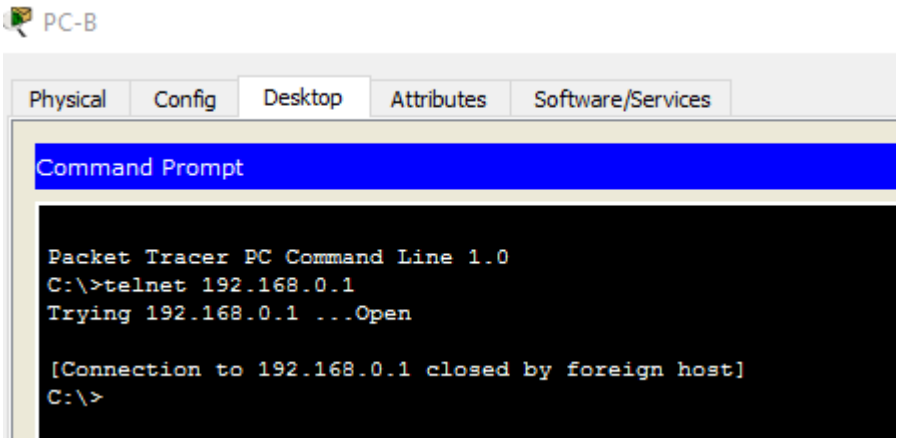
Device# PID SN
---
*0 CISCO1941/K9 FTX1524U9MJ

Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102

R1#



R1#show startup-config
Using 1127 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
!
!
enable secret 5 1mERr$WvpW0n5HghRrqnrwXCUUl.
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 1mERr$S3UmkqGQcDw6dk8CDb1hF.
!
!
license udi pid CISCO1941/K9 sn FTX1524U9MJ
!
!
!
!

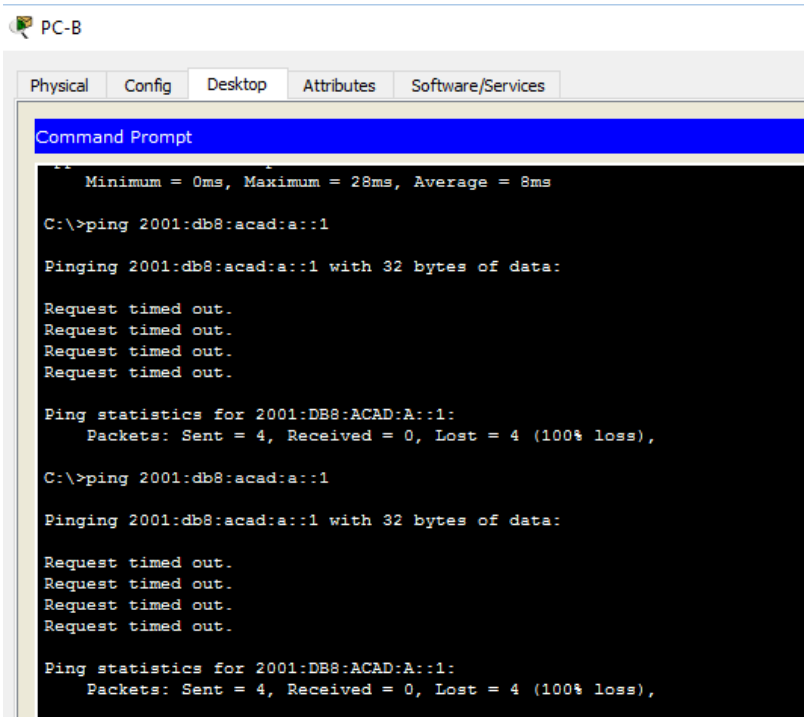
```
!
!
!
!
!
no ip domain-lookup
ip domain-name CCNA-lab.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized access prohibited!^C
!
!
!
!
line con 0
exec-timeout 5 0
password 7 0822455D0A1606181C1B0D1739
logging synchronous
```

```
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
logging synchronous
login local
transport input ssh
!
!
!
end


R1#
R1#


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

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
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

R1#


R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.0.1 YES manual up up
GigabitEthernet0/1 192.168.1.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
```

R1#

R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.0.1 YES manual up up
GigabitEthernet0/1 192.168.1.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ipv6 address 2001:db8:acad:a::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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



4.1.4.7 Práctica de laboratorio: configuración de los parámetros básicos del router con CCP

Topología

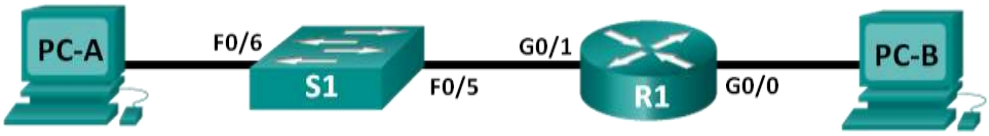


Tabla de direccionamiento

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 12. 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.

Parte 13. Configurar dispositivos y verificar la conectividad

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.

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

b. 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.

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

d. Ingrese al modo de configuración global.

e. Desactive la búsqueda del DNS.

f. Asigne un nombre de dispositivo al router.

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

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

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

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

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

l. Cifre las contraseñas de texto no cifrado.

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

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

o. 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 14. 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.

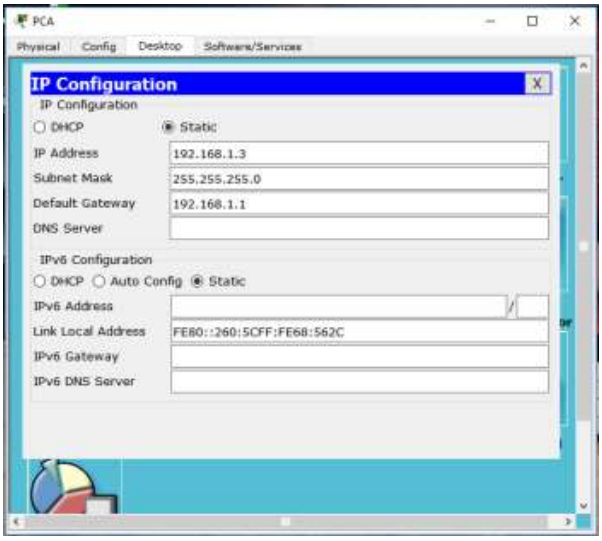
Asigne un usuario en la base de datos local del router para acceder a CCP con el nombre de usuario **admin** y la contraseña **adminpass1**.

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

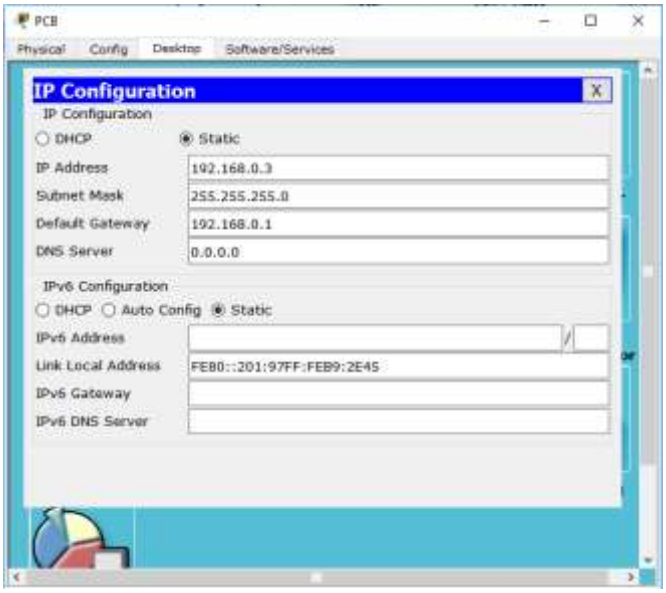
Solución

Topología

Iniciamos configurando el PCA, ip, mascara de subred y puerta de enlace.



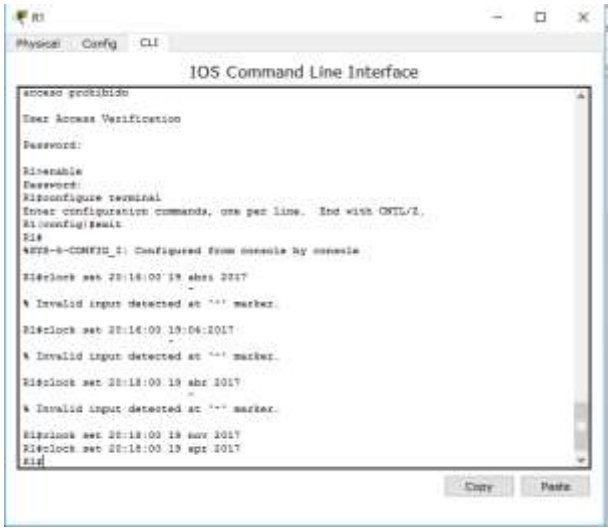
Configuración PCB, ip, mascara de subred y puerta de enlace.



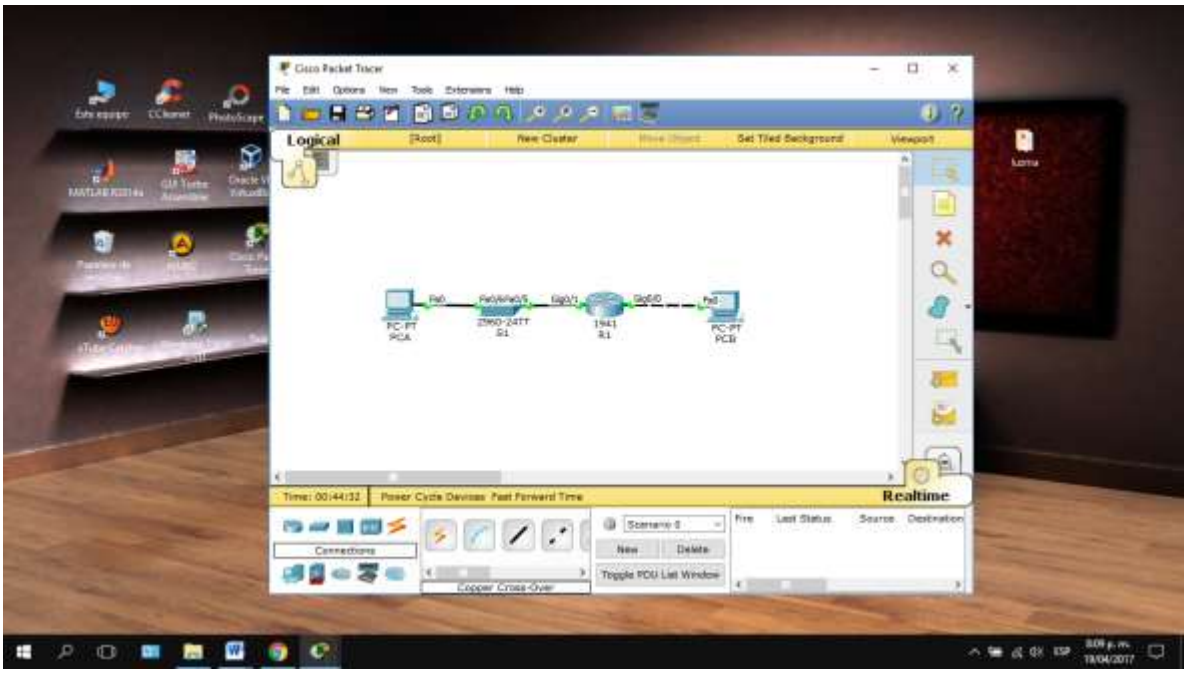
Configuración del ROUTER

R1

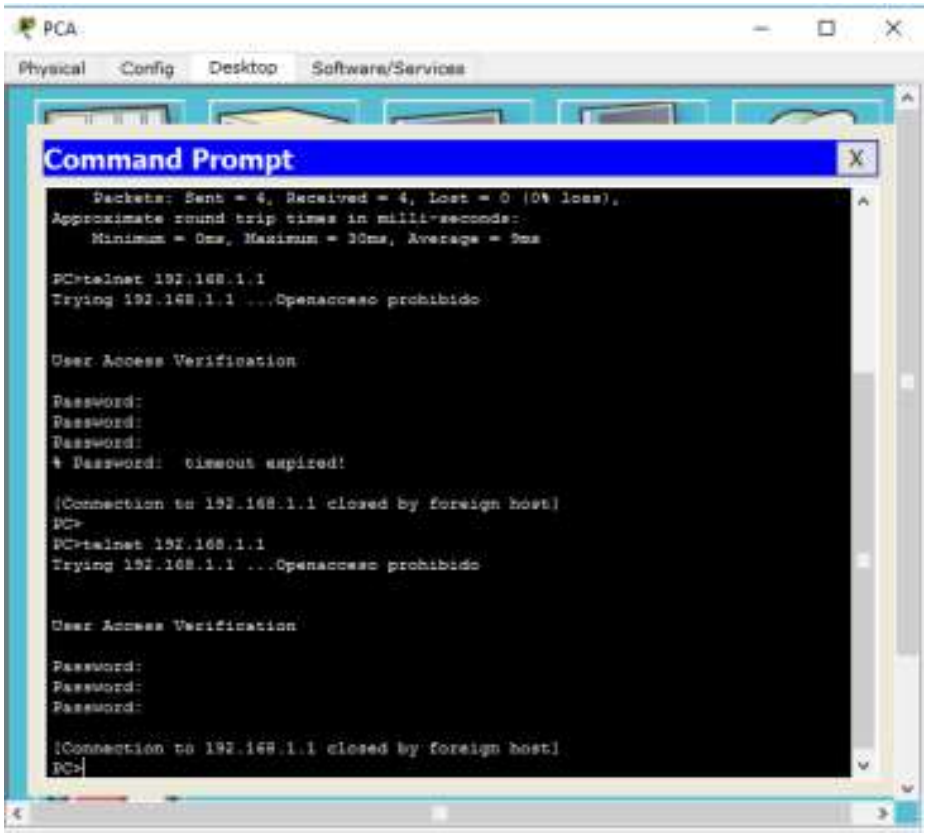
Configuración de hora y fecha en el router



Conexión establecida

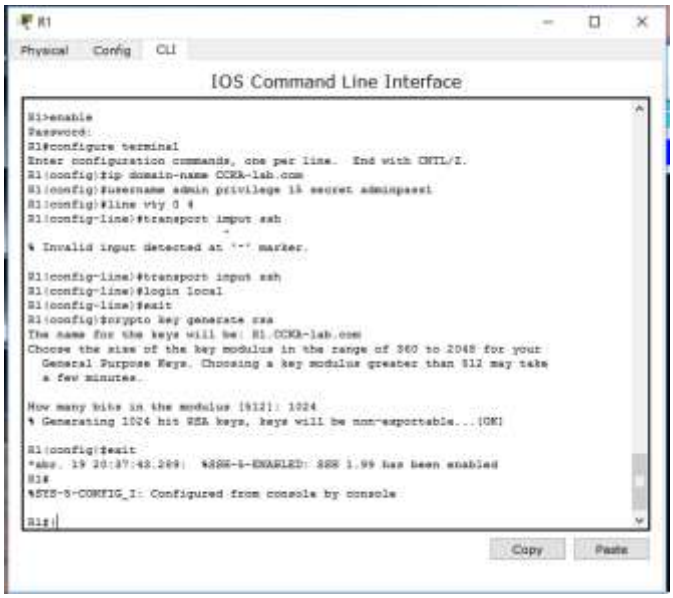


Prueba de conexión, realizando PING



Como TELNET es un protocolo no muy seguro

Configuración de SSH



5.1.3.6 Packet Tracer – Configuring Router-on-a-Stick Inter-VLAN Routing

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

Objetives

Part 1: Test Connectivity without Inter-VLAN Routing
Part 2: Add VLANs to a Switch
Part 3: Configure Sub interfaces
Part 4: Test Connectivity with Inter-VLAN Routing

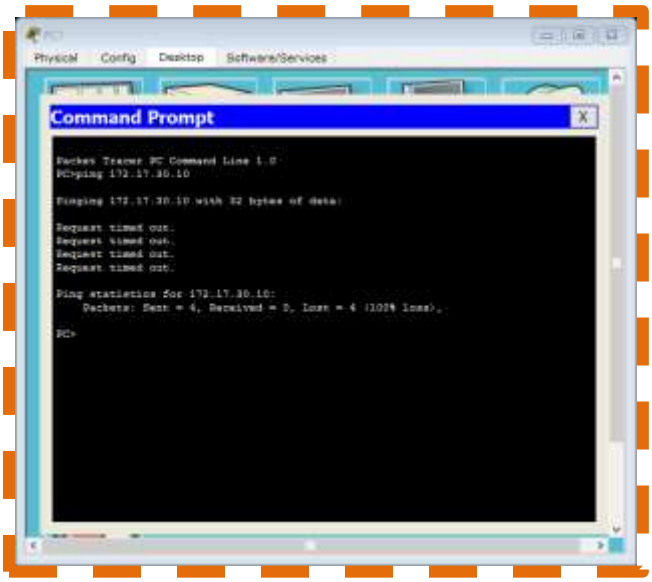
Scenario

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.

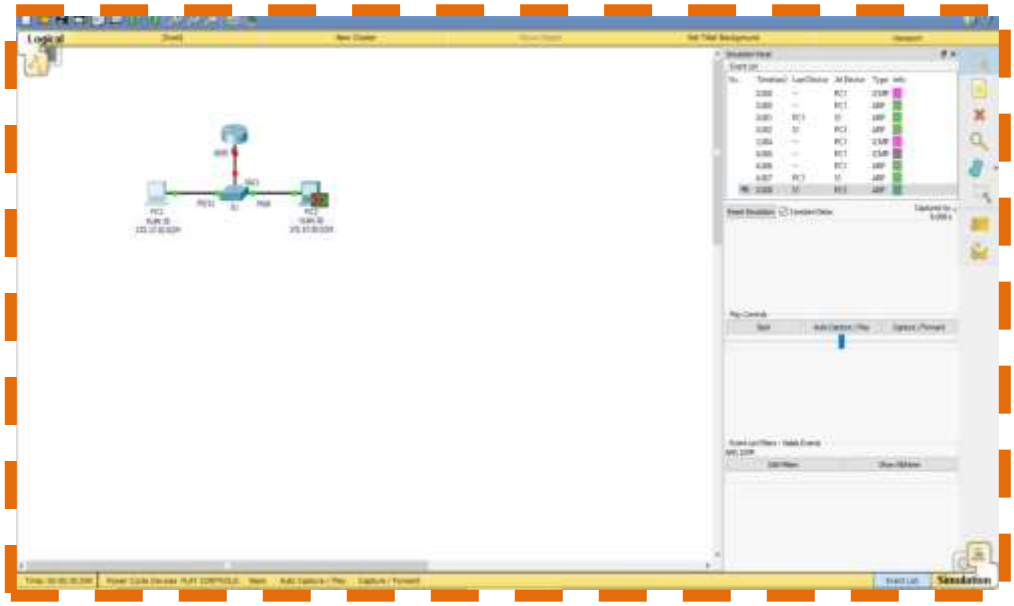
Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs are on separate networks and **R1** is not configured, the ping fails.



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?



La PC 1 está en una red diferente a PC 2

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**.

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>ENABLE
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#int fa0/11
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#
```

b. Issue the **show vlan brief** command to verify VLAN configuration.

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, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                         active    Fa0/11
30   VLAN0030                         active    Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful?

```
PC>ping 172.17.30.10

Pinging 172.17.30.10 with 32 bytes of data:

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

Ping statistics for 172.17.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Los PC'S se encuentran en distintas redes

Part 3: Configure Sub interfaces

Step 1: Configure sub interfaces 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>ENABLE
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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
R1(config-subif)#
```

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.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/0.10  172.17.10.1     YES manual administratively down down

GigabitEthernet0/0.30  172.17.30.1     YES manual administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
R1#
```

b. Enable the G0/0 interface. Verify that the subinterfaces are now active.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up

R1(config-if)#
```

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  up                    up

GigabitEthernet0/0.10  172.17.10.1     YES manual up                    up

GigabitEthernet0/0.30  172.17.30.1     YES manual up                    up

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
R1#
```

Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

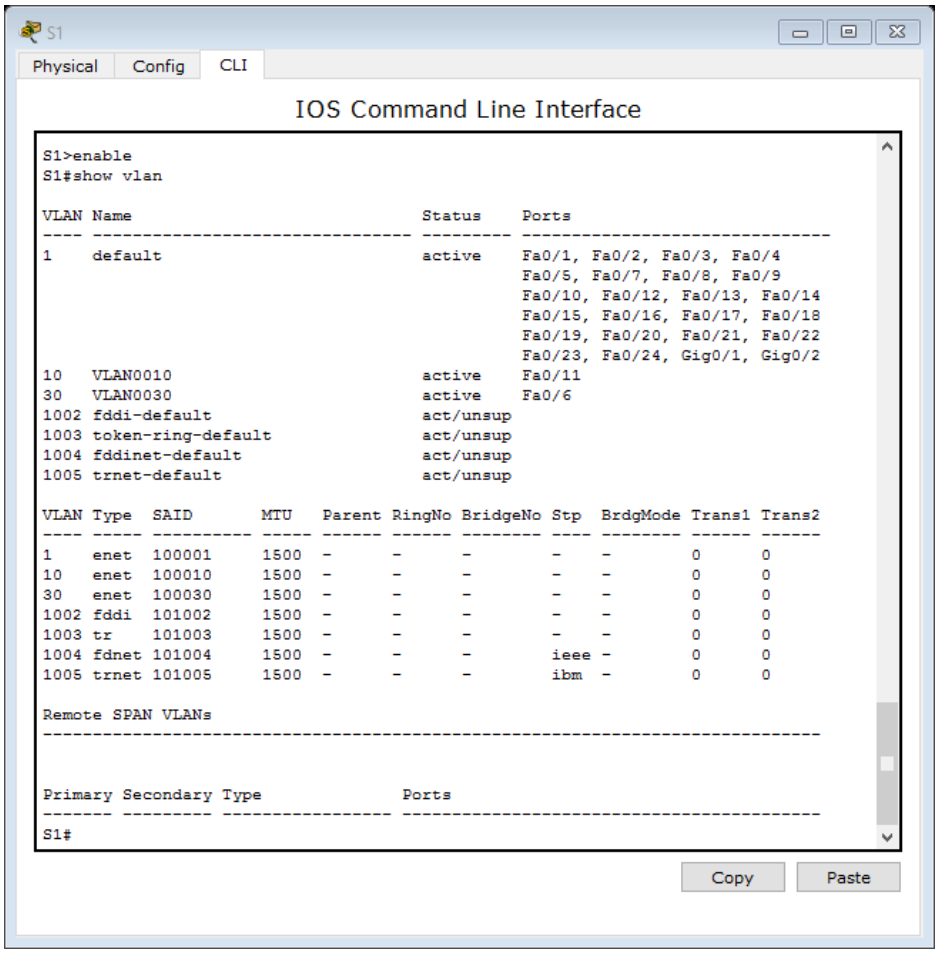
From **PC1**, ping **PC3**. The pings should still fail.

```
PC>ping 172.17.30.10

Pinging 172.17.30.10 with 32 bytes of data:

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

Ping statistics for 172.17.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Step 2: Enable trunking.

a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to?

Esta asignado a la VLAN 1 por defecto



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 T
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int g0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down

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

S1(config-if)#
```

c. How can you determine that the interface is a trunk port using the **show vlan** command?

```
S1#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, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
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
```

La interface G0/1 no se encuentra con el comando anterior.

d. Issue the **show interface trunk** command to verify the interface is configured as a trunk.

```
S1#SHOW INTERFACE TRUNK
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,30
S1#
```

En esta captura si se ve la interface g0/1 en modo trunk

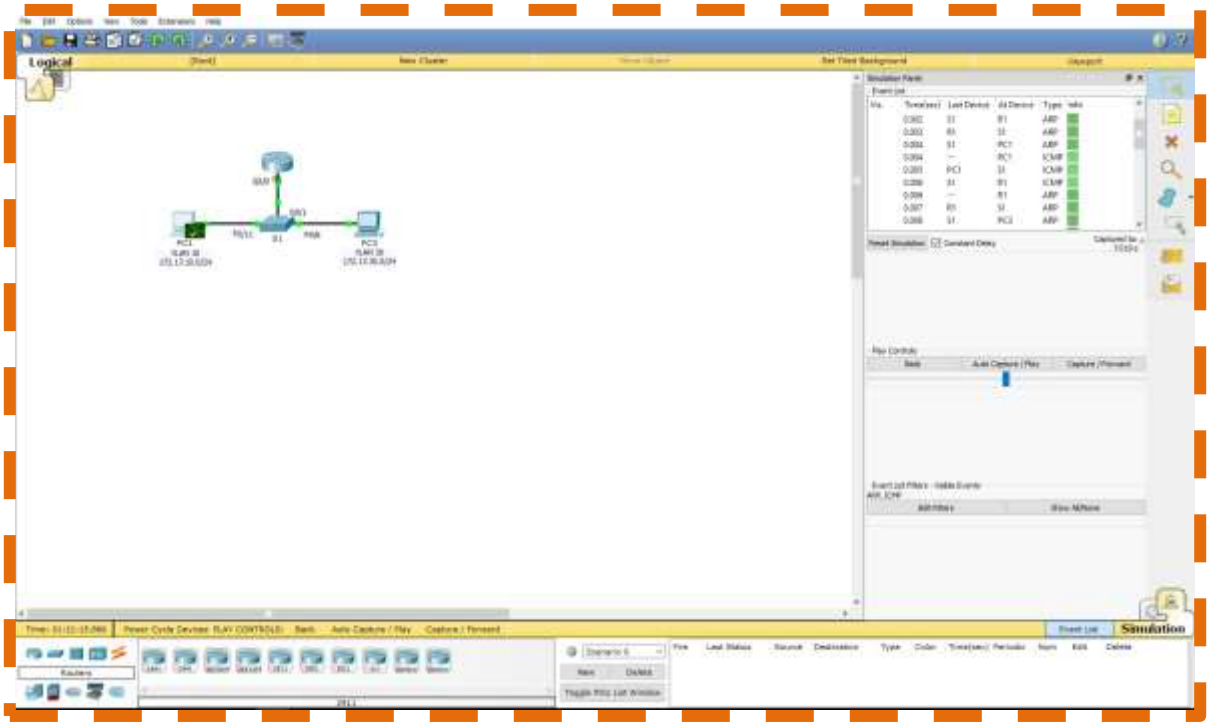
Step 3: Switch to Simulation mode to monitor pings.

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**.

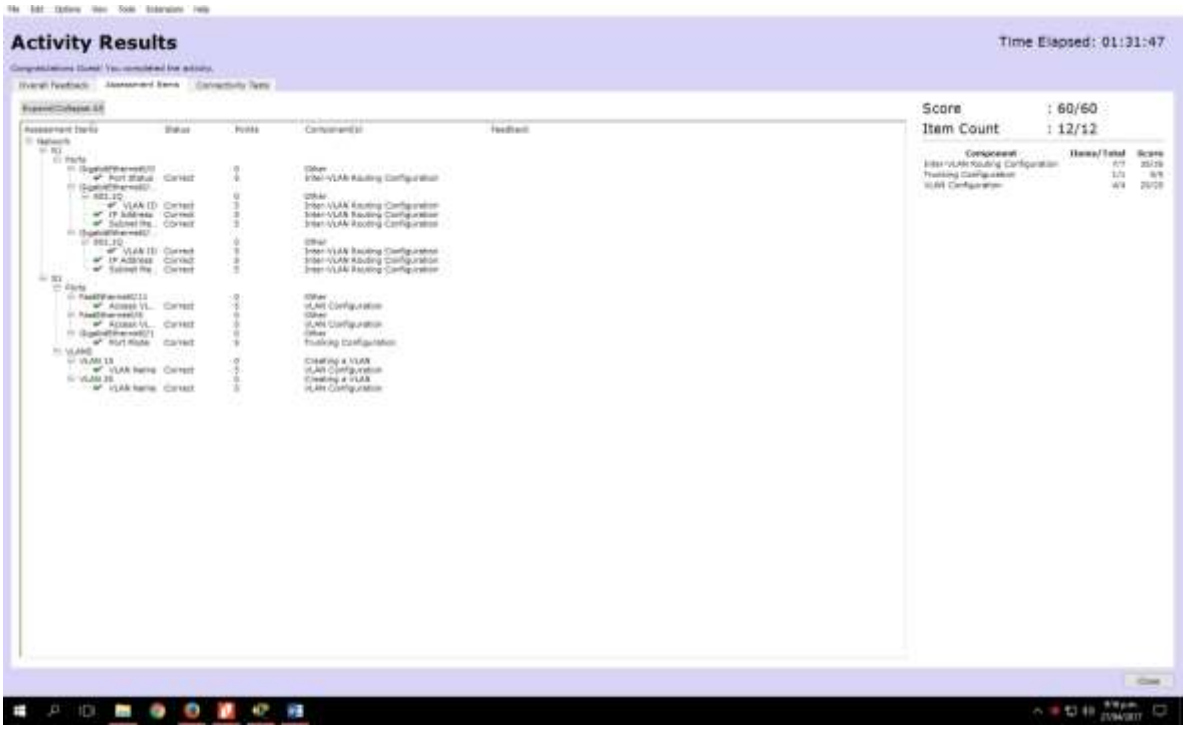
c. You should see ARP requests and replies between **S1** and **R1**. Then ARP requests and replies between **R1** and **S3**. Then **PC1** can encapsulate an ICMP echo request with the proper data-link layer information and R1 will route the request to **PC3**.

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.



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

Topología

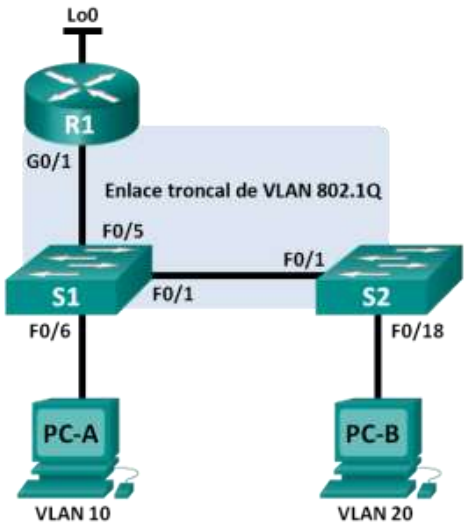


Tabla de direccionamiento

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.

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 consola y la contraseña de vty.
e. Configure **logging synchronous** para la línea de consola.
f. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.
g. Configure el gateway predeterminado en los dos switches.
h. Desactive administrativamente todos los puertos que no se usen en el switch.
i. 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.

R/ Enable

Conf t

Hostname

Vlan 20

Name

exit

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.

R/ 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.

R/ switchport mode Access

Paso 2. configurar las VLAN en el switch 2.

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

e. 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.

R/

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

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

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

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 3. Configurar una subinterfaz para la VLAN 1.

h. 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.

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

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

Paso 4. configurar una subinterfaz para la VLAN 10.

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

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

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

Paso 5. Configurar una subinterfaz para la VLAN 20.

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

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

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

Paso 6. Habilitar la interfaz G0/1.

Habilite la interfaz G0/1. En el espacio proporcionado, escriba los comandos que utilizó.

Solución

Comandos que se utilizaron para configurar la red

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

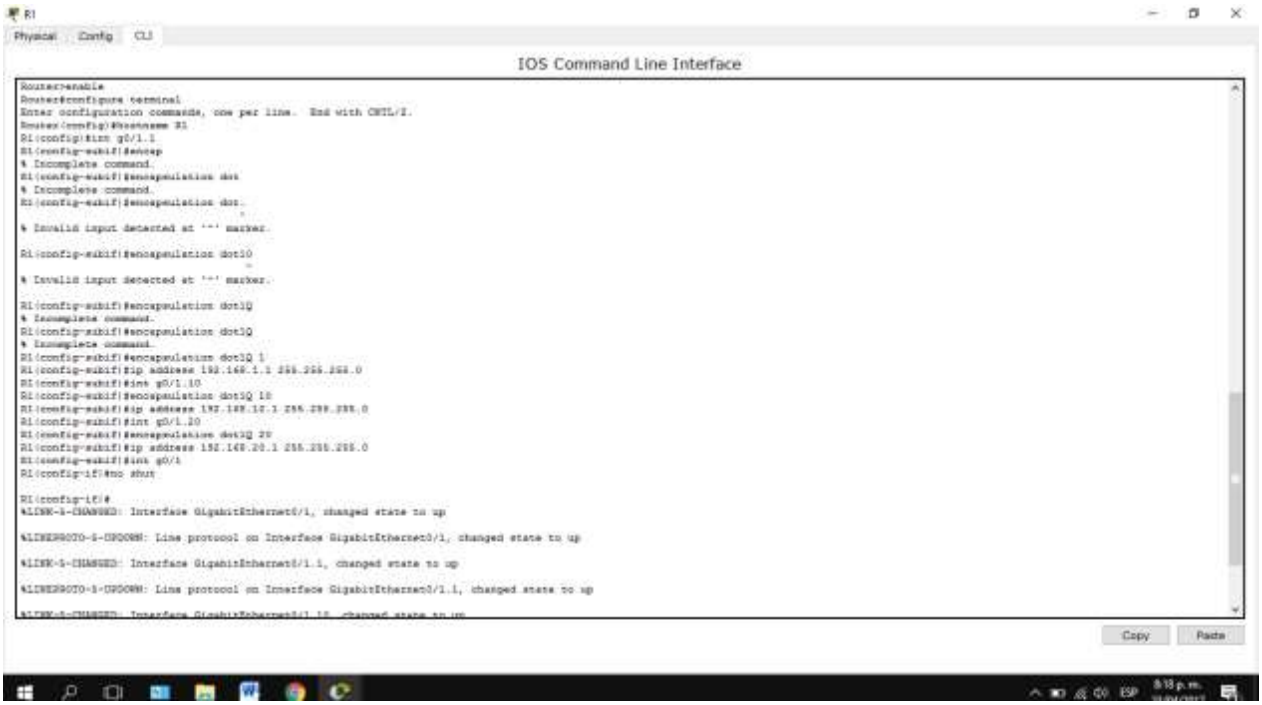
S2(config)# **vlan 10**
S2(config-vlan)# **name Students**
S2(config-vlan)# **vlan 20**
S2(config-vlan)# **name Faculty**

S2(config)# **interface f0/1**
S2(config-if)# **switchport mode trunk**
S2(config-if)# **interface f0/18**
S2(config-if)# **switchport access vlan 20**

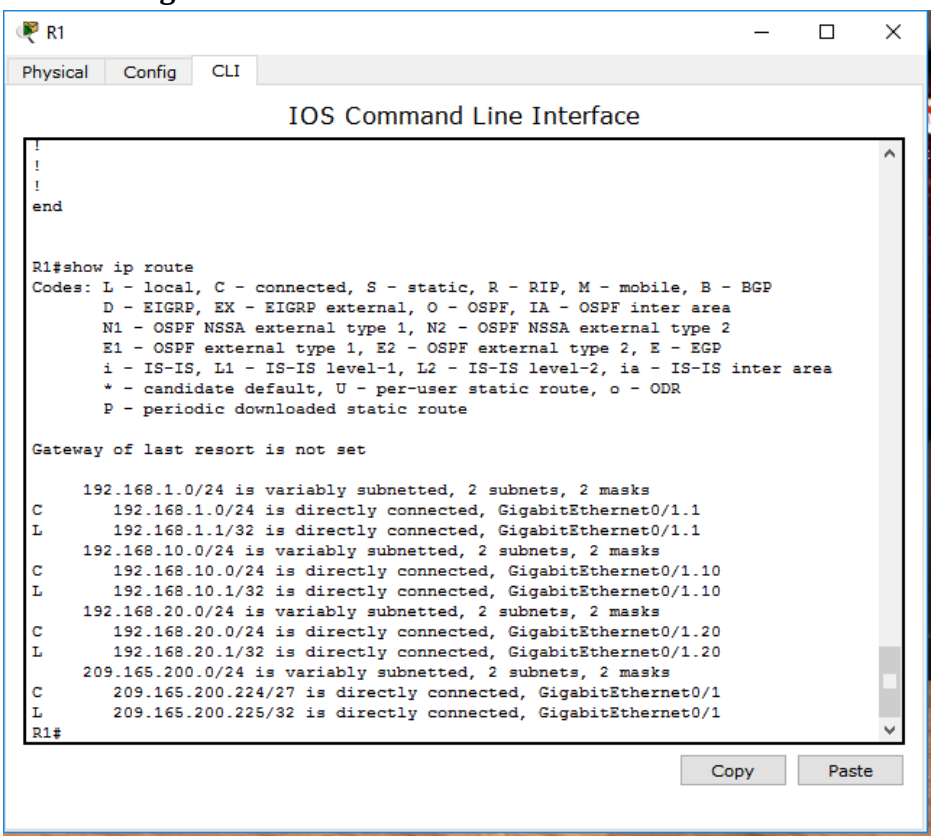
Router R1

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**

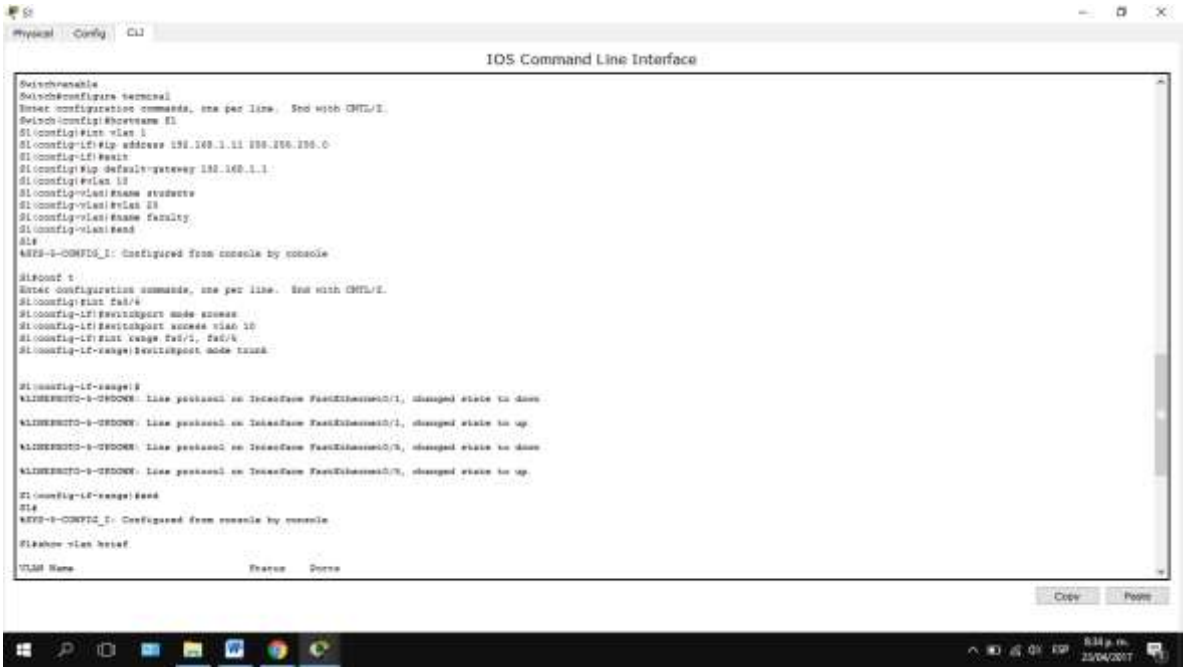
Configuración del router



Verificación de configuración del router



Configuración del S1

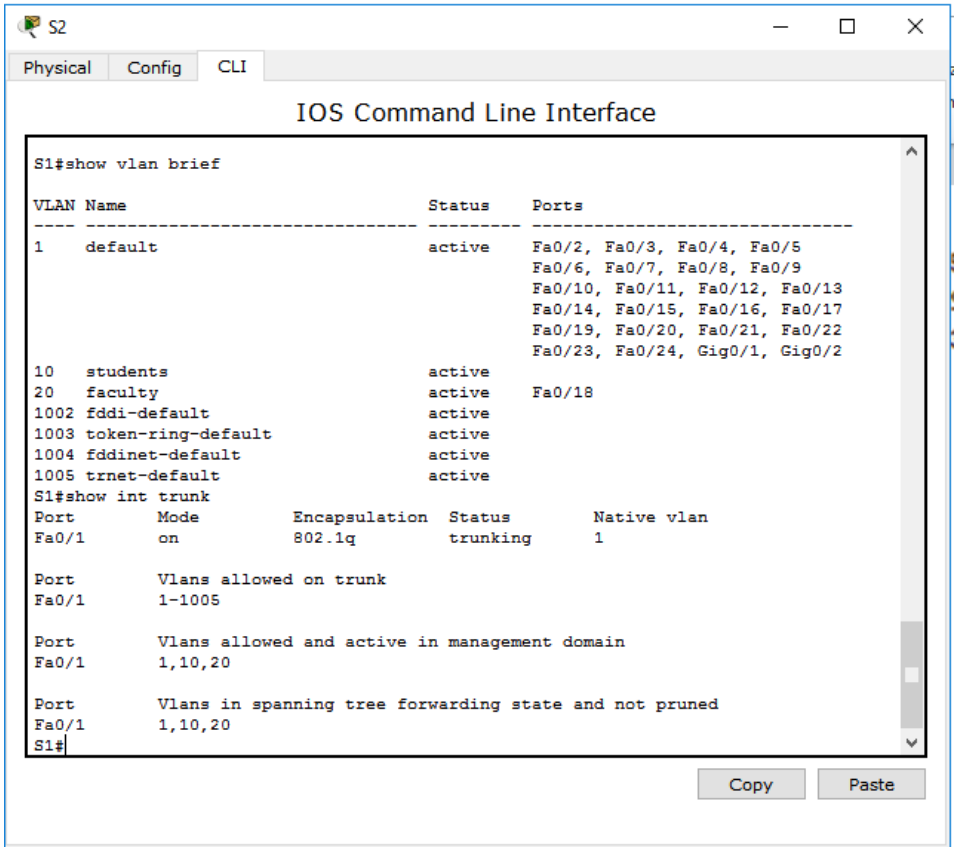


Verificación que se guardaron los cambios

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, 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   students                          active    Fa0/6
20   faculty                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/5       1,10,20
S1#
```

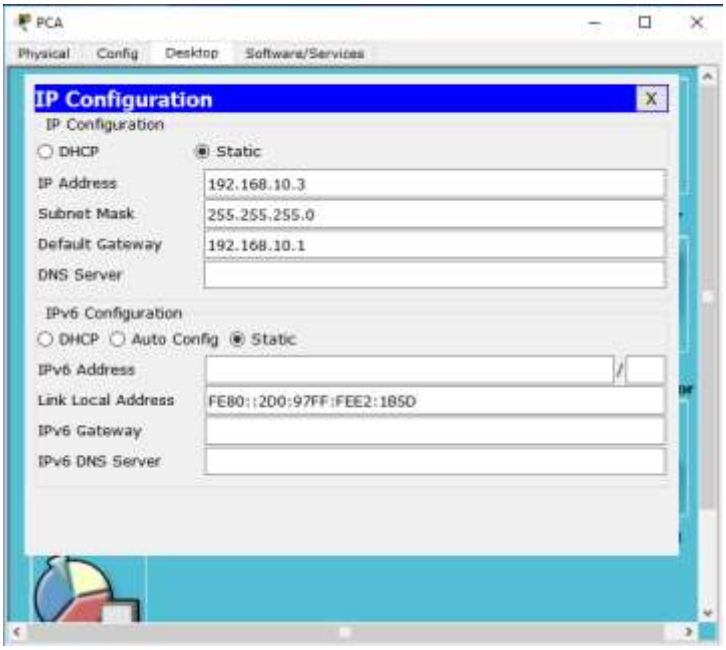
Configuración del S2

Verificación que se guardaron los cambios

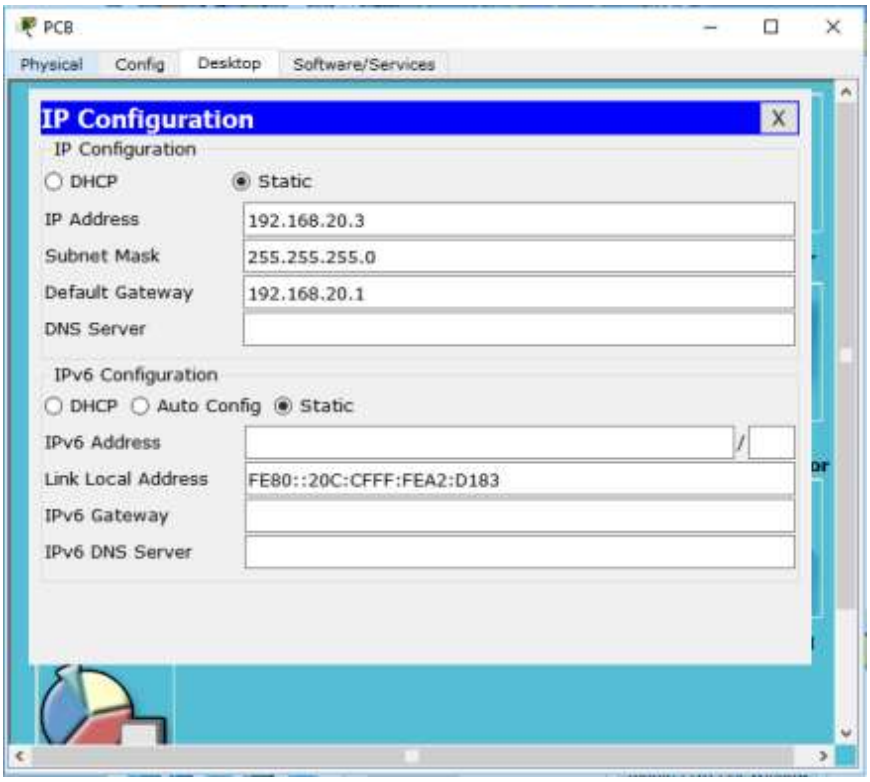


Configuración de las computadoras

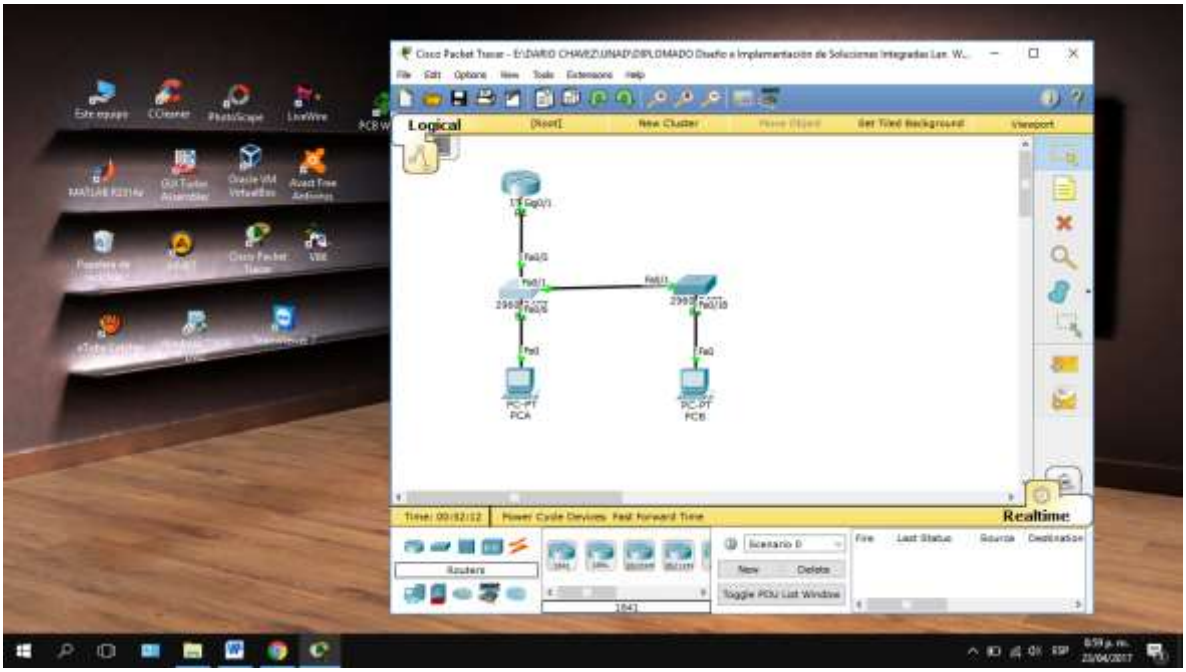
PCA



PCB



Red ya configurada

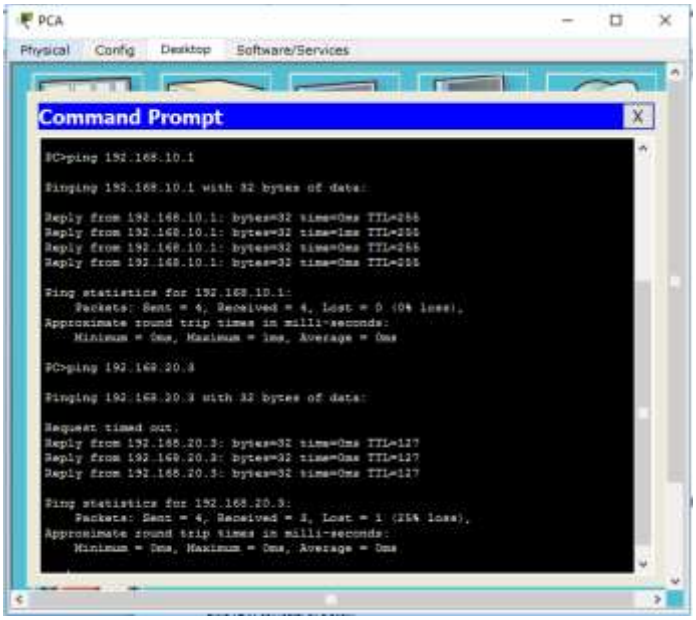


Paso 7. Verifique la conectividad.

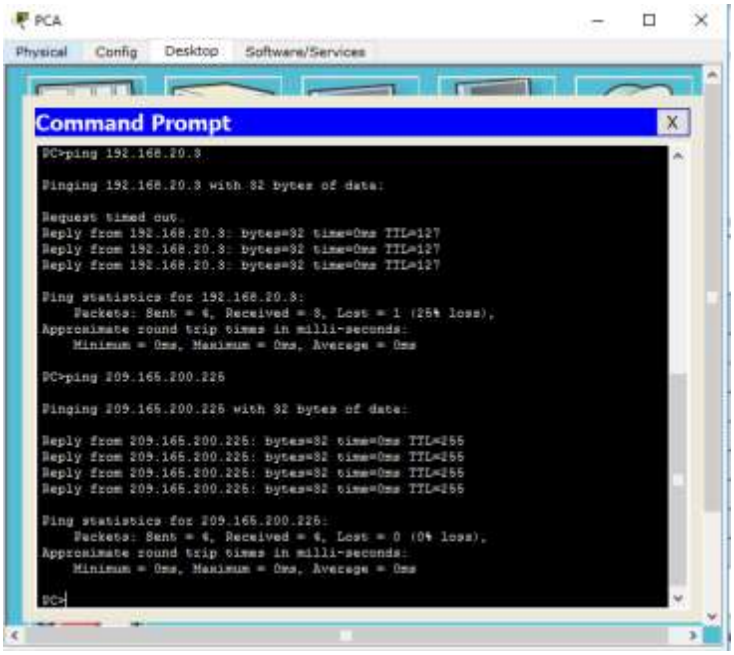
Introduzca el comando para ver la tabla de routing en el R1. ¿Qué redes se enumeran?

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

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

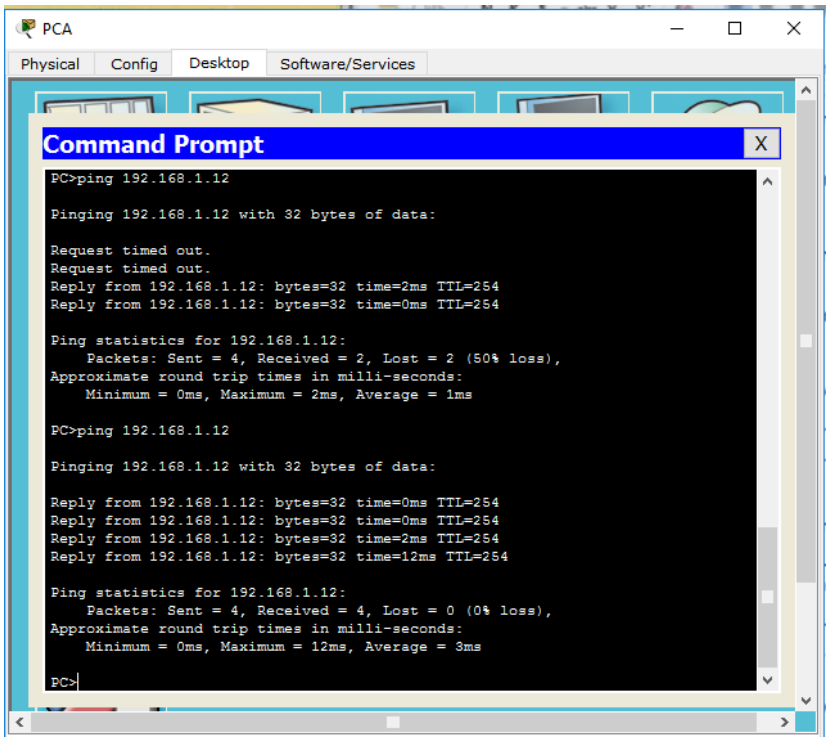


¿Es posible hacer ping de la PC-A a la interfaz Lo0? Si



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

.



6.2.2.5 Práctica De Laboratorio: Configuración de rutas estáticas y predeterminadas IPV4

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 15. 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 16. 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.

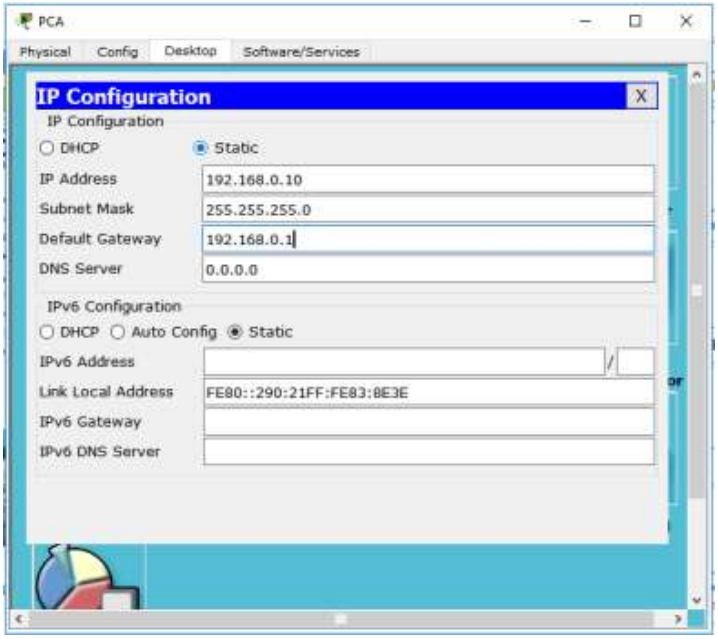
a. Configure los nombres de los dispositivos, como se muestra en la topología y en la tabla de direccionamiento.

b. Desactive la búsqueda del DNS.

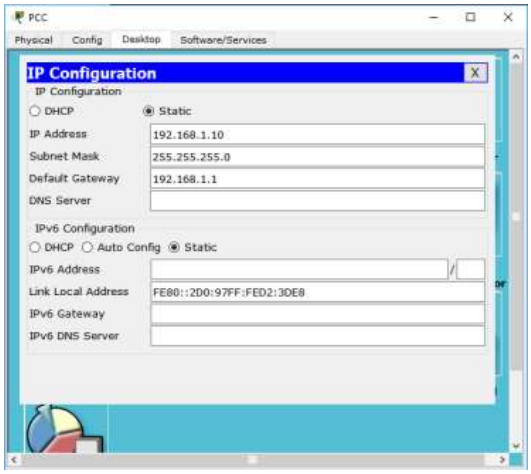
c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

Configuración de la ip del PCA



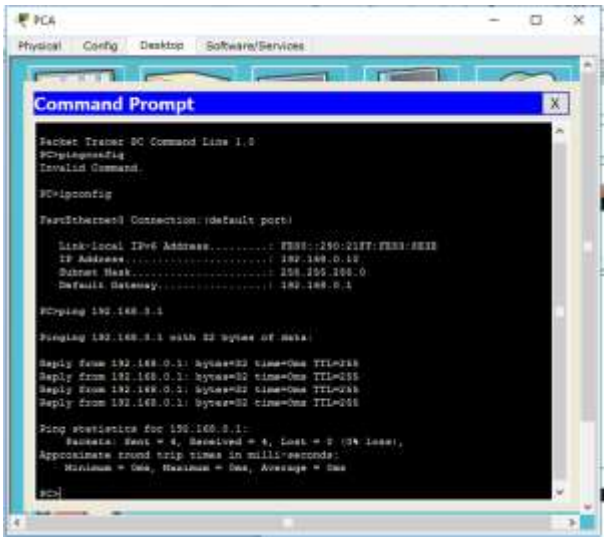
Configuración de la ip del PCB



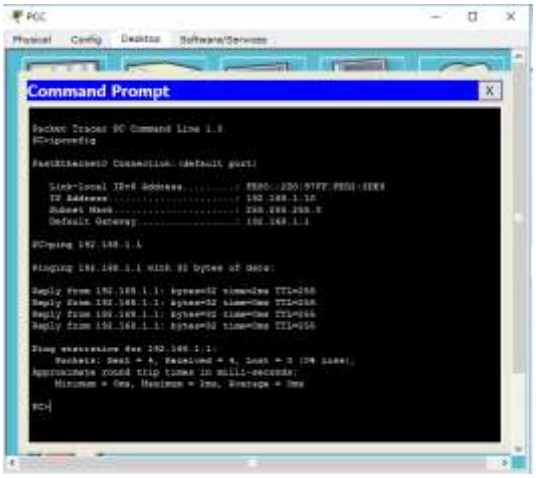
Configuración de R1

Configuración de R3

Se verifica conexión de las LANS



Ping PCA -PCC



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.

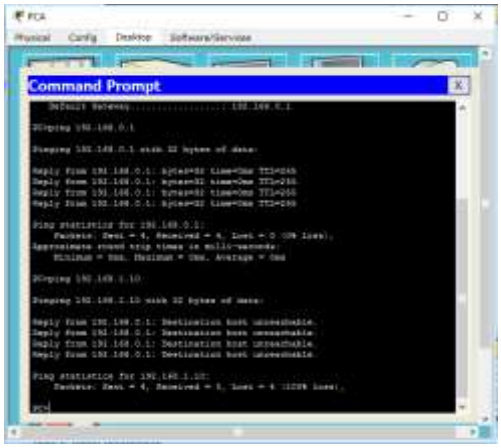
¿Es posible hacer ping del R1 a la interfaz S0/0/0 del R3? **_____si___**

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

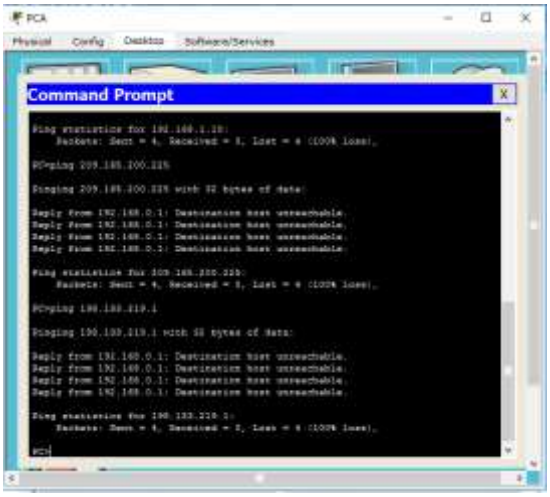
i. Pruebe la conectividad entre los dispositivos que no están conectados directamente.

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

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



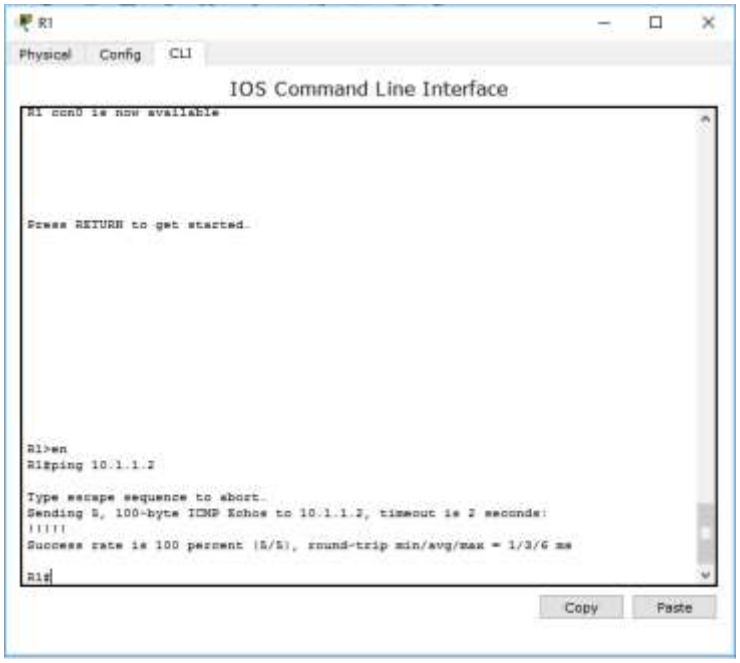
¿Es posible hacer ping de la PC-A a la interfaz Lo1? **___no_____**



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

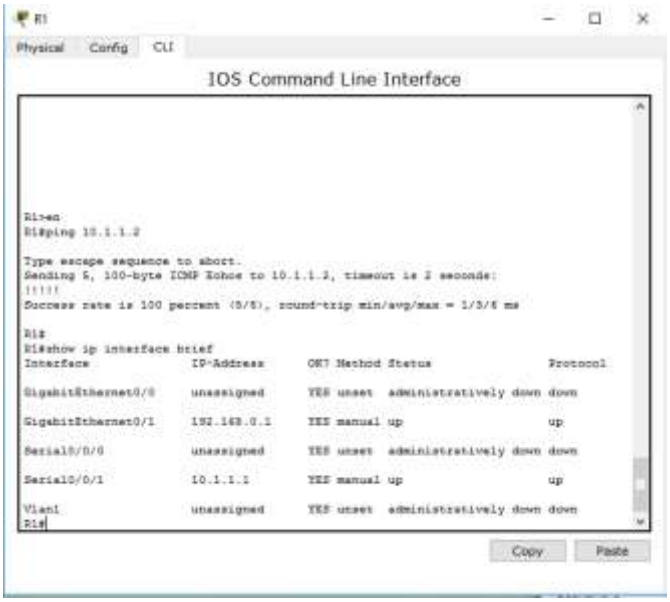
R/ No fueron satisfactorias porque le router no tiene rutas hacia redes distantes

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



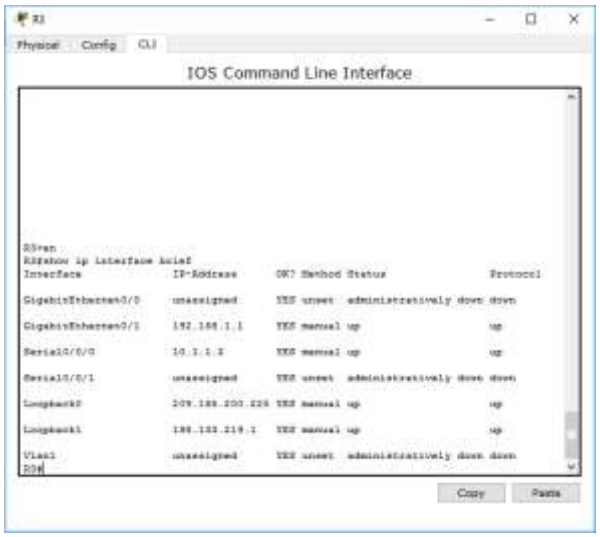
Paso 5. Reunir información.

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



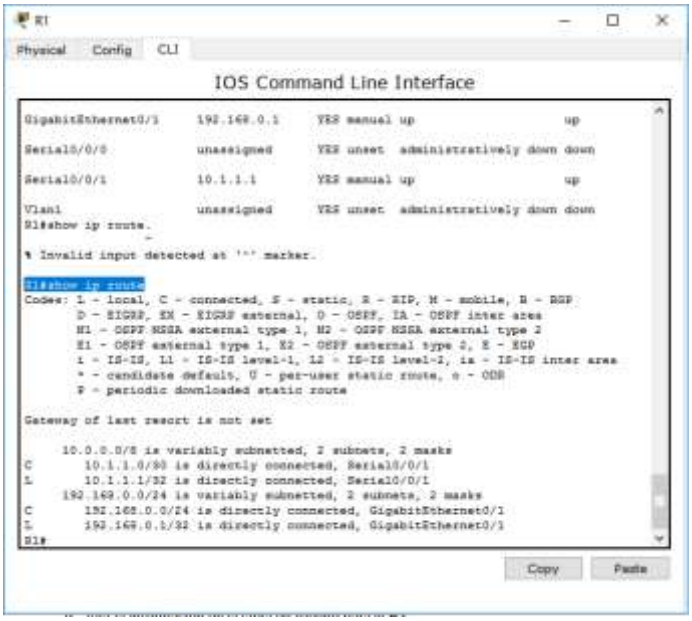
¿Cuántas interfaces están activadas en el R1? **2**

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



¿Cuántas interfaces están activadas en el R3? **4**

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

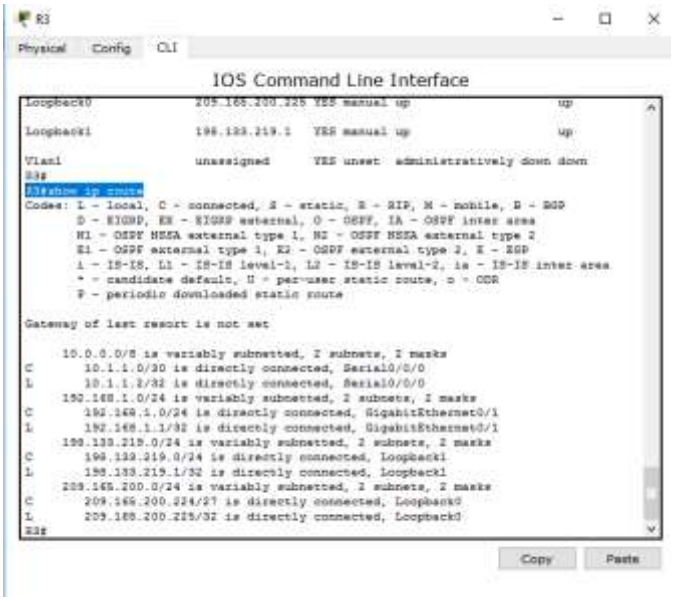


¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R1?

R/ Hacen falta

G0/1	192.168.1.1	255.255.255.0
Lo0	209.165.200.225	255.255.255.224
Lo1	198.133.219.1	255.255.255.0

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?

R/

Falta esta red

R1	G0/1	192.168.0.1	255.255.255.0	N/A

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

R/

Porque el router no está configurado con un protocolo de ruteo estático o dinámico y solo conoce sus redes directamente conectadas

Parte 17.

Parte 18. 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.

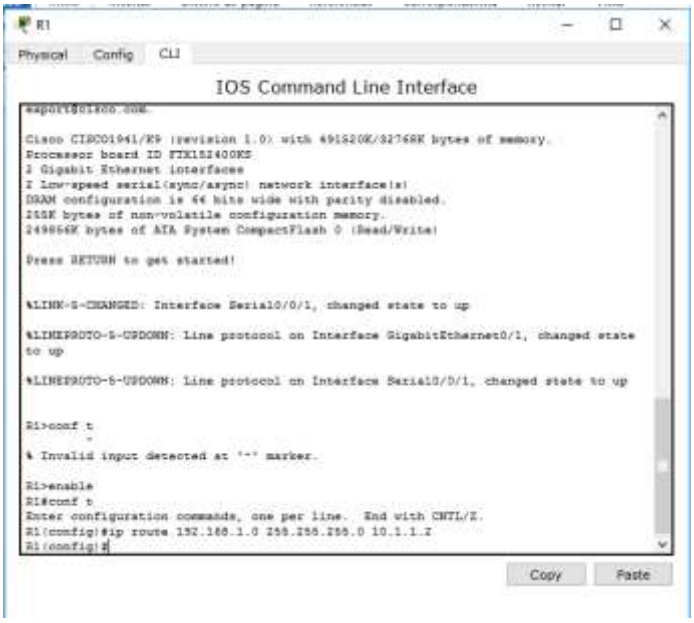
Nota: En esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos 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:

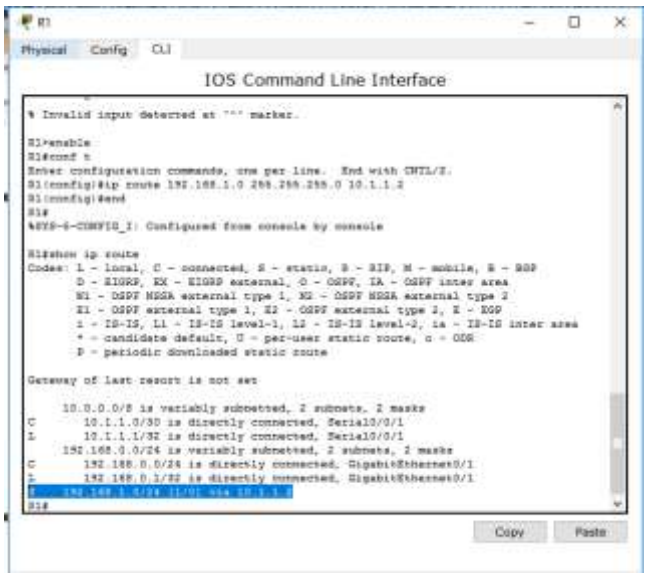
Router(config)# **ip route** *dirección-red máscara-subred dirección-ip*

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.

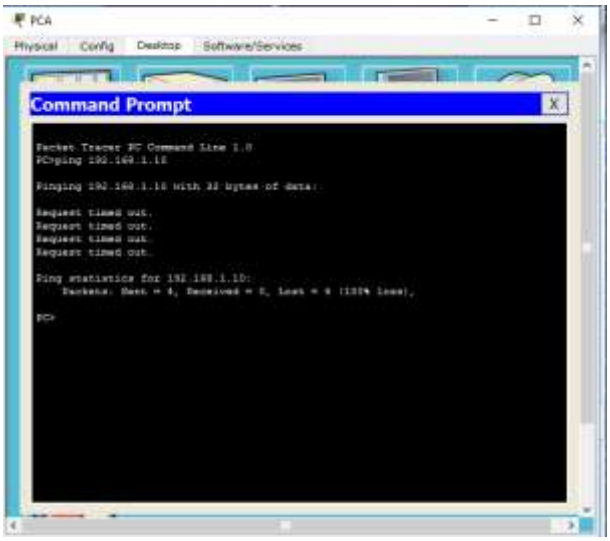


b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

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



¿Es posible hacer ping Del host PC-A host a al host PC-C? **No**



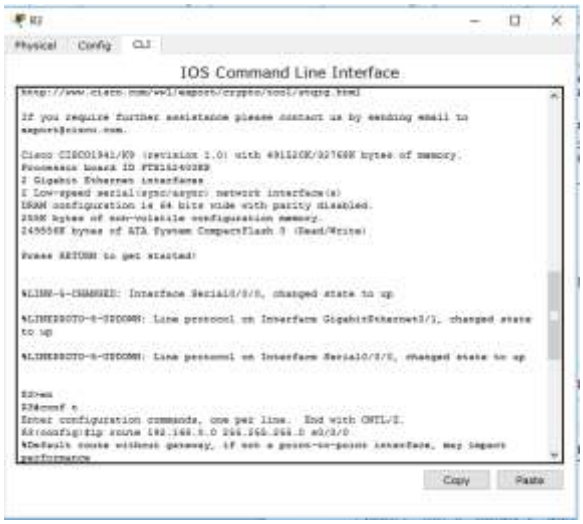
Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, este ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 192.168.0.0 en la tabla de routing.

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:

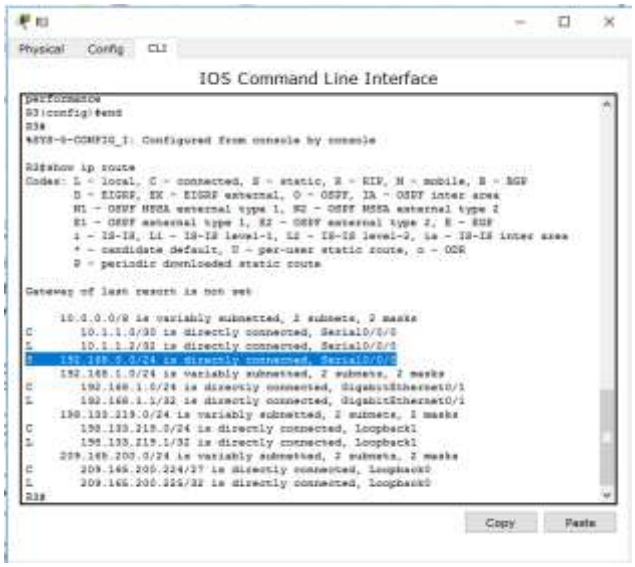
Router(config)# **ip route** *dirección-red máscara-subred interfaz-salida*

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.



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

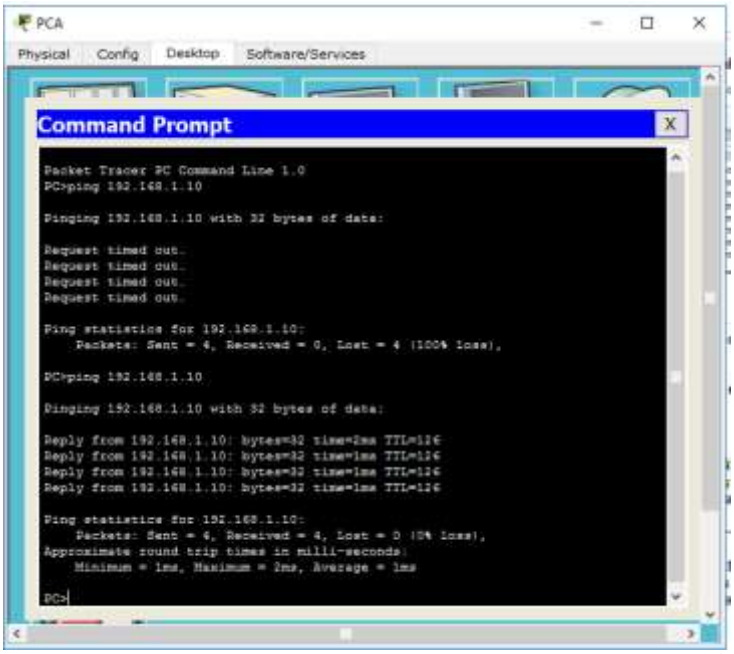
¿Cómo se indica esta ruta nueva en la tabla de routing?



e. ¿Es posible hacer ping Del host PC-A host al host PC-C? S**i**

Este ping debe tener éxito.

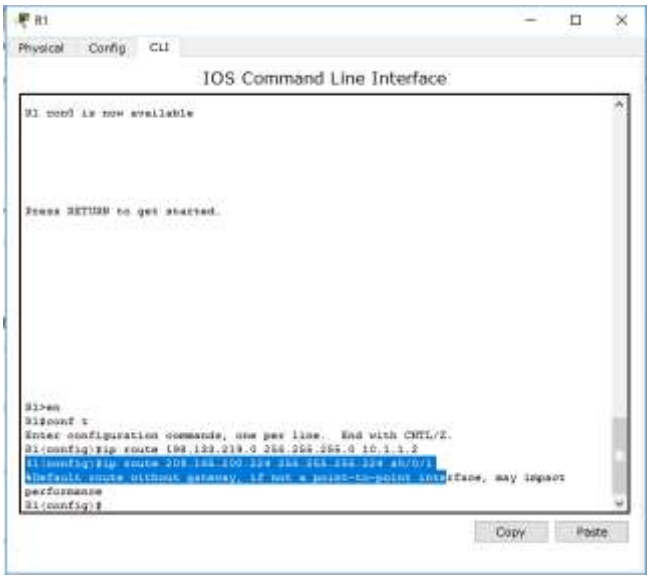
Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.



Paso 3. Configurar una ruta estática.

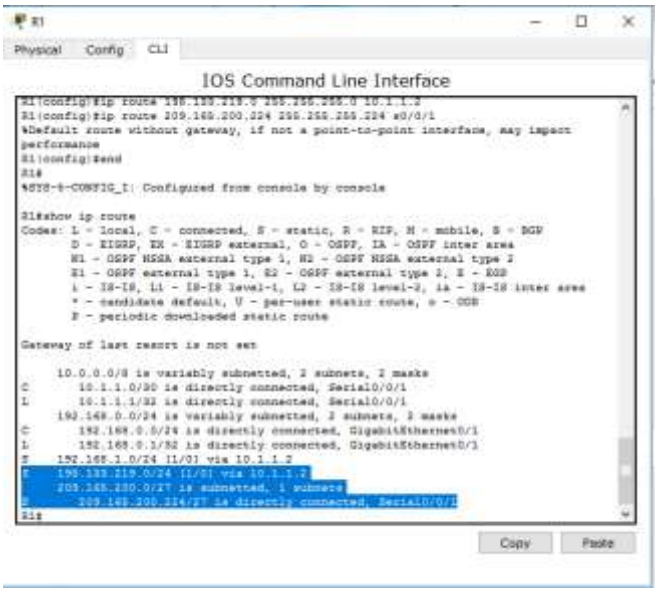
f. En el router R1, configure una ruta estática a la red 198.133.219.0 utilizando una de las opciones de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

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.



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

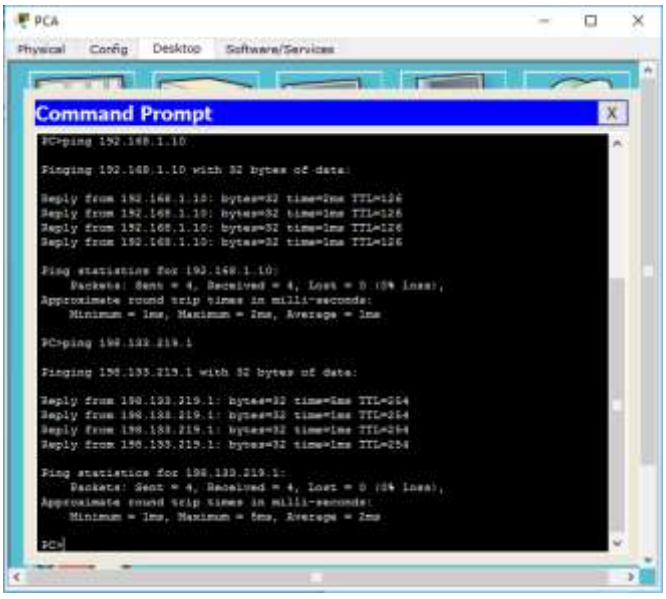
¿Cómo se indica esta ruta nueva en la tabla de routing?



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

SI

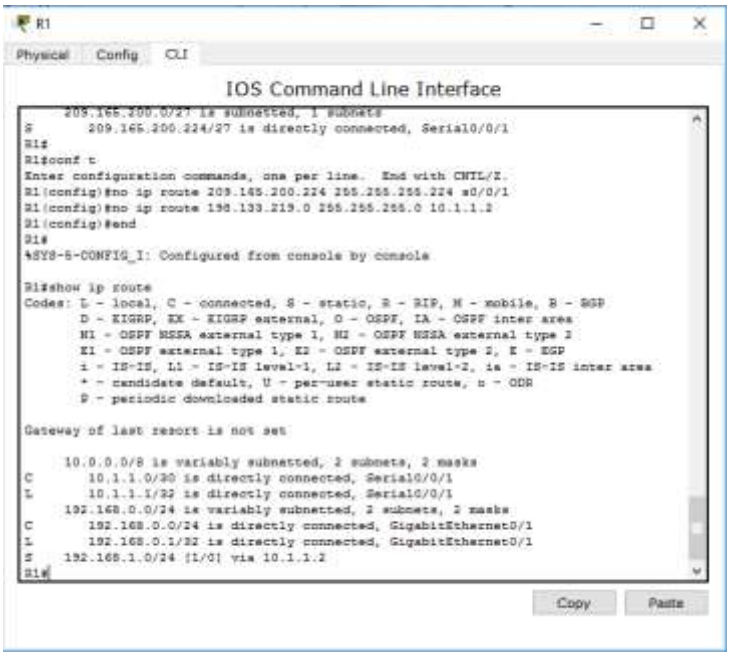
Este ping debe tener éxito.



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

j. 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 proporcionado, escriba los comandos que utilizó.

k. 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? **3 redes**

¿El gateway de último recurso está establecido? **No**

Parte 19. 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.

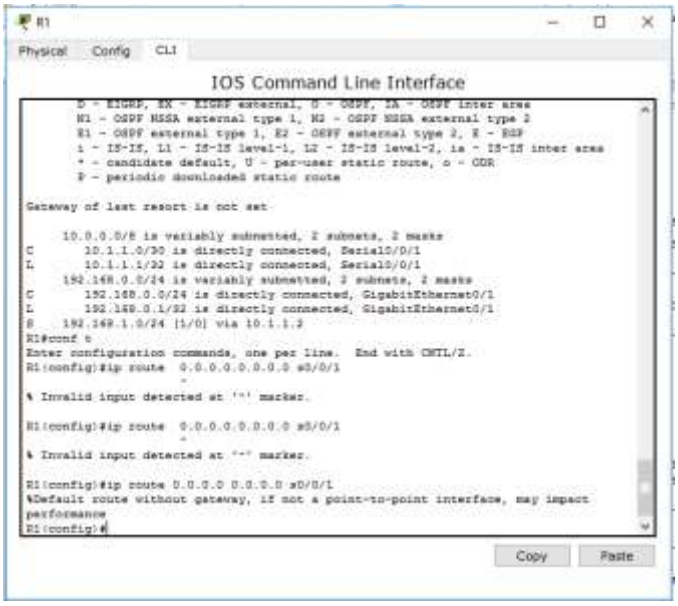
Una ruta predeterminada identifica el gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática

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”.

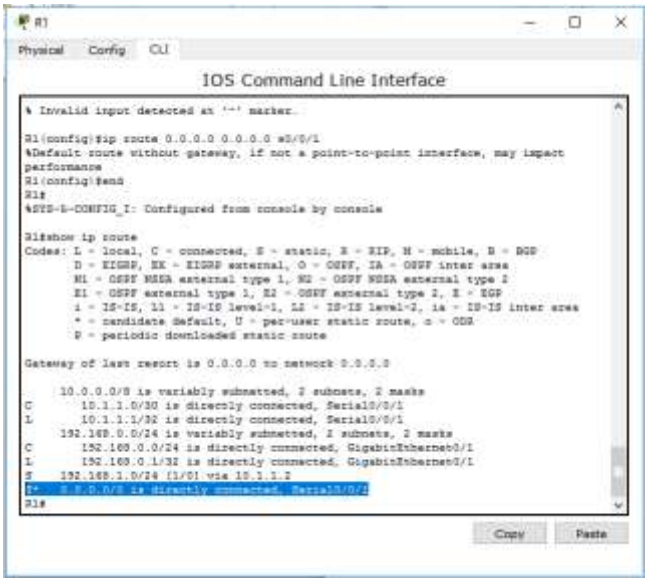
En una ruta predeterminada, se puede especificar la dirección IP del siguiente salto o la interfaz de salida. Para configurar una ruta estática predeterminada, utilice la siguiente sintaxis:

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.



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



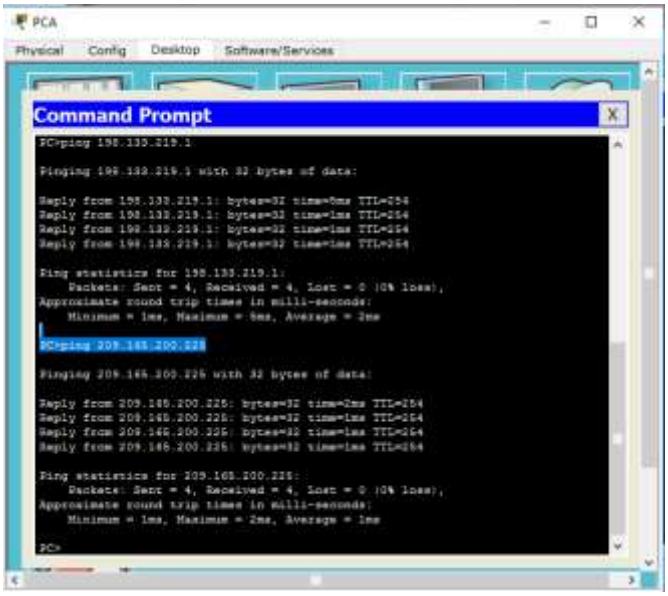
¿Cómo se indica esta ruta nueva en la tabla de routing?

Se indica de esta forma s*

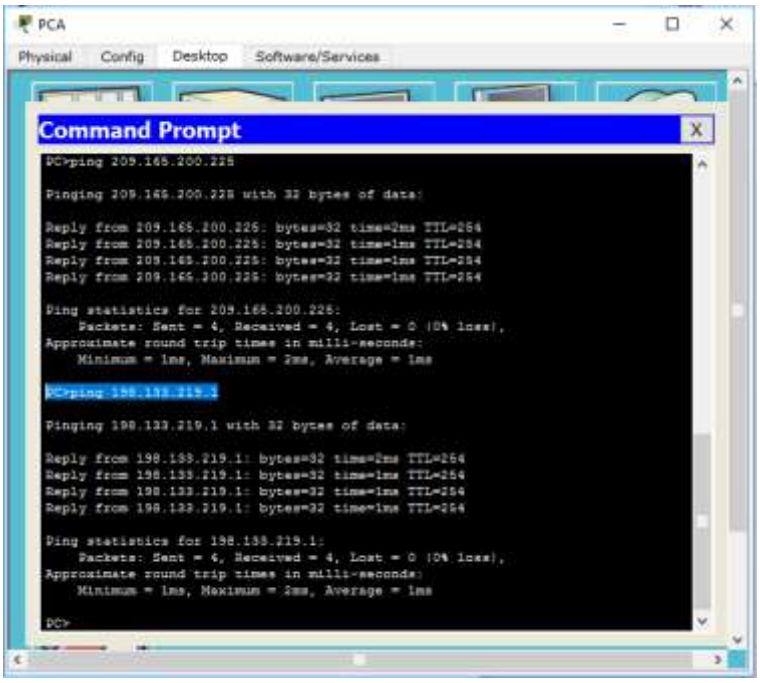
¿Cuál es el gateway de último recurso?

S* 0.0.0.0/0

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



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



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?

   R/

   Se usaría el siguiente comando

   Enable

   Conf t

   ip route 192.168.3.0 255.255.255.0 10.1.1.1

   ip route192.168.3.0 255.255.255.0 s0/0/0

   or ip route 0.0.0.0 0.0.0.0 s0/0/0

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

   R/

   El beneficio es que cuando se usa una ruta estática directamente conectada

   Las interfaces de salida se resuelven en una sola búsqueda, mientras que una ruta estática recursiva se necesita dos búsquedas para resolver las interfaces de salida

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

   R/ porque ayuda a enviar paquetes a redes desconocidas

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**

o

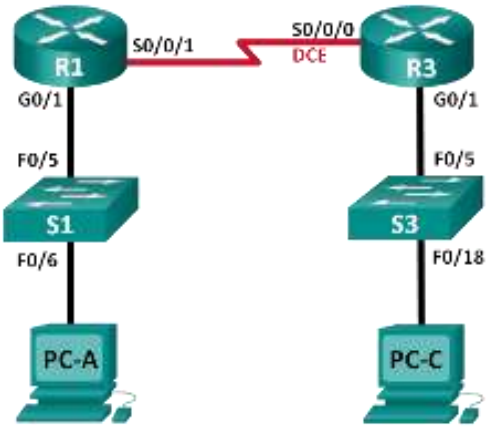
R1(config)# **no ip route 209.165.200.224 255.255.255.224**

Configuración de rutas predeterminadas

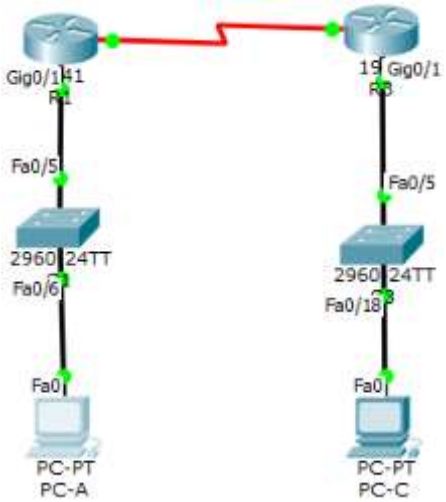
R1(config)# **ip route 0.0.0.0 0.0.0.0 s0/0/1**

Laboratorio: 6.2.4.5. Configuración de rutas estáticas y predeterminadas IPv6.

Topología de la guía:



Topología del laboratorio:



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

Tabla de direccionamiento:

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).

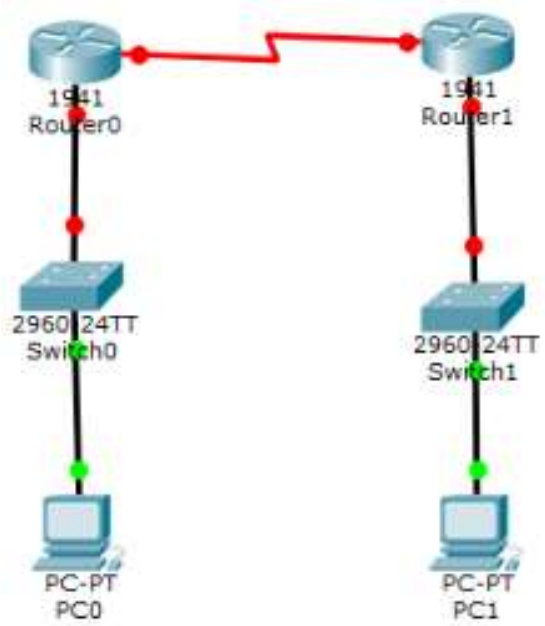
* Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola.

*Cables Ethernet y seriales, como se muestra en la topología

Parte 1: 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.

- **R1:**

```
Router> enable
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
```

- **R3:**

```
Router> enable
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
```

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.

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

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

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

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

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

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R1(config-if)# exit
R1(config)#
```

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

```
R1(config)#
R1(config)# interface serial0/0/1
R1(config-if)# ipv6 address FC00::1/64
R1(config-if)# exit
R1(config)#
```

d. Asigne un nombre de dispositivo al router R3.

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

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

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

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

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)# interface g0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64
R3(config-if)# no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

R3(config-if)#exit
R3(config)#
```

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**

```
R3(config)# interface serial0/0/0
R3(config-if)# ipv6 address FC00::2/64
R3(config-if)# No shutdown

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

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

a. 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.

b. 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.

c. 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.

d. 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**.

e. 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.

f. 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.

- **PC-A:**

- **PC-C:**

Paso 5: Usar ipconfig y ping para verificar la conectividad LAN.

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

```
Packet Tracer PC Command Line 1.0
PC> ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0001.97E8.2C5B
   Link-local IPv6 Address.....: FE80::201:97FF:FEE8:2C5B
   IP Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: 0.0.0.0
   DNS Servers.....: 0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-1D-BC-9C-DC-00-01-97-E8-2C-5B


PC>
```

```
PC> ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.....: 0001.97E8.2C5B
   Link-local IPv6 Address.....: FE80::201:97FF:FEE8:2C5B
   IPv6 Address.....: 2001:DB8:ACAD:A:201:97FF:FEE8:2C5B/64
   Default Gateway.....: FE80::202:16FF:FE4A:E802
   DNS Servers.....: ::
   DHCPv6 Client DUID.....: 00-01-00-01-1D-BC-9C-DC-00-01-97-E8-2C-5B

PC>
```

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?

Rta: Si.

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

Rta: Es 2001:DB8:ACAD:A:201:97FF:FEE8:2C5B/64

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

Rta: Es FE80::201:97FF:FEE8:2C5B

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

Rta: Es FE80::202:16FF:FE4A:E802

d. 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>**

```
PC> ping FE80::202:16FF:FE4A:E802

Pinging FE80::202:16FF:FE4A:E802 with 32 bytes of data:

Reply from FE80::202:16FF:FE4A:E802: bytes=32 time=67ms TTL=255
Reply from FE80::202:16FF:FE4A:E802: bytes=32 time=0ms TTL=255
Reply from FE80::202:16FF:FE4A:E802: bytes=32 time=0ms TTL=255
Reply from FE80::202:16FF:FE4A:E802: bytes=32 time=0ms TTL=255

Ping statistics for FE80::202:16FF:FE4A:E802:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 67ms, Average = 16ms

PC>
```

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

Rta: Si.

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 67ms, Average = 16ms
```

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

```
PC> ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.................: 0001.965B.647A
   Link-local IPv6 Address.........: FE80::201:96FF:FE5B:647A
   IPv6 Address....................: 2001:DB8:ACAD:B:201:96FF:FE5B:647A/64
   Default Gateway.................: FE80::260:2FFF:FEDE:6202
   DNS Servers.....................: ::
   DHCPv6 Client DUID..............: 00-01-00-01-50-3D-53-40-00-01-96-5B-64-7A

PC>
```

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

Rta: Si.

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

Rta: Es 2001:DB8:ACAD:B:201:96FF:FE5B:647A/64

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

Rta: Es FE80:: 201:96FF:FE5B:647A

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

Rta: Es FE80:: 260:2FFF:FEDE:6202

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

```
PC> ping FE80::260:2FFF:FEDE:6202

Pinging FE80::260:2FFF:FEDE:6202 with 32 bytes of data:

Reply from FE80::260:2FFF:FEDE:6202: bytes=32 time=1ms TTL=255
Reply from FE80::260:2FFF:FEDE:6202: bytes=32 time=0ms TTL=255
Reply from FE80::260:2FFF:FEDE:6202: bytes=32 time=0ms TTL=255
Reply from FE80::260:2FFF:FEDE:6202: bytes=32 time=0ms TTL=255

Ping statistics for FE80::260:2FFF:FEDE:6202:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

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

Rta: Si.

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

PC>
```

k. 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*

```
PC> ping 2001:DB8:ACAD:B:201:96FF:FE5B:647A

Pinging 2001:DB8:ACAD:B:201:96FF:FE5B:647A with 32 bytes of data:

Reply from 2001:DB8:ACAD:A:202:16FF:FE4A:E802: Destination host unreachable.
Reply from 2001:DB8:ACAD:A:202:16FF:FE4A:E802: Destination host unreachable.
Reply from 2001:DB8:ACAD:A:202:16FF:FE4A:E802: Destination host unreachable.
Reply from 2001:DB8:ACAD:A:202:16FF:FE4A:E802: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:B:201:96FF:FE5B:647A:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

¿El ping se realizó correctamente?

Rta: Fallaron los pings.

¿Por qué o por qué no?

Rta: El ping falla por que los router no tienen configurado rutas estéticas o dinámicas y solo conocen acerca de sus redes directa mente conectas sin las rutas apropiadas los router descartaran los paquetes destinados hacia redes desconocidas.

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

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

```
R1# show ipv6 interface brief
GigabitEthernet0/0         [administratively down/down]
GigabitEthernet0/1         [up/up]
    FE80::202:16FF:FE4A:E802
    2001:DB8:ACAD:A:202:16FF:FE4A:E802
Serial0/0/0                [administratively down/down]
Serial0/0/1                [administratively down/down]
    FE80::202:16FF:FE4A:E801
    FC00::1
Vlan1                      [administratively down/down]
R1#
```

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

Rta: Las dos direcciones so: FE80::202:16FF:FE4A:E802. Esta es una dirección IPv6 link-local; y 2001:DB8:ACAD:A:202:16FF:FE4A:E802. Esta es una dirección IPv6 de unidifusión global.

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

Rta: L as direcciones en la s0/0/1 son: FE80::202:16FF:FE4A:E801. Es dirección IPv6 link-local; y la dirección FC00::1, la cual es una dirección IPv6 de unidifusión global.

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

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::202:16FF:FE4A:E802
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A:202:16FF:FE4A:E802, subnet is 2001:DB8:ACAD:A::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF4A:E802
  MTU is 1500 bytes

Serial0/0/1 is administratively down, line protocol is down
  IPv6 is tentative, link-local address is FE80::202:16FF:FE4A:E801 [TEN]
  No Virtual link-local address(es):
  Global unicast address(es):
    FC00::1, subnet is FC00::/64 [TEN]
  Joined group address(es):
    FF02::1
  MTU is 1500 bytes
```

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

Rta: Las direcciones multidifusión encontradas son: FF02::1, FF02::2 y FF02::1:FF4A:E802.

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

Rta: La dirección del grupo multidifusión de s0/0/1 es: FF02::1.

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

Rta: La dirección de multidifusión FF02::1 sirve en todos los modos de los segmentos de la red local.

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

Rta: La multidifusión FF02::2 es usada en todos los router en el segmento de red local.

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

Rta: Son las de divisiones de multidifusión de nodos solicitados, cada interface unicast o enicast tiene que tener un nodo multicast solicitado para resolver las direcciones de las direcciones de los vecinos en el enlace local.

c. 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.

```
R1# show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

        D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A:202:16FF:FE4A:E802/128 [0/0]
     via GigabitEthernet0/1, receive
C   FC00::/64 [0/0]
     via Serial0/0/1, directly connected
L   FC00::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

¿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?

Rta: El motivo por el cual no hizo ping es porque no hay rutas.

Parte 2: 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)#

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 serial0/0/1
R1(config)#
```

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

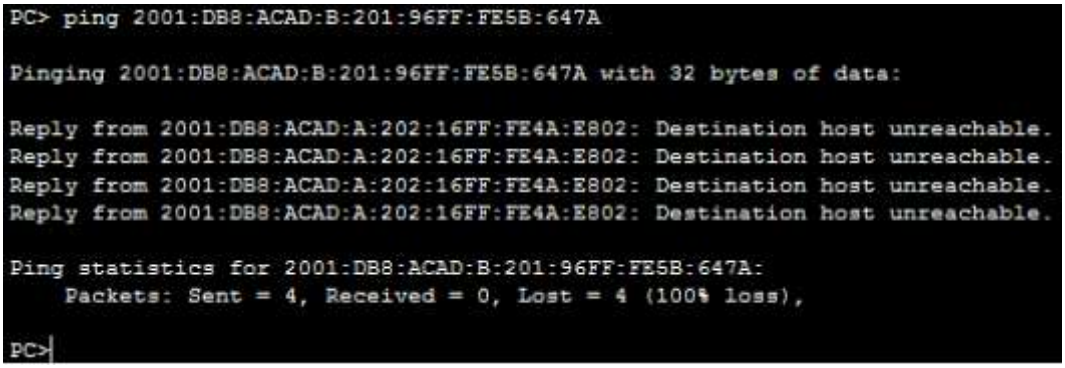
```
R1# show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
       D - EIGRP, EX - EIGRP external
C    2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L    2001:DB8:ACAD:A:202:16FF:FE4A:E802/128 [0/0]
     via GigabitEthernet0/1, receive
S    2001:DB8:ACAD:B::/64 [1/0]
     via Serial0/0/1, receive
C    FC00::/64 [0/0]
     via Serial0/0/1, directly connected
L    FC00::1/128 [0/0]
     via Serial0/0/1, receive
L    FF00::/8 [0/0]
     via Null0, receive
R1#
```

¿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?

Rta: Se identifica con la letra "S".

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



Rta: Aun no es posible hacer ping.

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)#

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 serial0/0/0
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.

```
PC> ping 2001:DB8:ACAD:B:201:96FF:FE5B:647A

Pinging 2001:DB8:ACAD:B:201:96FF:FE5B:647A with 32 bytes of data:

Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=10ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B:201:96FF:FE5B:647A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms

PC>
```

¿El ping se realizo corretamente? ¿Por qué?

Rta: Las rutas estáticas configuradas en R1 y R3 hacen que el ping sea satisfactorio.

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*>

***a.* 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**

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 serial0/0/1
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# EXIT
R1#
```

b. 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**

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 serial0/0/0
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# EXIT
R3#
```

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

```
R1# show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A:202:16FF:FE4A:E802/128 [0/0]
     via GigabitEthernet0/1, receive
S   2001:DB8:ACAD:B::/64 [1/0]
     via FC00::2, receive
C   FC00::/64 [0/0]
     via Serial0/0/1, directly connected
L   FC00::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

¿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?

Rta: Está con la letra "S" ubicándose de tercera en la tabla.

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

```
PC> ping 2001:db8:acad:b:201:96ff:fe5b:647a

Pinging 2001:db8:acad:b:201:96ff:fe5b:647a with 32 bytes of data:

Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=18ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=11ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=12ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=10ms TTL=126

Ping statistics for 2001:DB8:ACAD:B:201:96FF:FE5B:647A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 18ms, Average = 12ms

PC>
```

¿El ping se realizó correctamente?

Rta: 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>*

a. 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)#

```
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# ipv6 route ::/0 serial0/0/1
R1(config)# exit
R1#
```

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

```
R3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# ipv6 route ::/0 serial0/0/0
R3(config)# exit
R3#
```

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

```
R1# show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via Serial0/0/1, receive
C   2001:DB8:ACAD:A::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A:202:16FF:FE4A:E802/128 [0/0]
     via GigabitEthernet0/1, receive
C   FC00::/64 [0/0]
     via Serial0/0/1, directly connected
L   FC00::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

¿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?

Rta: Está identificada con la letra "S", y se encuentra de primera en la entrada en la tabla.

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

```
PC> ping 2001:DB8:ACAD:B:201:96FF:FE5B:647A

Pinging 2001:DB8:ACAD:B:201:96FF:FE5B:647A with 32 bytes of data:

Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:ACAD:B:201:96FF:FE5B:647A: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:ACAD:B:201:96FF:FE5B:647A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>
```

*¿**El ping se realizó correctamente?***

Rta: Al hacer ping a la PC-C, este es satisfactorio.

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?***

Rta: Sí, porque actual mente se está implementando las redes ipv6 y en un futuro se va a poder conectar con las configuraciones ipv6, entonces ya podemos elegir si nos conectamos con ipv4 o ipv y para esto es necesario configurar. En una transición se podrían utilizar la ipv4 y la ipv6 al mismo tiempo.

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?***

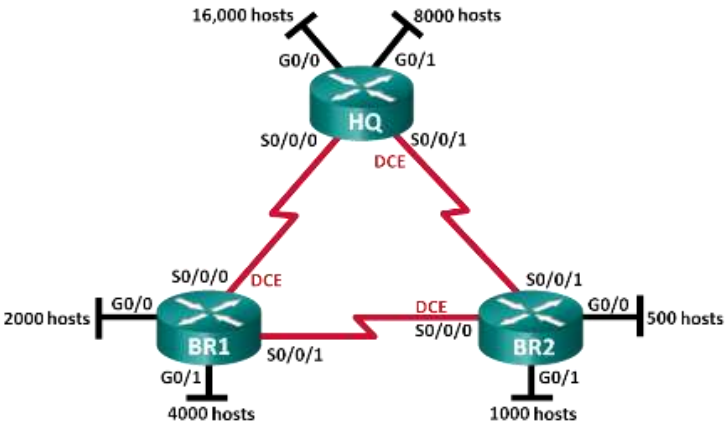
Rta: Cuando se configura una ruta estática en ipv6 se utiliza el comando ipv6 route en vez de ip route. La necesidad e ingresar show ipv6 route para ver la tabla de ruteo de ipv67 comparada con la tabla de ruteo ipv4 con el comando show ip route.

Tabla de resumen de interfaces del router:

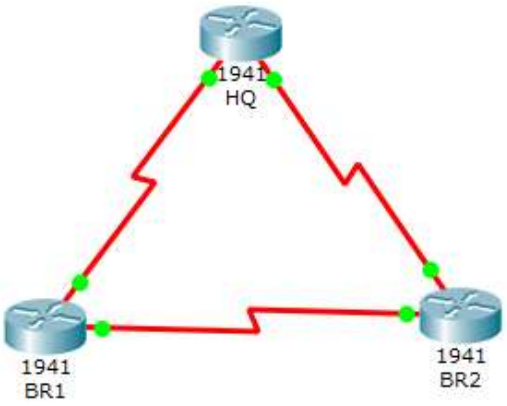
Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet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

Laboratorio: 6.3.3.7. Diseño e Implementación de Direccionamiento IPv4 con VLSM.

Topología de la guía:



Topología del laboratorio:



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?

Rta: Se encuentran disponibles 32766 host.

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

Rta: 31506

Subredes	**Cantidad de host.**
HQ G0/0	16.000
HQ G0/1	8.000
BR1 G0/0	2.000
BR1 G0/1	4.000
BR2 G0/0	500
BR2 G0/1	1.000
HQ – BR1	2
HQ – BR2	2
BR1 – BR2	2
TOTAL	31.506 Host.

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

Rta: 9 subredes.

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)

Rta: La subred más grande es la del enlace HQ G0/0 (16000 Host) (LAN-A).

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

Rta: Se necesitan 16000 IP.

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones?

Rta: 18

¿Cuántas direcciones host admite esa subred?

Rta: Admite 16382.

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

Rta: Si.

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

Rta: Se forman la 128 y la 192.

Utilice la primera dirección de red para esta subred.

Paso 3: Determinar la segunda subred más grande que se necesita.

Descripción de la subred.

Rta: La segunda subred más grande es la del enlace HQ G0/1 (8000 Host) (LAN-B).

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

Rta: Se necesitan 8000 IP.

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

Rta: La máscara de subred más pequeña que admite esta cantidad es la 19.

¿Cuántas direcciones host admite esa subred?

Rta: Admite 8190 host.

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

Rta: Si.

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

Rta: la 192 y la 224.

Utilice la primera dirección de red para esta subred.

Paso 4: Determinar la siguiente subred más grande que se necesita.

Descripción de la subred

Rta: La siguiente subred más grande es la de BR1 G0/1 (4000 Host) (LAN-D)

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

Rta: Para esta subred se necesitan 4000 Ip.

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

Rta: La más pequeña es la 20.

¿Cuántas direcciones host admite esa subred?

Rta: Esta subred admite 4094 Host.

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

Rta: Si.

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

Rta: La 224 y la 240.

Utilice la primera dirección de red para esta subred.

Paso 5: Determinar la siguiente subred más grande que se necesita.

Descripción de la subred

Rta: La siguiente subred más grande es la de BR1 G0/0 (2000 Host) (LAN-C)

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

Rta: Se necesitan 2000 Ip.

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

Rta: La más pequeña es la subred 21.

¿Cuántas direcciones host admite esa subred?

Rta: Admite 20146 Host.

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

Rta: Si.

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

Rta: La 240 y la 248.

Utilice la primera dirección de red para esta subred.

Paso 6: Determinar la siguiente subred más grande que se necesita.

Descripción de la subred

Rta: A las anteriores le sigue la subred BR2 G0/1 (1000 Host) (LAN-F)

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

Rta: Para esta subred son necesarias 1000 Ip.

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

Rta: La más pequeña es la subred 22.

¿Cuántas direcciones host admite esa subred?

Rta: Admite 1022 Host.

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

Rta: Si.

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

Rta: la 248 y la 252.

Utilice la primera dirección de red para esta subred.

Paso 7: Determinar la siguiente subred más grande que se necesita.

Descripción de la subred

Rta: La siguiente subred más grande es la de BR2 G0/0 (500 Host) (LAN-E)

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

Rta: Para esta red son necesarias 500 Ip.

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

Rta: La más pequeña es la 23.

¿Cuántas direcciones host admite esa subred?

Rta: Esta subred admite 510 Host.

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

Rta: Si.

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

Rta: La 252 y la 254.

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?

Rta: Para cada enlace de subred serial se necesitan 2 host.

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones host?

Rta: La subred más pequeña que admite esta subred es la 30.

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

Rta: Se obtienes las subredes.

b. 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.

Rta: Están 172.16.254.1/30, 172.16.254.4/30, 172.16.254.8/30

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

Rta: HQ – BR1, HQ – BR2, 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.

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	172.16.128.1/18	172.16.191.255/18
HQ G0/1	8 000	172.16.192.0/19	172.16.192.1/19	172.16.223.255/19
BR1 G0/1	4 000	172.16.224.0/20	172.16.224.1/20	172.16.239.255/20
BR1 G0/0	2 000	172.16.240.0/21	172.16.240.1/21	172.16.247.255/21
BR2 G0/1	1.000	172.16.248.0/22	172.16.248.1/22	172.16.251.255/22
BR2 G0/0	500	172.16.252.0/23	172.16.252.1/23	172.16.253.255/23
HQ S0/0/0-BR1 S0/0/0	2	172.16.254.0/30	172.16.254.1/30	172.16.254.3/30
HQ S0/0/1-BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5/30	172.16.254.7/30
BR1 S0/0/1-BR2 S0/0/0	2	172.16.254.8/30	172.16.254.9/30	172.16.254.11/30

Paso 2: Completar la tabla de direcciones de interfaces de dispositivos.

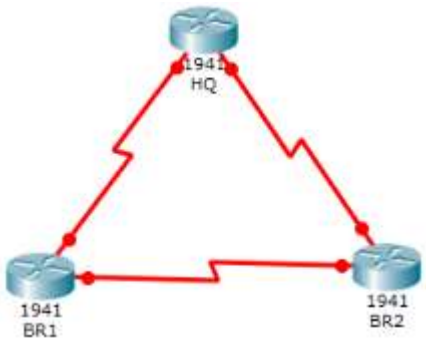
Asigne la primera dirección host en la subred a las interfaces Ethernet. A HQ se le debería asignar la primera dirección host en los enlaces seriales a BR1 y BR2. A BR1 se le debería asignar la primera dirección host para el enlace serial a BR2.

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.

- **HQ:**

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname HQ
HQ(config)#EXIT
HQ#
```

- **BR1:**

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname BR1
BR1(config)# EXIT
BR1#
```

- **BR2:**

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname BR2
BR2(config)# EXIT
BR2#
```

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

- **HQ:**

```
HQ# CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)# no ip domain-lookup
HQ(config)#
```

- **BR1:**

```
BR1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR1(config)# no ip domain-lookup
BR1(config)#
```

- **BR2:**

```
BR2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR2(config)# no ip domain-lookup
BR2(config)#
```

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

- **HQ:**

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

- **BR1:**

```
BR1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR1(config)# enable password class
BR1(config)#
```

- **BR2:**

```
BR2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR2(config)# enable password class
BR2(config)#
```

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

- **HQ:**

```
HQ(config)# line console 0
HQ(config-line)# password cisco
HQ(config-line)# login
HQ(config-line)# exit
HQ(config)#
```

- **BR1:**

```
BR1(config)# line console 0
BR1(config-line)# password cisco
BR1(config-line)# login
BR1(config-line)# exit
BR1(config)#
```

- **BR2:**

```
BR2(config)# line console 0
BR2(config-line)# password cisco
BR2(config-line)# login
BR2(config-line)# exit
BR2(config)#
```

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

- **HQ:**

```
HQ(config)# line vty 0 15
HQ(config-line)# password cisco
HQ(config-line)# login
HQ(config-line)#exit
HQ(config)#
```

- **BR1:**

```
BR1(config)# line vty 0 15
BR1(config-line)# password cisco
BR1(config-line)# login
BR1(config-line)#exit
BR1(config)#
```

- **BR2:**

```
BR2(config)# line vty 0 15
BR2(config-line)# password cisco
BR2(config-line)# login
BR2(config-line)# exit
BR2(config)#
```

f. Cifre las contraseñas de texto no cifrado.

- **HQ:**

```
HQ# config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)# service password-encryption
HQ(config)#
```

- **BR1:**

```
BR1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR1(config)# service password-encryption
BR1(config)#
```

- **BR2:**

```
BR2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR2(config)# service password-encryption
BR2(config)#
```

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

- **HQ:**

```
HQ# config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)# banner motd "El Acceso No Autorizado esta Prohibido!"
HQ(config)#
```

- **BR1:**

```
BR1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR1(config)# banner motd "El acceso no Autorizado Esta Prohibido!"
BR1(config)#
```

- **BR2:**

```
BR2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
BR2(config)# banner motd "El Acceso no Autorizado Esta Prohibido!"
BR2(config)#
```

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.

- **HQ:**

```
HQ(config-if)# exit
HQ(config)# interface g0/0
HQ(config-if)# Description LAN-A
HQ(config-if)# ip address 172.16.128.1 255.255.192.0
HQ(config-if)# no shutdown

HQ(config-if)#

HQ(config-if)#EXIT
HQ(config)# interface g0/1
HQ(config-if)# Description LAN-B
HQ(config-if)# ip address 172.16.192.1 255.255.224.0
HQ(config-if)# no shutdown

HQ(config-if)#

HQ(config-if)#exit
HQ(config)# interface serial0/0/0
HQ(config-if)# Description Connection to BR1
HQ(config-if)# Ip address 172.16.254.1 255.255.255.252
HQ(config-if)# no shutdown

HQ(config)# interface serial0/0/1
HQ(config-if)# Description Connection to BR2
HQ(config-if)# ip address 172.16.254.5 255.255.255.252
HQ(config-if)# no shutdown
```

- **BR1:**

```
BR1(config)# interface g0/0
BR1(config-if)# Description LAN-C
BR1(config-if)# ip address 172.16.240.1 255.255.248.0
BR1(config-if)# no shutdown

BR1(config-if)#

BR1(config)# interface g0/1
BR1(config-if)# Description LAN-D
BR1(config-if)# ip address 172.16.224.1 255.255.240.0
BR1(config-if)# no shutdown

BR1(config-if)#

BR1(config)# interface serial0/0/0
BR1(config-if)# Description Connection to HQ
BR1(config-if)# ip address 172.16.254.2 255.255.255.252
BR1(config-if)# no shutdown

BR1(config-if)#

BR1(config)# interface serial0/0/1
BR1(config-if)# Description Connection to BR2
BR1(config-if)# ip address 172.16.254.9 255.255.255.252
BR1(config-if)# no shutdown
```

- **BR2:**

```
BR2(config)# interface g0/0
BR2(config-if)# Description LAN-E
BR2(config-if)# ip address  172.16.252.1 255.255.254.0
BR2(config-if)# no shutdown

BR2(config-if)#

BR2(config)# interface g0/1
BR2(config-if)# Description LAN-F
BR2(config-if)# ip address 172.16.248.1 255.255.252.0
BR2(config-if)# no shutdown

BR2(config-if)#

BR2(config)# interface serial 0/0/1
BR2(config-if)# Description Connection to HQ
BR2(config-if)# ip address 172.16.254.6 255.255.255.252
BR2(config-if)# no shutdown

BR2(config-if)#

BR2(config)# interface serial0/0/0
BR2(config-if)# Description Connection to BR1
BR2(config-if)# ip address 172.16.254.10 255.255.255.252
BR2(config-if)# no shutdown

BR2(config-if)#
```

b. Configure una descripción de interfaz para cada interfaz.

- **HQ:**

```
HQ(config-if)# exit
HQ(config)# interface g0/0
HQ(config-if)# Description LAN-A
```

```
HQ(config-if)#EXIT
HQ(config)# interface g0/1
HQ(config-if)# Description LAN-B
```

```
HQ(config-if)#exit
HQ(config)# interface serial0/0/0
HQ(config-if)# Description Connection to BR1

HQ(config)# interface serial0/0/1
HQ(config-if)# Description Connection to BR2
```

- **BR1:**

```
BR1(config)# interface g0/0
BR1(config-if)# Description LAN-C

BR1(config)# interface g0/1
BR1(config-if)# Description LAN-D

BR1(config)# interface serial0/0/0
BR1(config-if)# Description Connection to HQ

BR1(config)# interface serial0/0/1
BR1(config-if)# Description Connection to BR2
```

- **BR2:**

```
BR2(config)# interface g0/0
BR2(config-if)# Description LAN-E
```

```
BR2(config)# interface g0/1
BR2(config-if)# Description LAN-F
```

```
BR2(config)# interface serial 0/0/1
BR2(config-if)# Description Connection to HQ
```

```
BR2(config)# interface serial0/0/0
BR2(config-if)# Description Connection to BR1
```

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

HQ(config-if)# clock rate 128000

- **HQ:**

```
HQ(config)#interface serial0/0/0
HQ(config-if)# clock rate 128000
This command applies only to DCE interfaces
HQ(config-if)#exit
HQ(config)# interface serial0/0/1
HQ(config-if)# clock rate 128000
This command applies only to DCE interfaces
HQ(config-if)#
```

- **BR1:**

```
BR1(config)# interface serial0/0/0
BR1(config-if)# clock rate 128000
BR1(config-if)#exit
BR1(config)# interface serial0/0/1
BR1(config-if)# clock rate 128000
BR1(config-if)#
```

- **BR2:**

```
BR2(config)# interface serial0/0/0
BR2(config-if)# clock rate 128000
This command applies only to DCE interfaces
BR2(config-if)# exit
BR2(config)# interface serial0/0/1
BR2(config-if)# clock rate 128000
BR2(config-if)#exit
```

d. Active las interfaces.

- **HQ:**

```
HQ(config)# interface serial0/0/0
HQ(config-if)# no shutdown
HQ(config-if)#exit
HQ(config)# interface serial0/0/1
HQ(config-if)# no shutdown
HQ(config-if)#exit
```

```
HQ(config)# interface g0/0
HQ(config-if)# no shutdown
HQ(config-if)# exit
HQ(config)# interface g0/1
HQ(config-if)# no shutdown
HQ(config-if)#exit
HQ(config)#
```

- **BR1:**

```
BR1(config)# interface g0/0
BR1(config-if)# no shutdown
BR1(config-if)#exit
BR1(config)# interface g0/1
BR1(config-if)# no shutdown
BR1(config-if)# exit
```

```
BR1(config)# interface serial0/0/0
BR1(config-if)# no shutdown
BR1(config-if)# exit
BR1(config)# interface serial0/0/1
BR1(config-if)# no shutdown
BR1(config-if)# exit
```

- **BR2:**

```
BR2(config)# interface g0/0
BR2(config-if)# no shutdown
BR2(config-if)# exit
BR2(config)# interface g0/1
BR2(config-if)# no shutdown
BR2(config-if)# exit
```

```
BR2(config)# interface serial0/0/0
BR2(config-if)# no shutdown
BR2(config-if)#exit
BR2(config)# interface serial0/0/1
BR2(config-if)# no shutdown
BR2(config-if)# exit
```

Paso 4: Guardar la configuración en todos los dispositivos.

- **HQ:**

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

- **BR1:**

```
BR1# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

- **BR2:**

```
BR2# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Paso 5: Probar la conectividad.

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

```
HQ# ping 172.16.254.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms

HQ#
```

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

```
HQ# ping 172.16.254.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/32 ms

HQ#
```

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

```
BR1# ping 172.16.254.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms

BR1#
```

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.

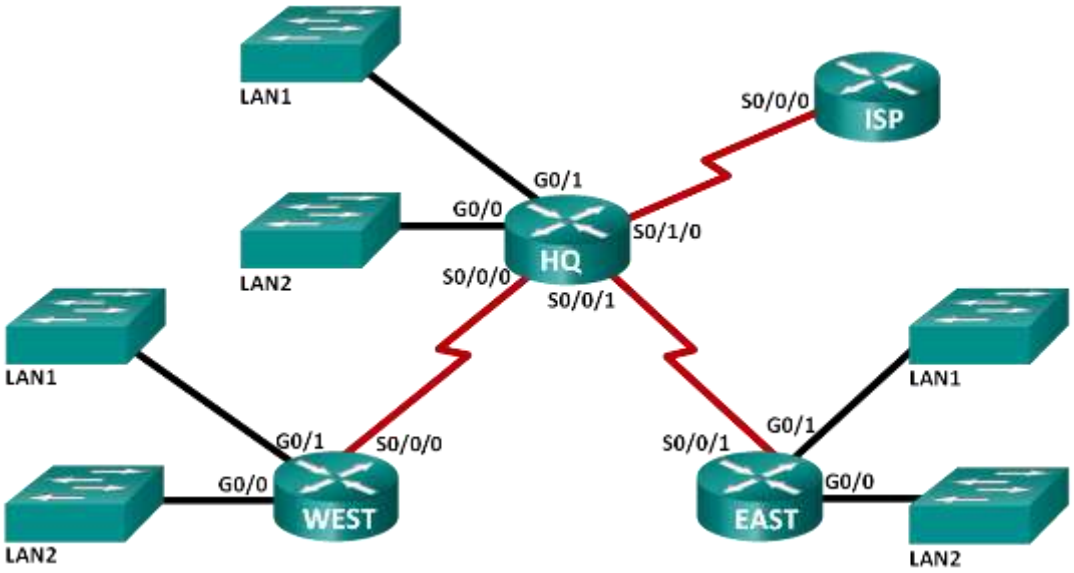
Reflexión

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

Rta: Tiene cuatro espacios para direcciones (La dirección de red, 2 direcciones de host y una dirección de broadcast). Se pueden calcular de la siguiente manera: tomando la dirección de red de la dirección previa y agregarle cuatro al último octeto.

Laboratorio: 6.4.2.5. Cálculo de Rutas Resumidas IPv4 e IPv6.

Topología de la guía:



Topología del laboratorio:

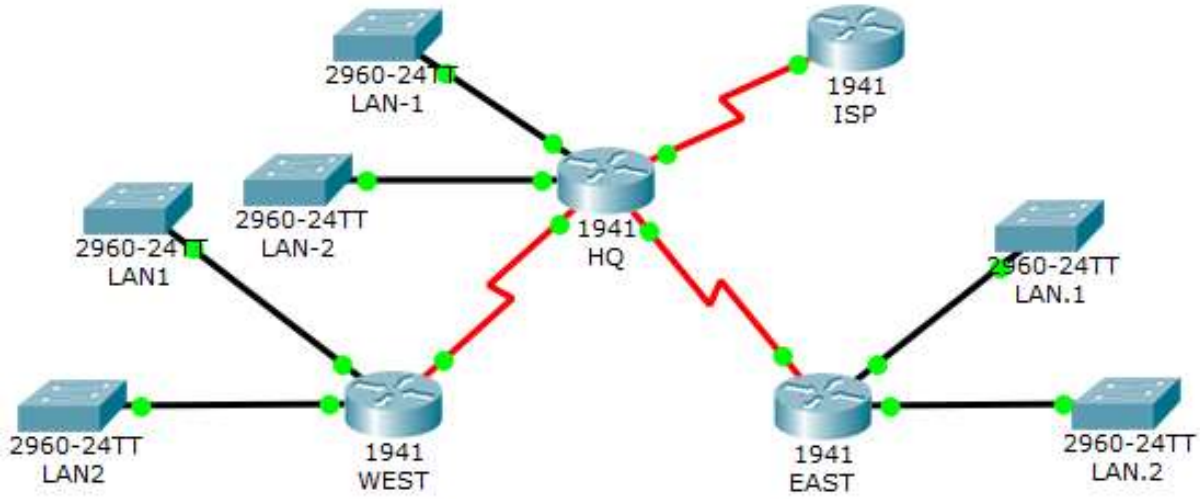


Tabla de direccionamiento:

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.

Subred:	Dirección IP y mascara de subred:
LAN1 de HQ	192.168.64.0/23
LAN2 de HQ	192.168.66.0/23

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

Subred:	Dirección IP en binario:
LAN1 de HQ	11000000.10101000.01000000.00000000
LAN2 de HQ	11000000.10101000.01000010.00000000

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.

Subred:	Dirección IP:	Mascara de subred:
LAN1 de HQ	11000000.10101000.0100000**0**0.00000000	/22
LAN2 de HQ	11000000.10101000.0100001**0**.00000000	

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

Rta: En las dos redes coinciden 22 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de HQ.	11000000.10101000.01000000.00000000	/22

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

Subred:	Dirección IP de la subred en formato binario:
LAN1 de HQ.	11000000.10101000.01000000.00000000
LAN2 de HQ.	11000000.10101000.01000010.00000000
Dirección de resumen de las LAN de HQ.	11000000.10101000.01000000.00000000

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

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de HQ	11000000.10101000.010000

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

Subred:	Dirección de la red HQ resumida:
LAN1 y LAN2 de HQ	11000000.10101000.01000000.00000000

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	/23	11000000.10101000.01000000.00000000
LAN2 de HQ	192.168.66.0	/23	11000000.10101000.01000010.00000000
Dirección de resumen de las LAN de HQ	192.168.64.0	/22	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.

Subred:	Dirección IPv4 y mascara de red:
LAN1 de EAST	192.168.68.0/24
LAN2 de EAST	192.168.69.0/24

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

Subred:	Dirección IP en binario:
LAN1 de EAST	11000000.10101000.01000100.00000000
LAN2 de EAST	11000000.10101000.01000101.00000000

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.

Subred:	Dirección IP en binario:	Mascara de subred:
LAN1 de EAST	11000000.10101000.0100010**0**.00000000	/23
LAN2 de EAST	11000000.10101000.0100010**1**.00000000	

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

Rta: En las dos redes coinciden 23 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de EAST.	11000000.10101000.01000100.00000000	/23

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.

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de EAST	11000000.10101000.0100010

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

Subred:	Dirección de la red ESTE resumida:
LAN1 y LAN2 de EAST	11000000.10101000.0100010**0**.00000000

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	/24	11000000.10101000.01000100.00000000
LAN2 de EAST	192.168.69.0	/24	11000000.10101000.01000101.00000000
Dirección de resumen de las LAN ESTE	192.168.68.0	/23	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.

Subred:	Dirección IPv4 y mascara de red:
LAN1 de OESTE	192.168.70.0/25
LAN2 de OESTE	192.168.70.128/25

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

Subred:	Dirección IP en binario:
LAN1 de OESTE	11000000.10101000.01000110.00000000
LAN2 de OESTE	11000000.10101000.01000110.10000000

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.

Subred:	Dirección IP en binario:	Mascara de subred:
LAN1 de OESTE	11000000.10101000.01000110.00000000	/24

LAN2 de OESTE	11000000.10101000.01000110.10000000	

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

Rta: En las dos redes coinciden 24 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de OESTE.	11000000.10101000.01000110.00000000	/24

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.

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de OESTE	11000000.10101000.01000110

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

Subred:	Dirección de la red OESTE resumida:
LAN1 y LAN2 de OESTE	11000000.10101000.01000110.00000000

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	/25	11000000.10101000.01000110.00000000
LAN2 de WEST	192.168.70.128	/25	11000000.10101000.01000110.10000000
Dirección de resumen de las LAN OESTE	192.168.70.0	/24	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.

Subred:	Dirección IP y mascara de red:
HQ	192.168.64.0/22
ESTE	192.168.68.0/23
OESTE	192.168.70.0/24

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

Subred:	Dirección IP en binario:
HQ	11000000.10101000.01000000.00000000
ESTE	11000000.10101000.01000100.00000000
OESTE	11000000.10101000.01000110.10000000

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.

Subred:	Dirección IP en binario:	Mascara de subred:
HQ	11000000.10101000.01000000.00000000	
ESTE	11000000.10101000.01000100.00000000	
OESTE	11000000.10101000.01000110.10000000	/21

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

Rta: En las tres redes coinciden 21 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de HQ, ESTE Y OESTE.	11000000.10101000.01000000.00000000	/21

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.

Subred:	Bit binaries coincidentes de las redes:
HQ, ESTE Y OESTE.	11000000.10101000.01000

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

Subred:	Dirección de las subredes resumida:
HQ, ESTE Y OESTE.	11000000.10101000.01000000.00000000

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	/22	11000000.10101000.01000000.00000000
EAST	192.168.68.0	/23	11000000.10101000.01000100.00000000
WEST	192.168.70.0	/24	11000000.10101000.01000110.10000000
Ruta resumida de la dirección de red	192.168.64.0	/21	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:

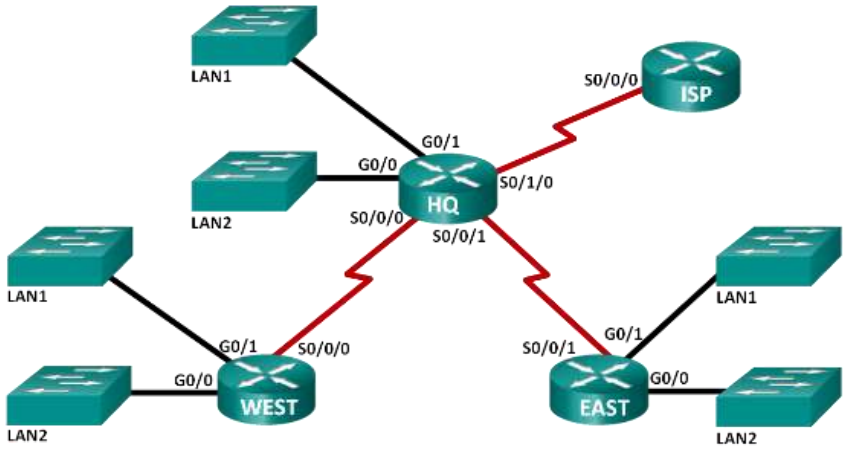


Tabla de direccionamiento:

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.

Subred:	Dirección IPv6 y mascara de subred:
LAN1 de HQ	2001:DB8:ACAD:E::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64

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

Subred:	Dirección ID en binario:
LAN1 de HQ	00000000.00001110
LAN2 de HQ	00000000.00001111

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.

Subred:	Dirección ID:	Mascara de subred:
LAN1 de HQ	00000000.00001110	/63
LAN2 de HQ	00000000.00001111	

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

Rta: Coinciden 63 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de HQ.	2001:DB8:ACAD:E::	/63

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.

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de HQ	0000000000000111

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

Subred:	Dirección de la red HQ resumida:
LAN1 y LAN2 de HQ	0000000000001110

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	2001 DB8 ACAD	00000000.00001110
LAN2 de HQ	2001:DB8:ACAD:F::/64	2001 DB8 ACAD	00000000.00001111
Dirección de resumen de las LAN de HQ	2001:DB8:ACAD:E::/63	2001 DB8 ACAD	00000000.00001110

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.

Subred:	Dirección IPv6 y mascara de red:
LAN1 de EAST	2001:DB8:ACAD:1::/64
LAN2 de EAST	2001:DB8:ACAD:2::/64

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

Subred:	Dirección ID en binario:
LAN1 de EAST	00000000.00000001
LAN2 de EAST	00000000.00000010

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.

Subred:	Dirección ID en binario:	Mascara de subred:
LAN1 de EAST	00000000.00000001	/62
LAN2 de EAST	00000000.00000010	

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

RTA: Coinciden 62 bits.

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

Subred resumida:	Dirección IP resumida:	Mascara de subred:
Resumen de las LAN de EAST.	2001:DB8:ACAD:0::	/62

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.

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de EAST	00000000.000000

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

Subred:	Dirección de la red ESTE resumida:
LAN1 y LAN2 de EAST	00000000.00000000

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	2001 DB8 ACAD	00000000.00000001
LAN2 de EAST	2001:DB8:ACAD:2::/64	2001 DB8 ACAD	00000000.00000010
Dirección de resumen de las LAN ESTE	2001:DB8:ACAD:0::/62	2001 DB8 ACAD	00000000.00000000

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.

Subred:	Dirección IPv6 y mascara de red:
LAN1 de OESTE	2001:DB8:ACAD:9::/64
LAN2 de OESTE	2001:DB8:ACAD:A::/64

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

Subred:	**Dirección ID en binario:**
LAN1 de OESTE	00000000.00001001
LAN2 de OESTE	00000000.00001010

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.

Subred:	**Dirección ID en binario:**	**Mascara de subred:**
LAN1 de OESTE	00000000.00001001	/60
LAN2 de OESTE	00000000.00001010	

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

Rta:

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

Subred resumida:	**Dirección IP resumida:**	**Mascara de subred:**
Resumen de las LAN de OESTE.	2001:DB8:ACAD:8::	/62

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.

Subred:	Bit binaries coincidentes de las redes:
LAN1 y LAN2 de OESTE	00000000.000010

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

Subred:	Dirección de la red ESTE resumida:
LAN1 y LAN2 de OESTE	00000000.00001000

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	2001 DB8 ACAD	00000000.00001001
LAN2 de WEST	2001:DB8:ACAD:A::/64	2001 DB8 ACAD	00000000.00001010
Dirección de resumen de las LAN OESTE	2001:DB8:ACAD:8::/62	2001 DB8 ACAD	00000000.00001000

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.

Subred:	Dirección IP de los primeros 64 bits y mascara de red:
HQ	2001:DB8:ACAD:E::/63
ESTE	2001:DB8:ACAD:0::/62
OESTE	2001:DB8:ACAD:8::/62

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

Subred:	Dirección ID en binario:
HQ	00000000.00001110
ESTE	00000000.00000000
OESTE	00000000.00001000

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.

Subred:	Dirección IP en binario:	Mascara de subred:
HQ	00000000.00001110	/60
ESTE	00000000.00000000	
OESTE	00000000.00001000	

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

Rta: Se encontraron 60 bits coincidentes en la tres subredes sumatorias.

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

Subred resumida:	Dirección ID resumida:	Mascara de subred:
Resumen de las LAN de HQ, ESTE Y OESTE.	00000000.00000000	/60

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.

Subred:	Bit binaries coincidentes de las ID de las subredes:
HQ, ESTE Y OESTE.	00000000.0000

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

Subred:	Dirección ID de la redes resumida:
HQ, ESTE Y OESTE.	00000000.00000000

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	2001 DB8 ACAD	00000000.00001110
EAST	2001:DB8:ACAD:0::/62	2001 DB8 ACAD	00000000.00000000
WEST	2001:DB8:ACAD:8::/62	2001 DB8 ACAD	00000000.00001000
Ruta resumida de la dirección de red:	2001:DB8:ACAD:0::/60	2001 DB8 ACAD	00000000.00000000

Reflexión

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

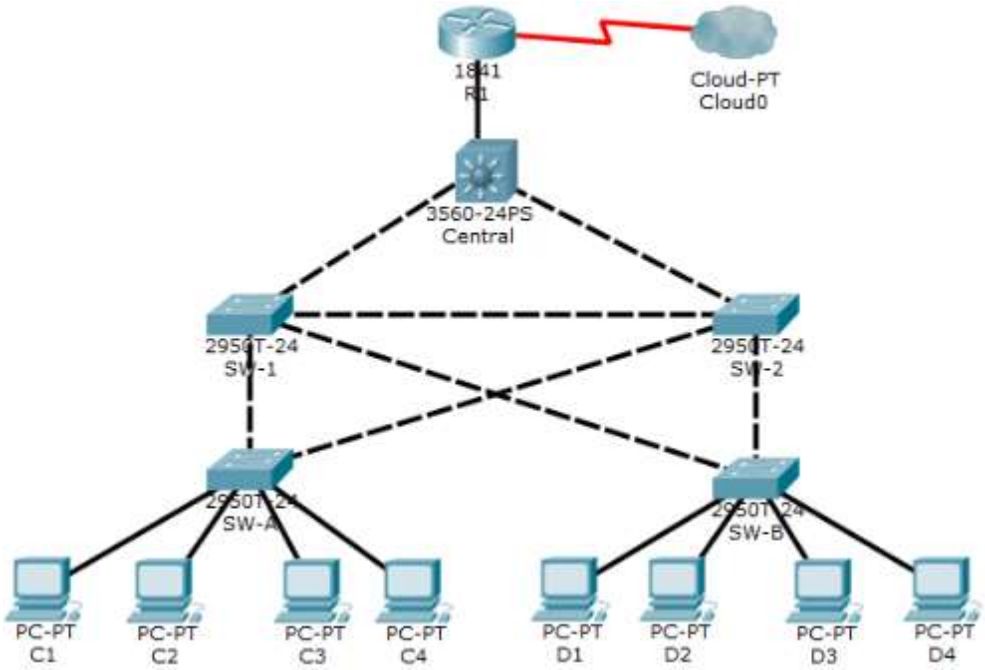
Rta: Entre las diferencias se encuentran: en ipv4 se encuentran 32 bits, mientras que en ipv6 hay 128 bits; en ipv4 hay que convertir de decimal a binarios y en ipv6 hay que convertir de hexadecimal a binario.

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

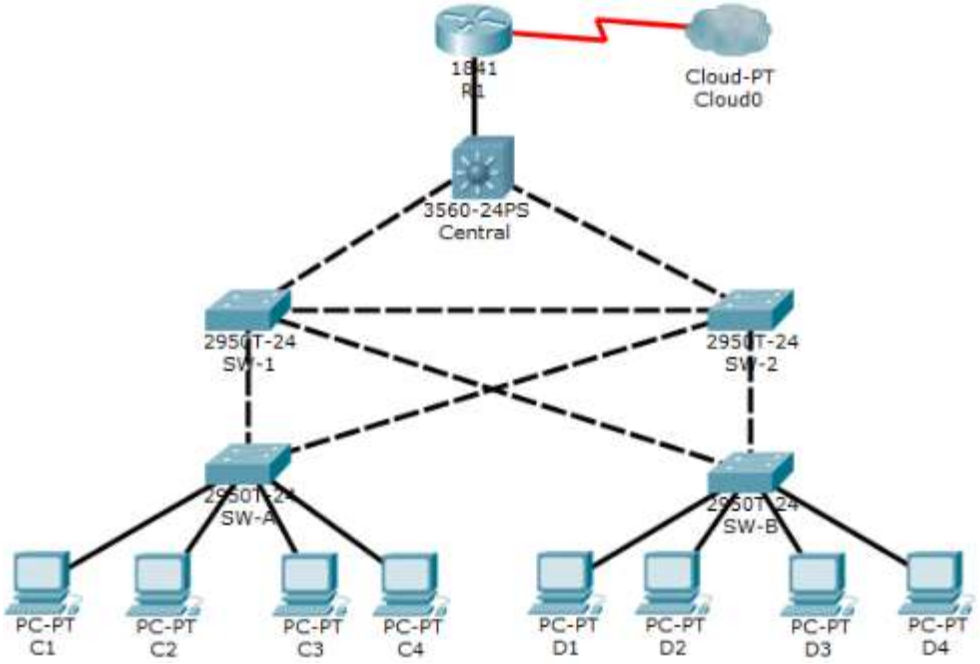
Rta: Porque pueden llevar el proceso con eficiencia, además que requiere menos memoria en el router.

Laboratorio: 6.5.1.2. Layer 2 Security.

Topología de la guía:



Topología del laboratorio:



Packet Tracer: Layer 2 Security.

Objectives:

Assign the Central switch as the root bridge.

Secure spanning-tree parameters to prevent STP manipulation attacks.

Enable storm control to prevent broadcast storms.

Enable port security to prevent MAC address table overflow attacks.

Background / Scenario:

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent against spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. In addition, the network administrator would like to enable storm control to prevent broadcast storms. Finally, to prevent against MAC address table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses that can be learned per switch port. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

All switch devices have been preconfigured with the following:

* Enable password: **ciscoenpa55**

* Console password: **ciscoconpa55**

```
!
line con 0
 password ciscoconpa55
!
```

* VTY line Password: **ciscovtypa55**

```
line vty 0 4
 password ciscovtypa55
 login
```

Part 1: Configure Root Bridge.

Step 1: Determine the current root bridge.

From Central, issue the show spanning-tree command to determine the current root bridge and to see the ports in use and their status. (Desde el centro, ejecute el comando show spanning-tree para determinar el puente raíz actual y para ver los puertos en uso y su estado).

```
Central>enable
Password:
Central# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C61.9058
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p
Fa0/1            Desg FWD 19        128.1    P2p

Central#
```

Which switch is the current root bridge?(¿Los botones de que es el puente raíz actual?)

RTA: Current root is SW-1. (La raíz actual está SW-1)

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.) Con base en el puente raíz actual, **¿cuál es el árbol de expansión resultante?** (Dibujar la topología de árbol de expansión).

Step 2: Assign Central as the primary root bridge.

Using the spanning-tree vlan 1 root primary command, assign Central as the root bridge.

Central (config) # spanning-tree vlan 1 root primary

```
Central# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)# spanning-tree vlan 1 root primary
Central(config)#
```

Step 3: Assign SW-1 as a secondary root bridge.

Assign SW-1 as the secondary root bridge using the spanning-tree vlan 1 root secondary command.

SW-1(config)# spanning-tree vlan 1 root secondary

```
SW-1> enable
Password:
SW-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)# spanning-tree vlan 1 root secondary
SW-1(config)#
```

Step 4: Verify the spanning-tree configuration.

Issue the show spanning-tree command to verify that Centralis the root bridge.

```
Central# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Desg FWD 4         128.25   P2p
Fa0/1            Desg FWD 19        128.1    P2p

Central#
```

Which switch is the current root bridge?

Rta: Current root is Central.

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Part 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the SW-A and SW-B, use the spanning-tree portfast command. (Fast puerto está configurado en los puertos de acceso que se conectan a una sola estación de trabajo o servidor para que puedan activarse con mayor rapidez. En los puertos de acceso conectados del SW-A y SW-B, utilice el comando spanning-tree portfast).

SW-A(config)# interface range FastEthernet 0/1 - 4
SW-A(config-if-range)# spanning-tree portfast

```
SW-A# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)# interface range f0/1-4
SW-A(config-if-range)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
```

```
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 4 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
SW-A(config-if-range)#
```

SW-B(config)# interface range FastEthernet 0/1 - 4
SW-B(config-if-range)# spanning-tree portfast

```
SW-B> enable
Password:
SW-B#  config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)# interface range f0/1-4
SW-B(config-if-range)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 4 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
SW-B(config-if-range)#
```

Step 2: Enable BPDU guard on all access ports. (Habilitar guardia BPDU en todos los puertos de acceso).

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on SW-A and SW-B access ports. (BPDU Guard es una característica que puede ayudar a prevenir los interruptores sin escrúpulos y la suplantación de identidad en los puertos de acceso. Habilitar guardia BPDU en los puertos de acceso SW-A y B-).

SW-A(config)# interface range FastEthernet 0/1 - 4
SW-A(config-if-range)# spanning-tree bpduguard enable

```
SW-A# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)# interface range f0/1-4
SW-A(config-if-range)# spanning-tree bpduguard enable
SW-A(config-if-range)#
```

SW-B(config)# interface range FastEthernet 0/1 - 4
SW-B(config-if-range)# spanning-tree bpduguard enable

```
SW-B# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)# interface range f0/1-4
SW-B(config-if-range)# spanning-tree bpduguard enable
SW-B(config-if-range)#
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the spanning-tree bpduguard enablecommand in the interface configuration mode or

the spanning-tree portfast bpduguard default command in the global configuration mode. For grading purposes in this activity, please use the spanning-tree bpduguard enable command. (Spanning-tree BPDU guardia se puede habilitar en cada puerto, mediante el bpduguard del árbol de expansión enablecommand en el modo de configuración de interfaz o el comando predeterminado portfast bpduguard del árbol de expansión en el modo de configuración global. Para los propósitos de clasificación en esta actividad, por favor utilice el árbol de expansión bpduguard comando enable).

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the show spanning-tree command to determine the location of the root port on each switch. (Protección de raíz se puede habilitar en todos los puertos en un switch que no son puertos de raíz. Lo mejor es desplegado en los puertos que se conectan a otros conmutadores no root. Utilice el comando show spanning-tree para determinar la ubicación del puerto raíz en cada interruptor).

On SW-1, enable root guard on ports Fa0/23 and Fa0/24. OnSW-2, enable root guard on ports Fa0/23 and Fa0/24. (En SW-1, habilite protección de raíz en los puertos Fa0 / 23 y Fa0 / 24. OnSW-2, habilite protección de raíz en los puertos Fa0 / 23 y Fa0 / 24).

SW-1(config)# interface range fa0/23 - 24
SW-1(config-if-range)# spanning-tree guard root

```
SW-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)# interface range f0/23-24
SW-1(config-if-range)# spanning-tree guard root
SW-1(config-if-range)#
```

SW-2(config)# interface range fa0/23 - 24
SW-2(config-if-range)# spanning-tree guard root

```
SW-2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)# interface range f0/23-24
SW-2(config-if-range)# spanning-tree guard root
SW-2(config-if-range)#
```

Part 3: Enable Storm Control. (Habilitar el control de tormentas).

Step 1: Enable storm control for broadcasts. (Habilitar el control de tormentas para las emisiones).

a. Enable storm control for broadcasts on all ports connecting switches (trunk ports). (Habilitar el control de tormentas para las emisiones en todos los puertos de conexión (interruptores puertos troncales).

b. Enable storm control on interfaces connecting Central, SW-1, and SW-2. Set a 50 percent rising suppression level using the storm-control broadcast command. (Habilitar el control de tormentas en las interfaces de conexión central, SW-1, y SW-2. Establecimiento de un nivel de supresión de 50 por ciento ascendente utilizando el comando de emisión-control de tormentas).

SW-1(config)# interface range gi1/1 , fa0/1 , fa0/23 - 24
SW-1(config-if)# storm-control broadcast level 50

```
SW-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)# interface range g0/1, f0/1, f0/23-24
SW-1(config-if-range)# storm-control broadcast level 50
SW-1(config-if-range)#
```

SW-2(config)# interface range gi1/1 , fa0/1 , fa0/23 - 24
SW-2(config-if)# storm-control broadcast level 50

```
SW-2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)# interface range g0/1, f0/1, f0/23, f0/24
SW-2(config-if-range)# storm-control broadcast level 50
SW-2(config-if-range)#
```

Central(config-if)# interface range gi0/1 , gi0/2 , fa0/1
Central(config-if)# storm-control broadcast level 50

```
Central# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)# interface range g0/1, g0/2, f0/1
Central(config-if-range)# storm-control broadcast level 50
Central(config-if-range)#
```

Step 2: Verify storm control configuration. (Verificar la configuración de control de tormentas).

Verify your configuration with the show storm-control broadcast and the show run commands. (Verificar su configuración con la emisión del espectáculo control de tormentas y los comandos show ejecutar).

```
Central# show storm-control broadcast
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  --------
Fa0/1      Link Up         50.00%        50.00%         0.00%
Gig0/1     Link Up         50.00%        50.00%         0.00%
Gig0/2     Link Up         50.00%        50.00%         0.00%

Central#
```

```
Central# show run
Building configuration...

Current configuration : 1422 bytes
!
interface FastEthernet0/1
 storm-control broadcast level 50
!
```

```
interface GigabitEthernet0/1
 storm-control broadcast level 50
!
interface GigabitEthernet0/2
 storm-control broadcast level 50
```

Part 4: Configure Port Security and Disable Unused Ports

Step 1: Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on SW-Aand SW-B. Set the maximum number of learned MAC address to2, allow the MAC address to be learned dynamically, and set the violation to shutdown. (Este procedimiento debe realizarse en todos los puertos de acceso en SW-A y SW-B. Establecer el número máximo de direcciones MAC aprendidas to2, permita que la dirección MAC que se debe aprender de forma dinámica, y establecer la violación a la parada).

Note: A switch port must be configured as an access port to enable port security.

SW-A(config)# interface range fa0/1 - 22
SW-A(config-if-range)# switchport mode access
SW-A(config-if-range)# switchport port-security
SW-A(config-if-range)# switchport port-security maximum 2
SW-A(config-if-range)# switchport port-security violation shutdown
SW-A(config-if-range)# switchport port-security mac-address sticky

```
SW-A# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)# interface range f0/1-22
SW-A(config-if-range)# switchport mode access
SW-A(config-if-range)# switchport port-security
SW-A(config-if-range)# switchport port-security maximum 2
SW-A(config-if-range)# switchport port-security violation shutdown
SW-A(config-if-range)# switchport port-security mac-address sticky
SW-A(config-if-range)#
```

SW-B(config)# interface range fa0/1 - 22
SW-B(config-if-range)# switchport mode access
SW-B(config-if-range)# switchport port-security
SW-B(config-if-range)# switchport port-security maximum 2
SW-B(config-if-range)# switchport port-security violation shutdown
SW-B(config-if-range)# switchport port-security mac-address sticky

```
SW-B# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)# interface range f0/1-22
SW-B(config-if-range)# switchport mode access
SW-B(config-if-range)# switchport port-security
SW-B(config-if-range)# switchport port-security maximum 2
SW-B(config-if-range)# switchport port-security violation shutdown
SW-B(config-if-range)# switchport port-security mac-address sticky
SW-B(config-if-range)#
```

Why would you not want to enable port security on ports connected to other switches or routers?(*¿Por qué no quiere activar la seguridad portuaria en los puertos conectados a otros switches o routers?)*

RTA: Ports connected to other switch devices and routers can, and should, have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality. (Los puertos están conectados a otros dispositivos de conmutación y routers pueden, y deben, tener una multitud de direcciones MAC aprendidas para que solo puerto. Limitar el número de direcciones MAC que se pueden aprender en estos puertos puede afectar significativamente la funcionalidad de red).

Step 2: Verify port security. (Verificar la seguridad del puerto).

On SW-A, issue the show port-security interface fa0/1 command to verify that port security has been configured. (En SW-A, ejecute el comando show port-security interface Fa0/1 para verificar que la seguridad del puerto ha sido configurado).

```
SW-A# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW-A#
```

Step 3: Disable unused ports. (Deshabilitar los puertos no utilizados).

Disable all ports that are currently unused. (Desactivar todos los puertos que están actualmente sin uso).

SW-A(config)# interface range fa0/5 - 22

SW-A(config-if-range)# shutdown

```
SW-A# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)# interface range f0/5-22
SW-A(config-if-range)# shutdown

%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 FastEthernet0/19, 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
SW-A(config-if-range)#
```

SW-B(config)# interface range fa0/5 - 22
SW-B(config-if-range)# shutdown

```
SW-B# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)# interface range f0/5-22
SW-B(config-if-range)# shutdown

%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 FastEthernet0/19, 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
SW-B(config-if-range)#
```

Step 4: Check results.

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

Activity Results

Time Elapsed: 01:08:28

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

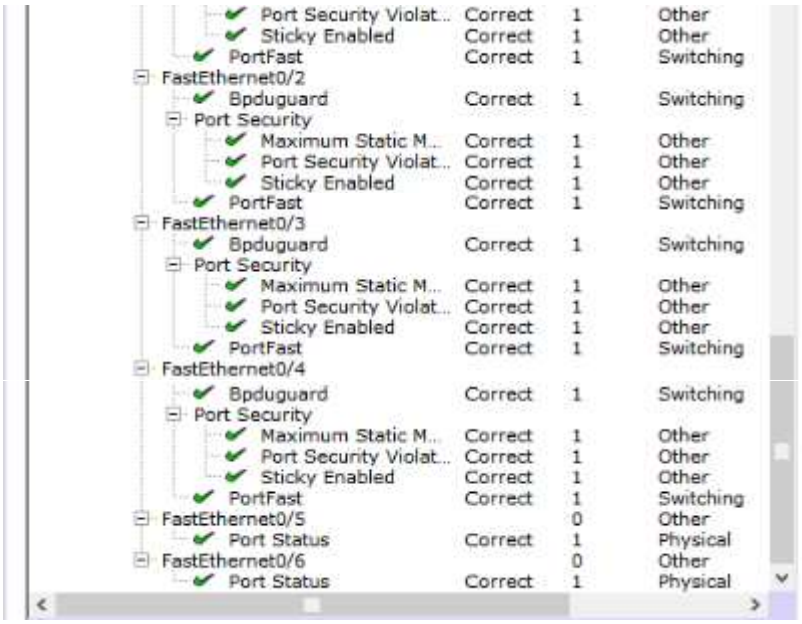
Expand/Collapse All

Assessment Items	Status	Points	Component
Network			
SW-1			
Ports			
FastEthernet0/1		0	Other
Storm Control	Correct	1	Switching
FastEthernet0/23			
Root Guard	Correct	1	Switching
Storm Control	Correct	1	Switching
FastEthernet0/24			
Root Guard	Correct	1	Switching
Storm Control	Correct	1	Switching
GigabitEthernet0/1		0	Other
Storm Control	Correct	1	Switching
SW-2			
Ports			
FastEthernet0/1		0	Other
Storm Control	Correct	1	Switching
FastEthernet0/23			
Root Guard	Correct	1	Switching
Storm Control	Correct	1	Switching
FastEthernet0/24			
Root Guard	Correct	1	Switching
Storm Control	Correct	1	Switching
GigabitEthernet0/1		0	Other
Storm Control	Correct	1	Switching
SW-A			
Ports			
FastEthernet0/1			
Bpduguard	Correct	1	Switching
Port Security			
Maximum Static M...	Correct	1	Other
Port Security Violat...	Correct	1	Other
Sticky Enabled	Correct	1	Other
FastEthernet0/2			
Bpduguard	Correct	1	Switching
Port Security			
Maximum Static M...	Correct	1	Other
Port Security Violat...	Correct	1	Other
Sticky Enabled	Correct	1	Other
PortFast	Correct	1	Switching
FastEthernet0/3			
Bpduguard	Correct	1	Switching
Port Security			
Maximum Static M...	Correct	1	Other
Port Security Violat...	Correct	1	Other
Sticky Enabled	Correct	1	Other
PortFast	Correct	1	Switching
FastEthernet0/4			
Bpduguard	Correct	1	Switching
Port Security			
Maximum Static M...	Correct	1	Other
Port Security Violat...	Correct	1	Other
Sticky Enabled	Correct	1	Other
PortFast	Correct	1	Switching
FastEthernet0/5		0	Other
Port Status	Correct	1	Physical
FastEthernet0/6		0	Other
Port Status	Correct	1	Physical
SW-B			
Ports			
FastEthernet0/1			
Bpduguard	Correct	1	Switching
Port Security			
Maximum Static M...	Correct	1	Other

Score : 55/55

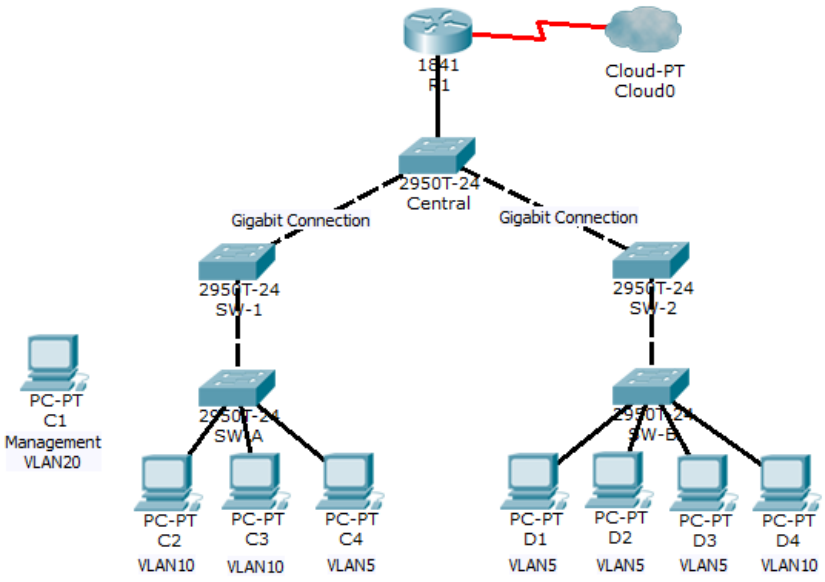
Item Count : 55/55

Component	Items/Total	Score
Other	24/24	24/24
Physical	4/4	4/4
Switching	27/27	27/27



6.5.1.3 Packet Tracer - Layer 2 VLAN Security

Topología



Objetives

✓ 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.

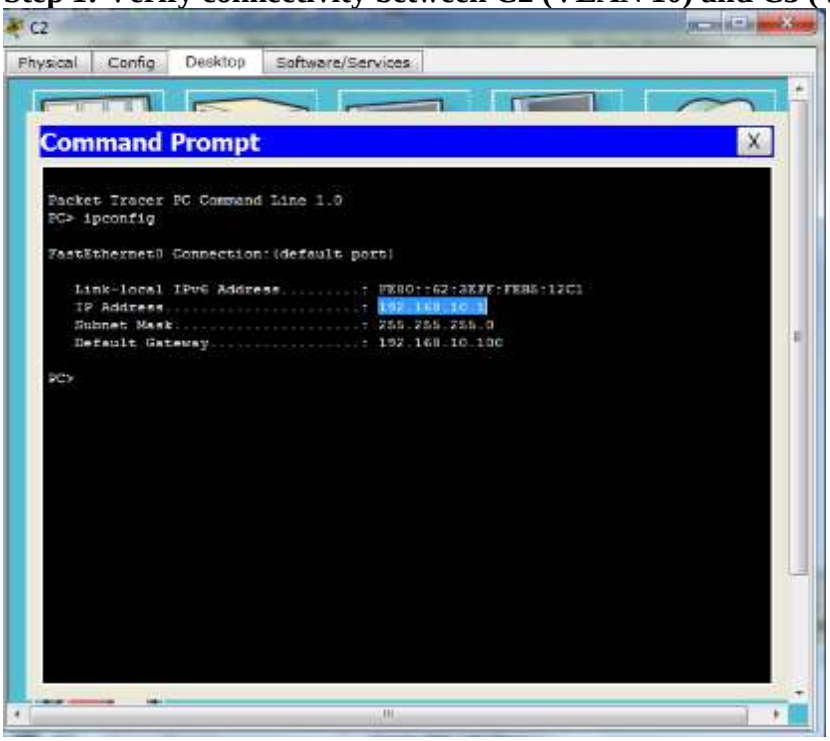
In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to allow the management PC to be able to connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

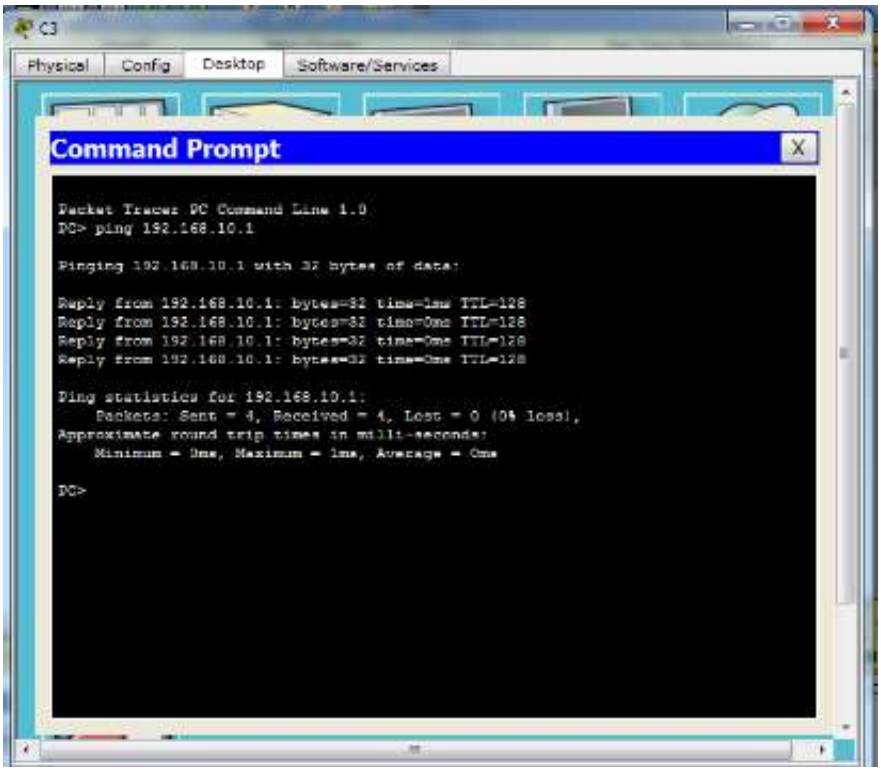
All devices have been preconfigured with:

- ✓ Enable secret password: ciscoenpa55
- ✓ Console password: ciscoconpa55
- ✓ VTY line password: **ciscovtypa55**

Part 1: Verify Connectivity

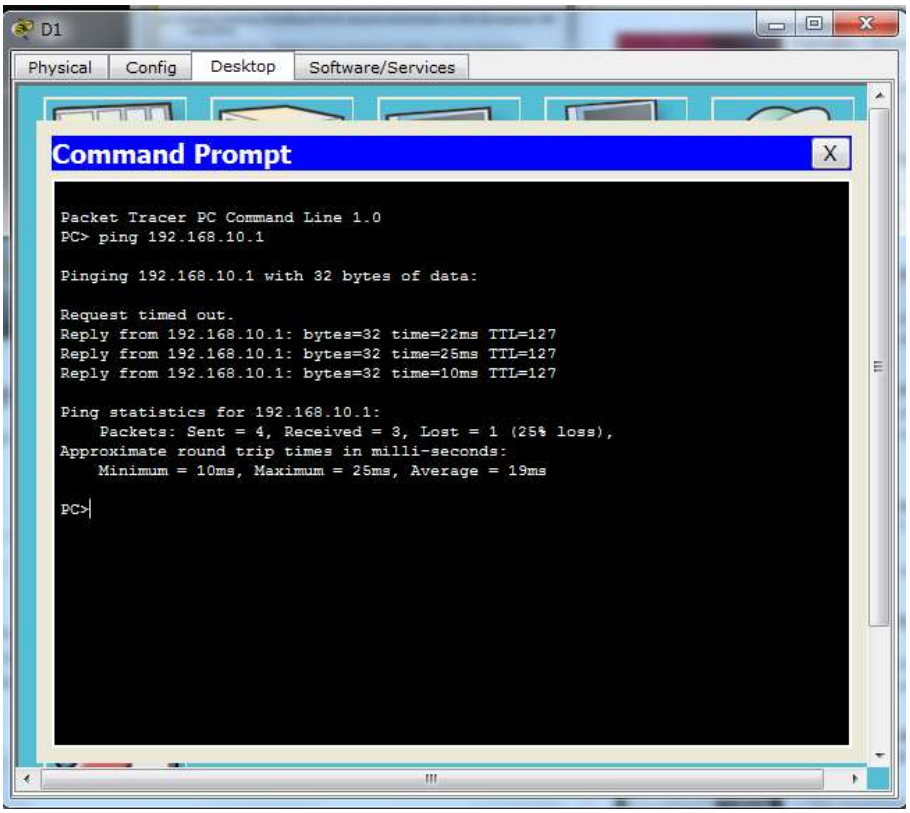
Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).





Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

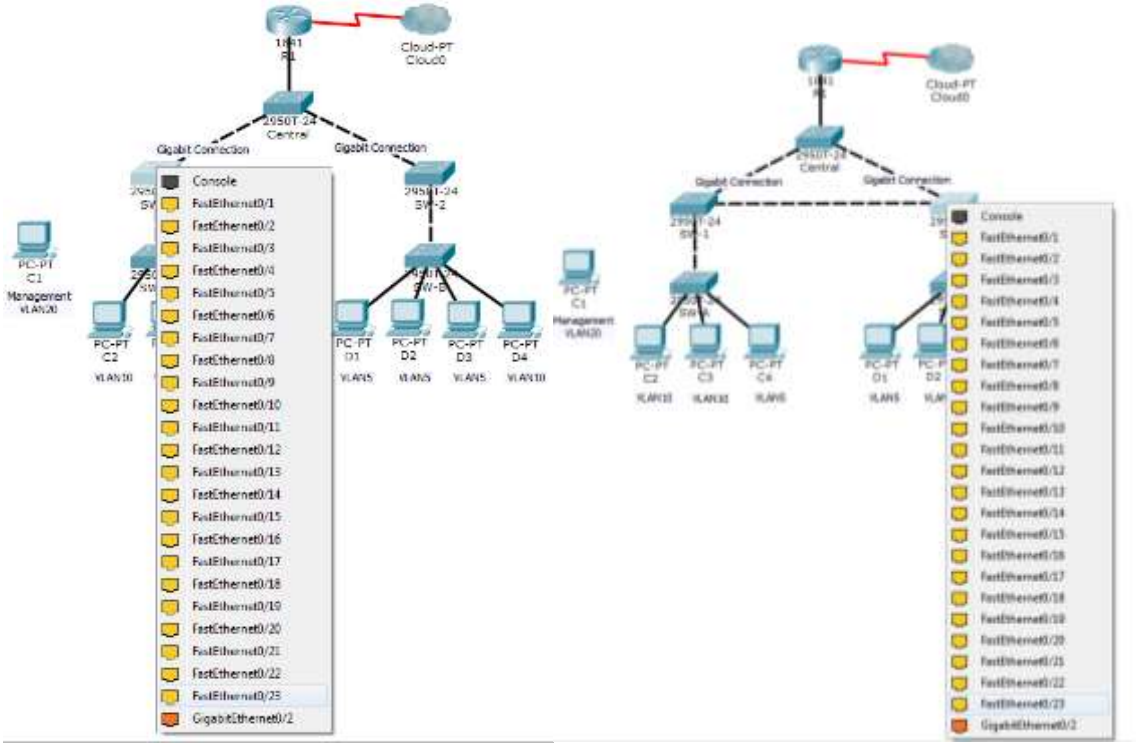
Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.



Part 2: Create a Redundant Link between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

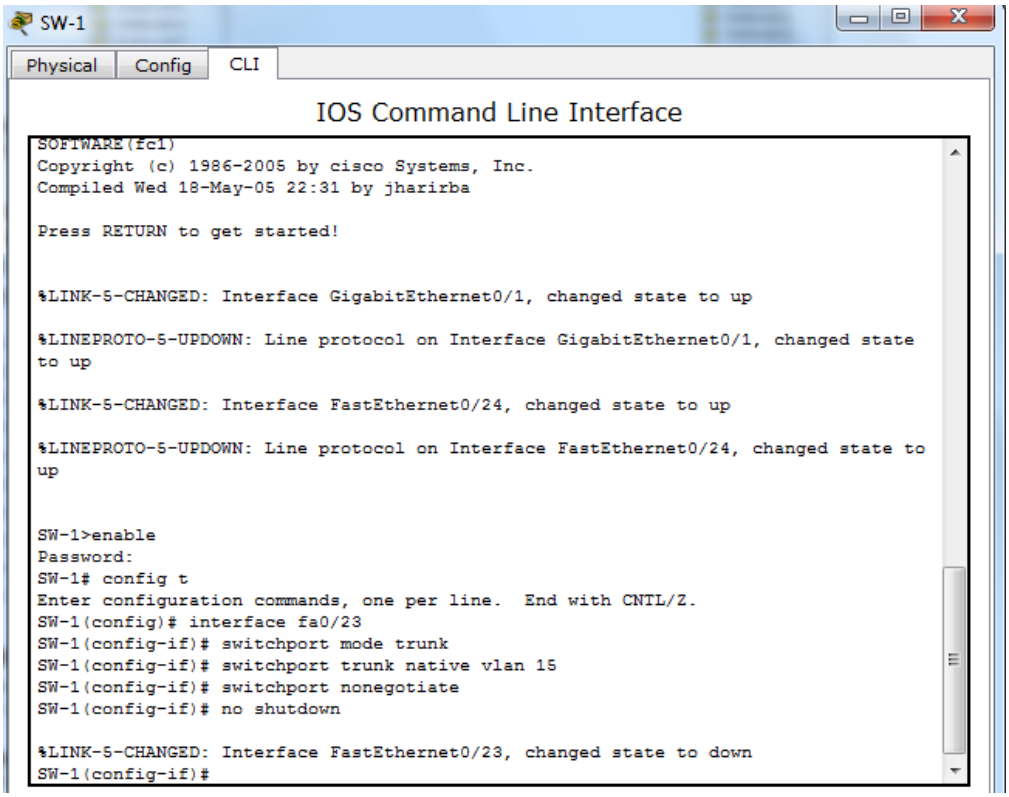
Using a crossover cable, connect port Fa0/23 on **SW-1** to port Fa0/23 on **SW-2**.



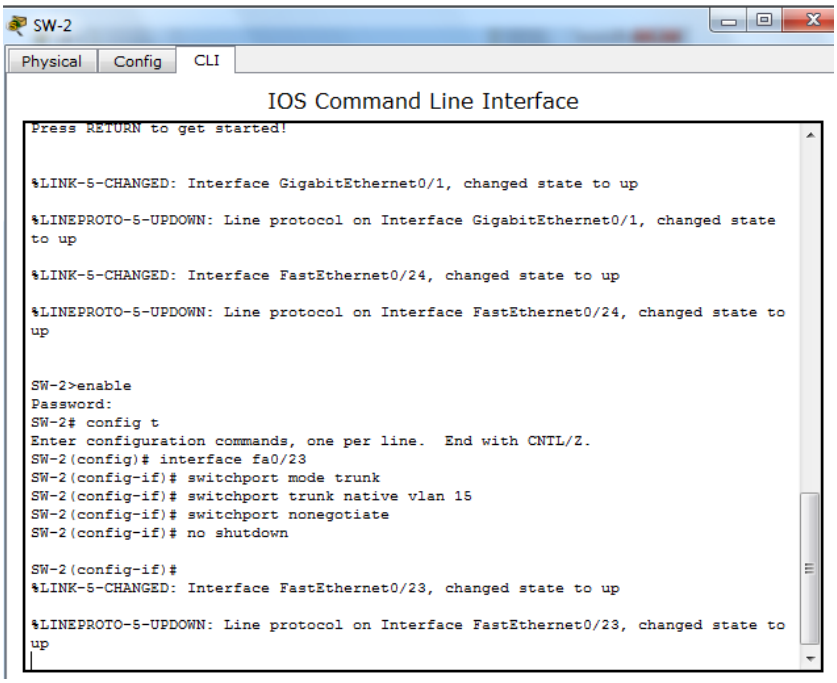
Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

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 nonegotiate**
SW-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.

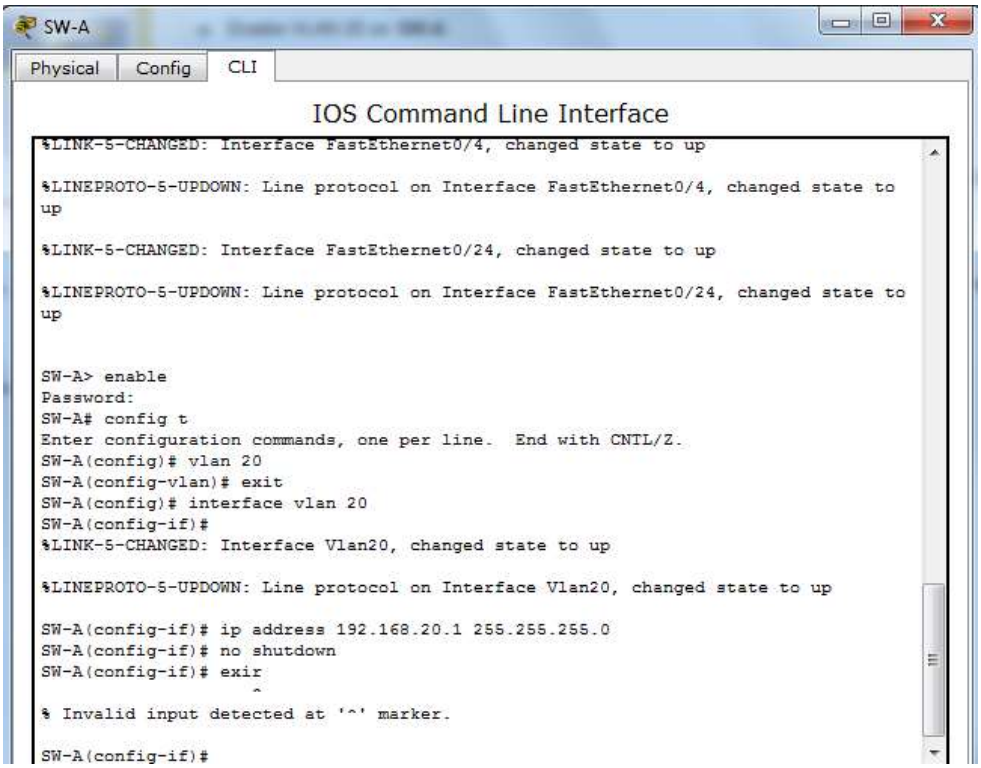
Step 1: Enable a management VLAN (VLAN 20) on SW-A.

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

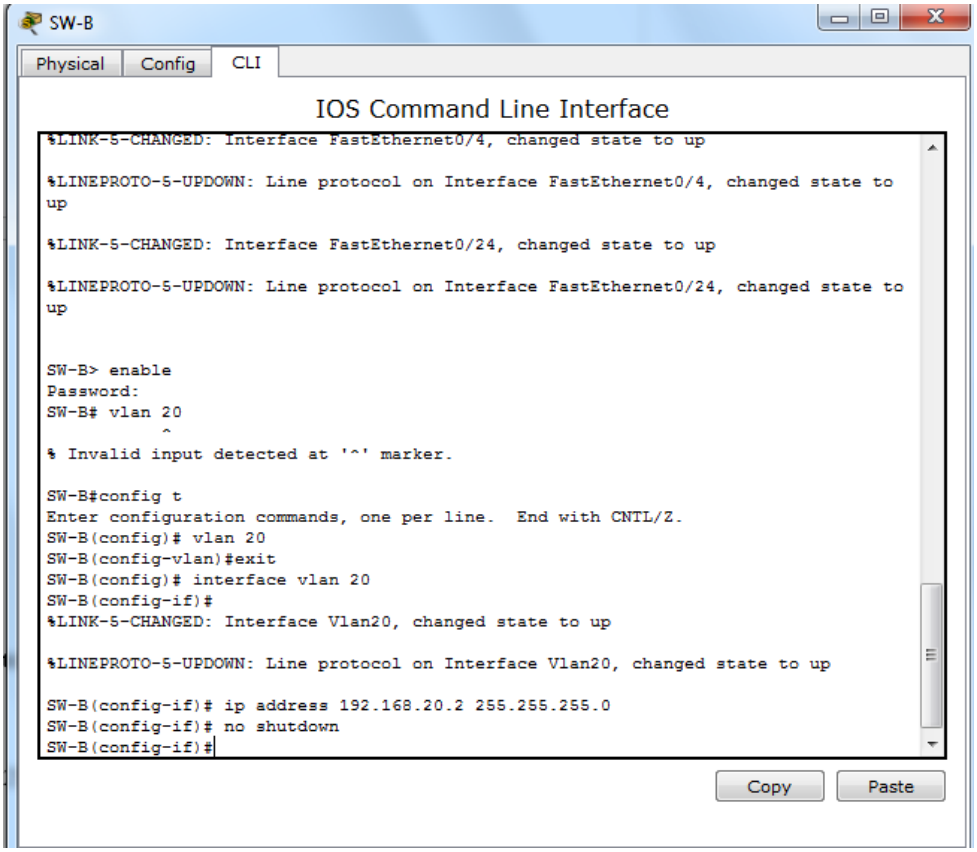
SW-1(config)# vlan 20
SW-1(config-vlan)# exit

SW-2(config)# vlan 20
SW-2(config-vlan)# exit

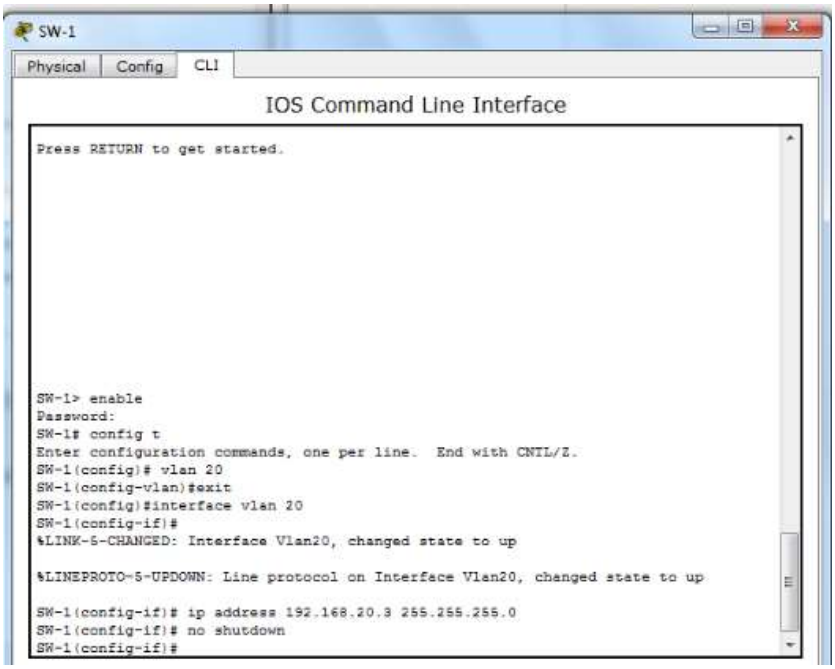
Central(config)# vlan 20
Central(config-vlan)# exit

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

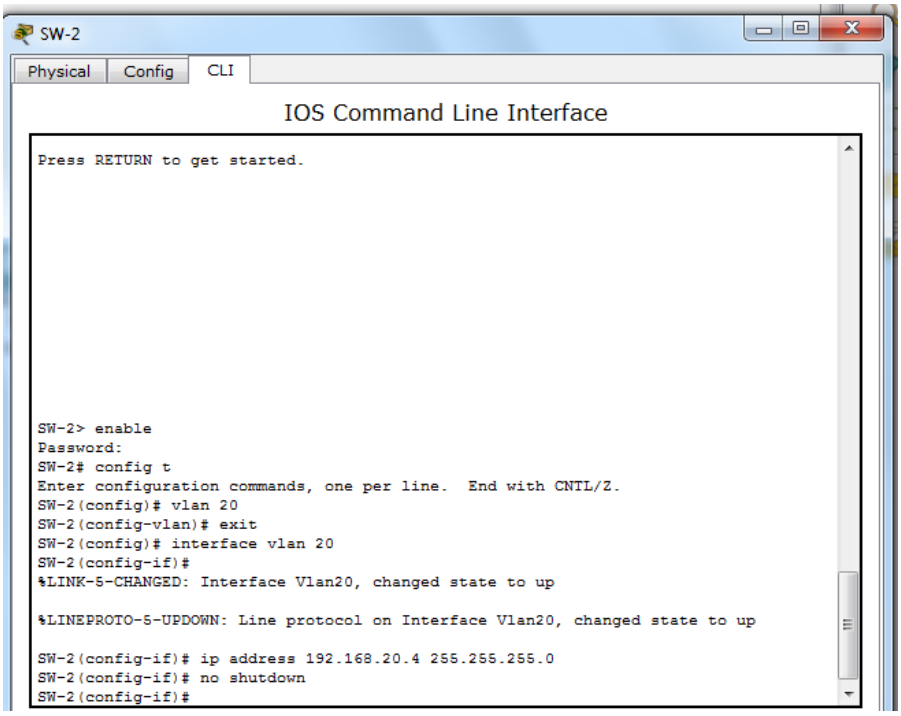
SW-B(config)# interface vlan 20
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0



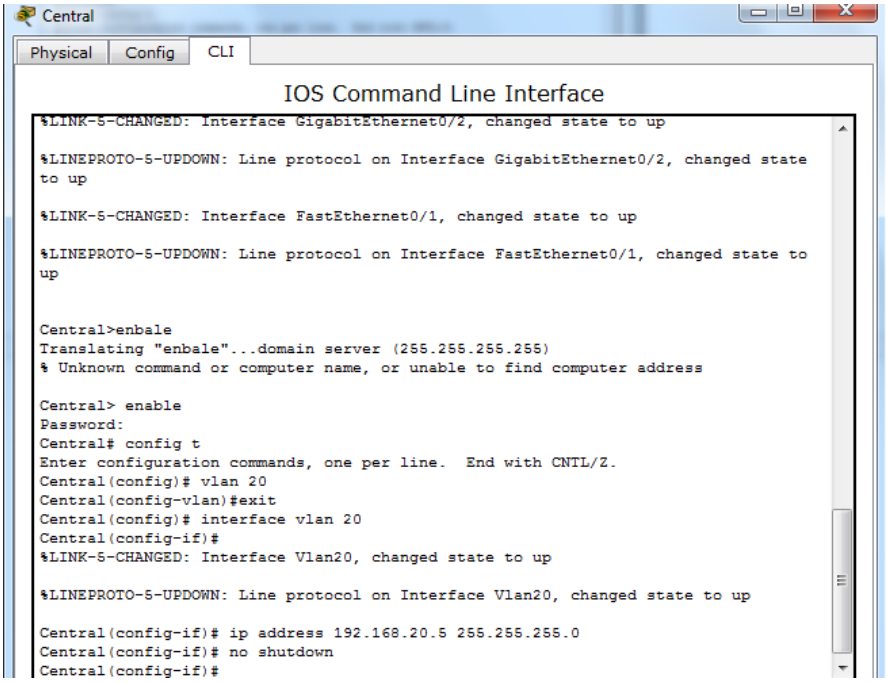
SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0



SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

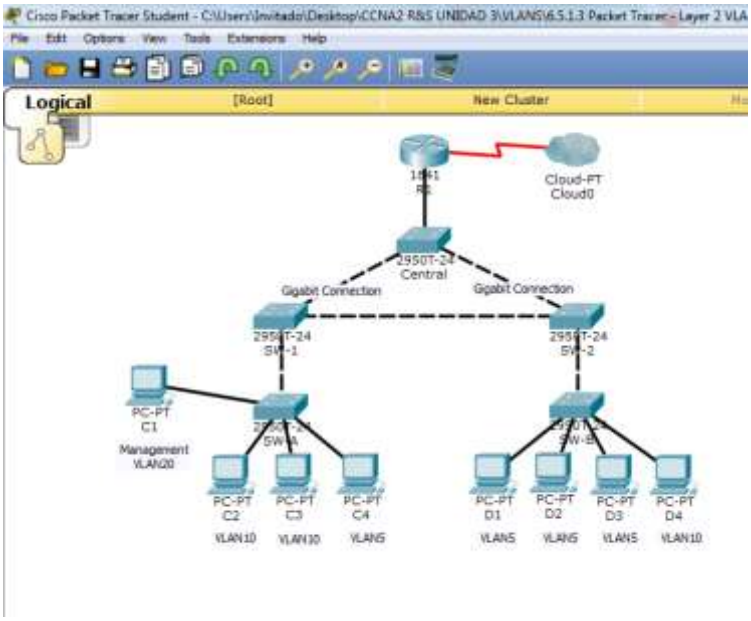


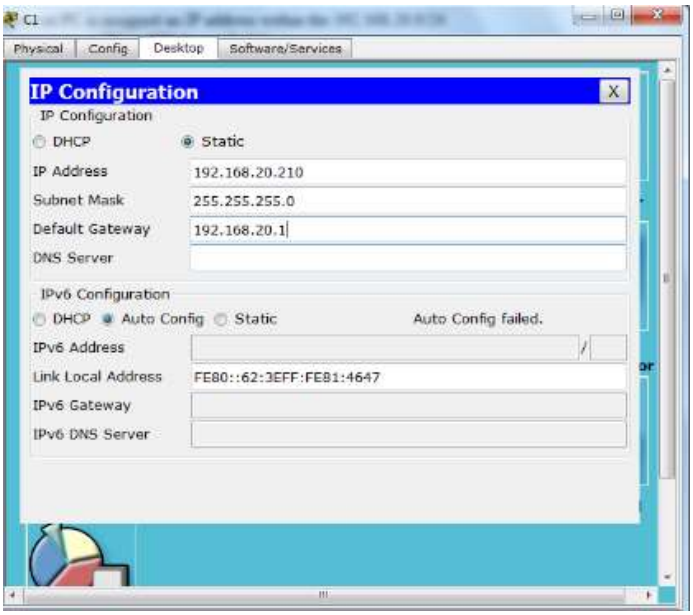
Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0



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.

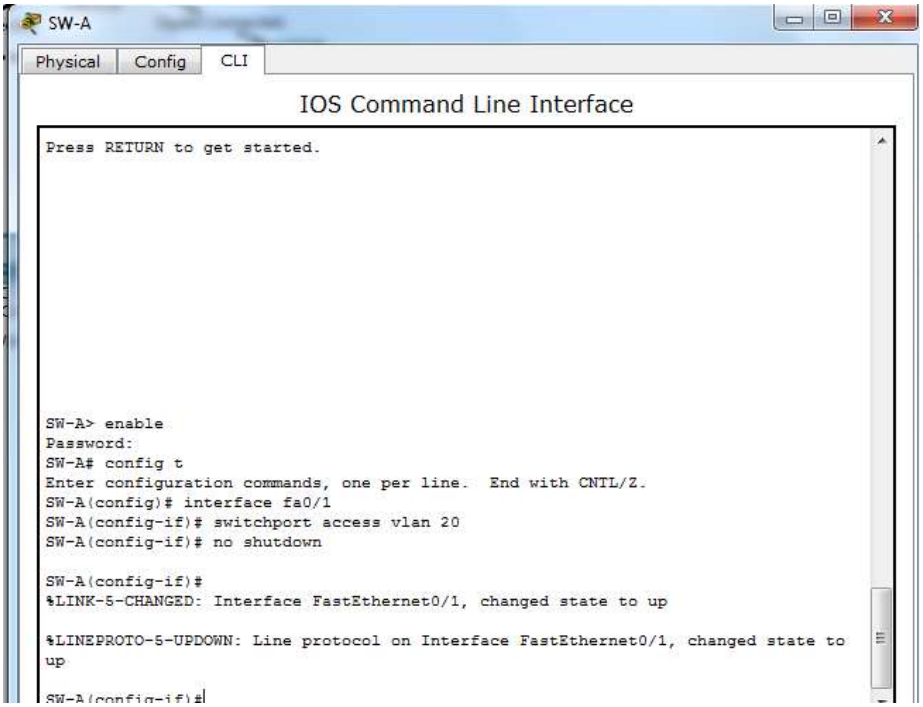




Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface Fa0/1 must be part of VLAN 20.

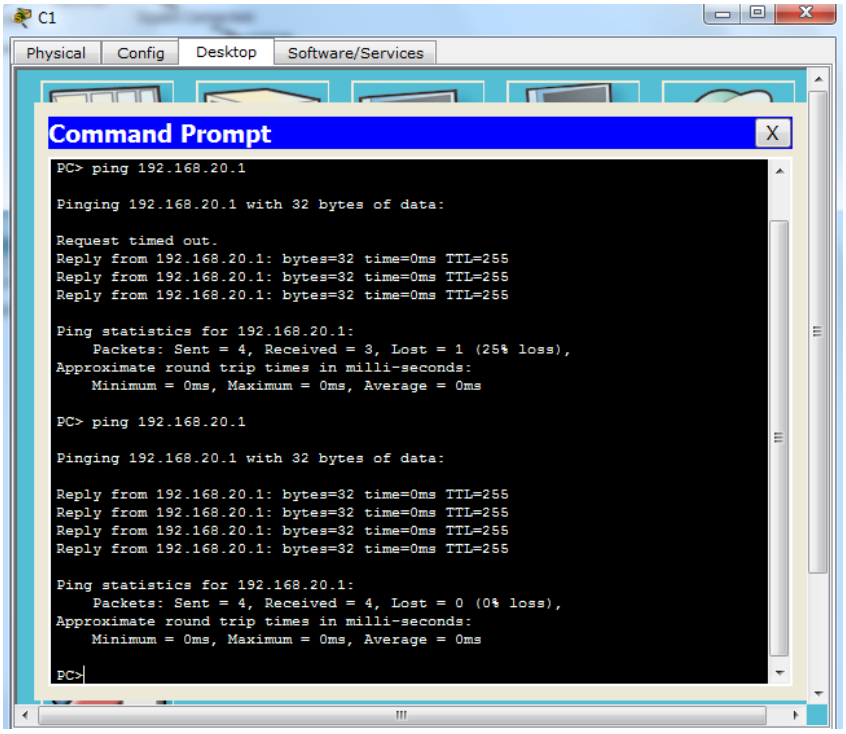
SW-A(config)# interface fa0/1
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# no shutdown



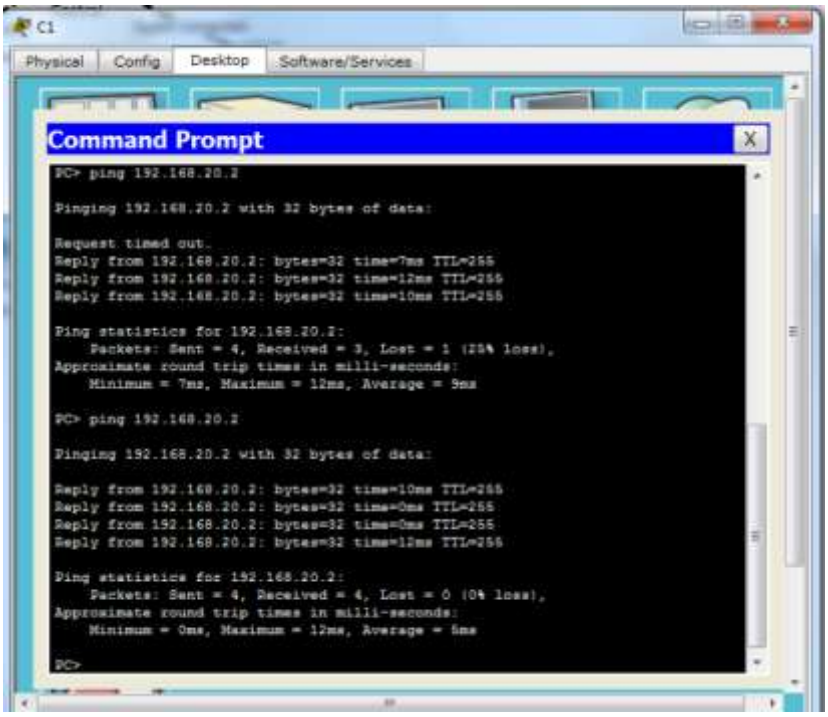
Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and Central.

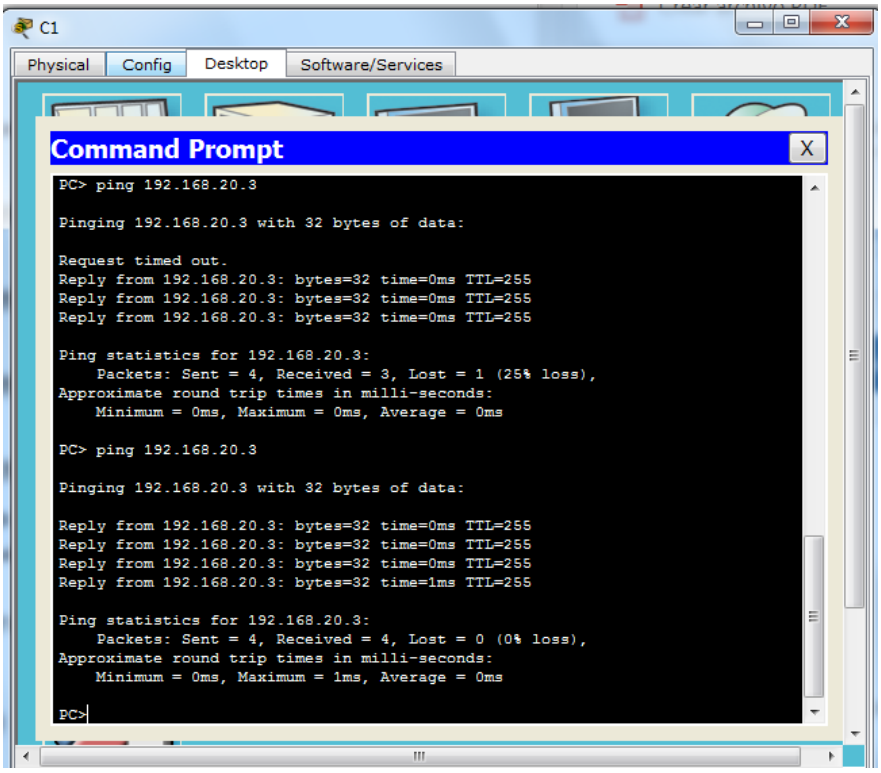
SW-A



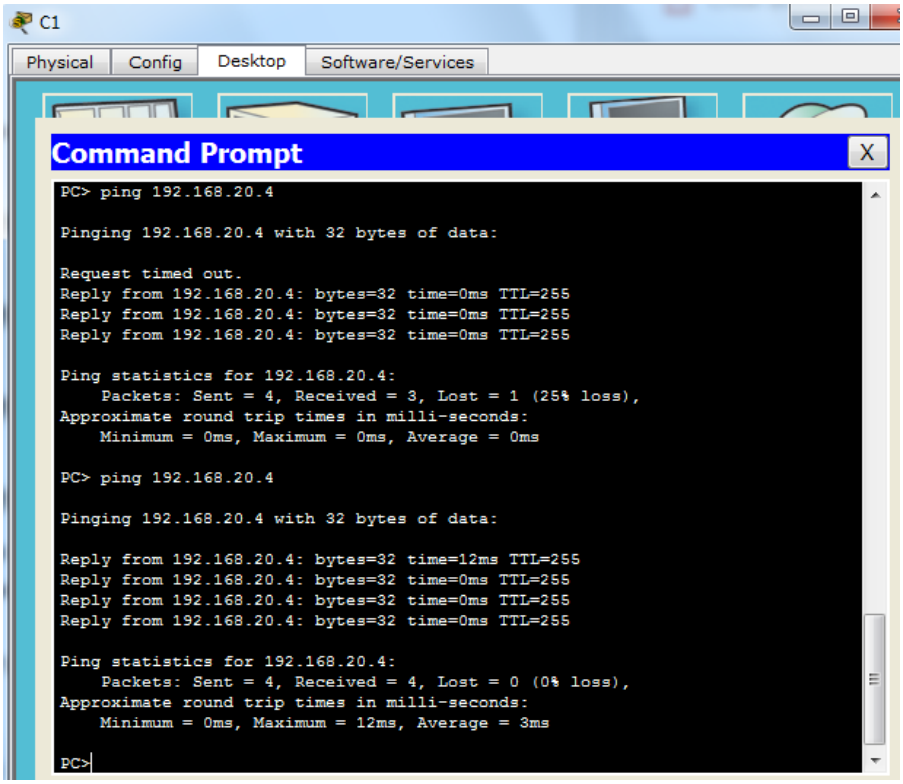
SW-B



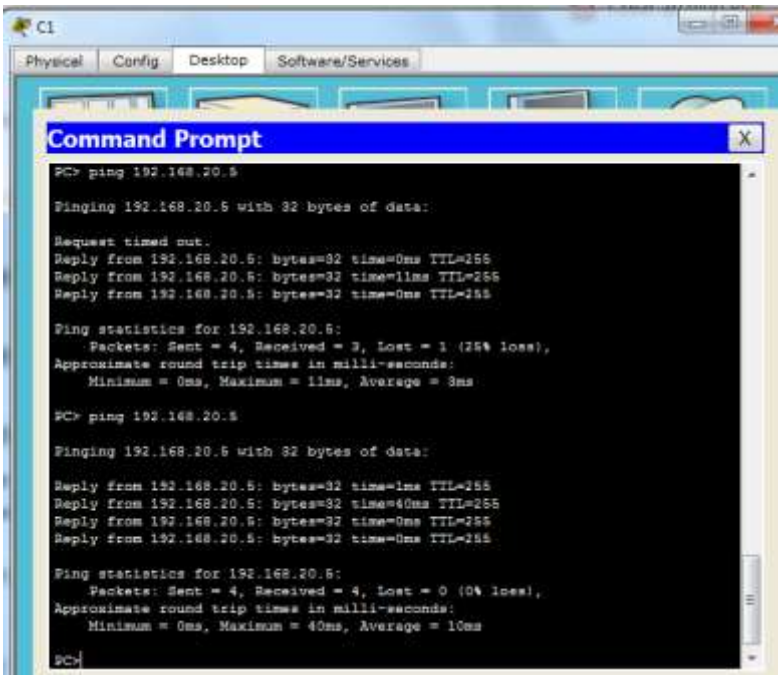
SW-1


C1
Physical
Config
Desktop
Software/Services
Command Prompt
X
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=255
Reply from 192.168.20.3: bytes=32 time=0ms TTL=255
Reply from 192.168.20.3: bytes=32 time=0ms TTL=255
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
PC> ping 192.168.20.3
Pinging 192.168.20.3 with 32 bytes of data:
Reply from 192.168.20.3: bytes=32 time=0ms TTL=255
Reply from 192.168.20.3: bytes=32 time=0ms TTL=255
Reply from 192.168.20.3: bytes=32 time=0ms TTL=255
Reply from 192.168.20.3: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.20.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

SW-2


C1
Physical
Config
Desktop
Software/Services
Command Prompt
X
PC> ping 192.168.20.4
Pinging 192.168.20.4 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.20.4:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC> ping 192.168.20.4
Pinging 192.168.20.4 with 32 bytes of data:
Reply from 192.168.20.4: bytes=32 time=12ms TTL=255
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Reply from 192.168.20.4: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.20.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
PC>

Central



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.

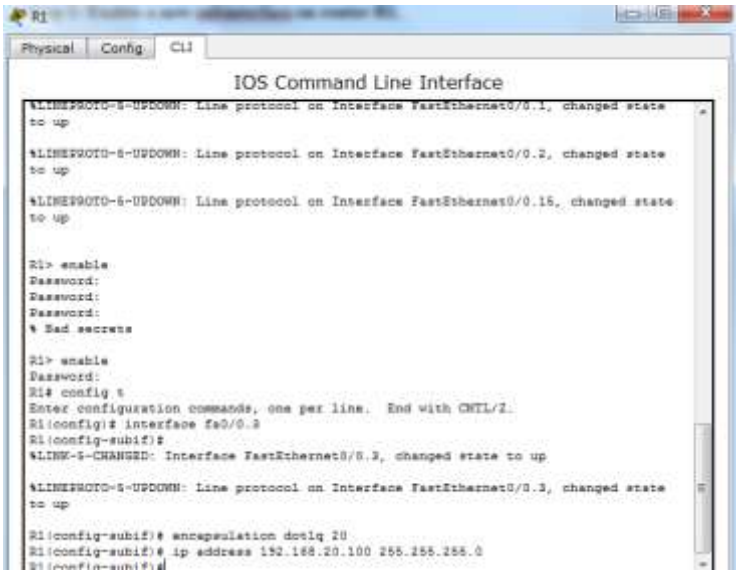
R1(config)# interface fa0/0.3

R1(config-subif)# encapsulation dot1q 20.

b. Assign an IP address within the 192.168.20.0/24 network.

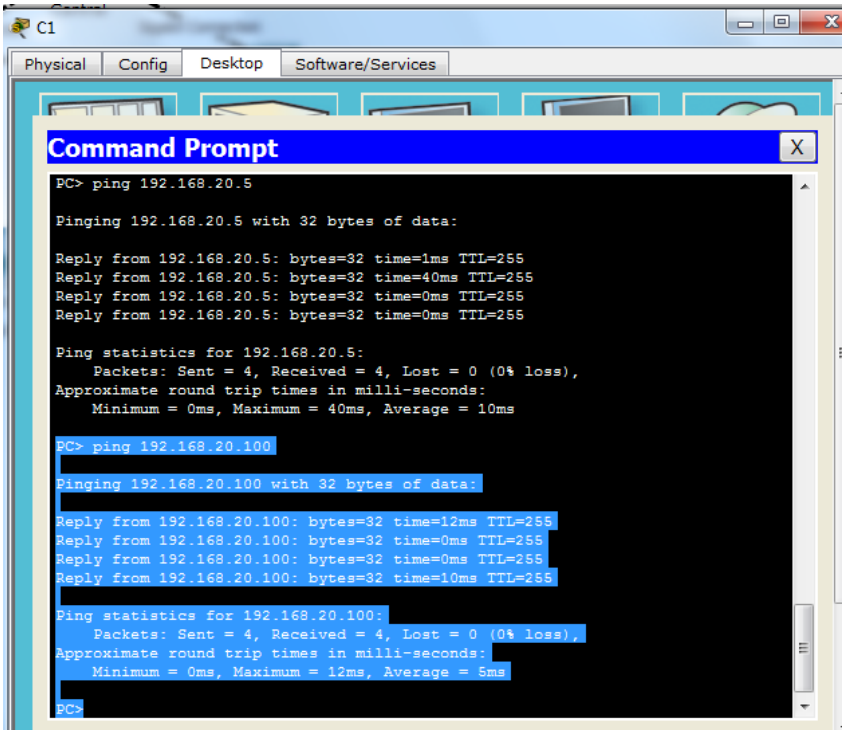
R1(config)# interface fa0/0.3

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.

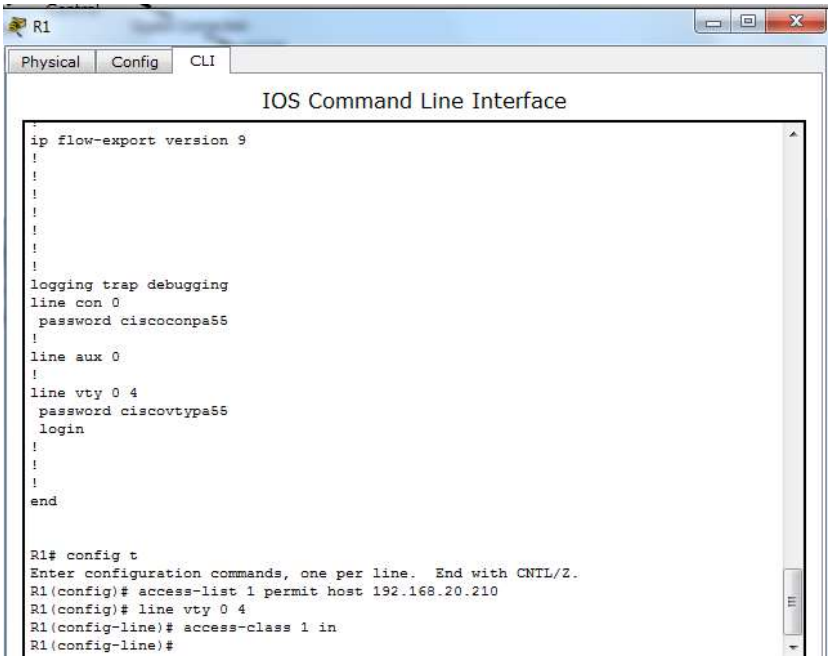
While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

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).

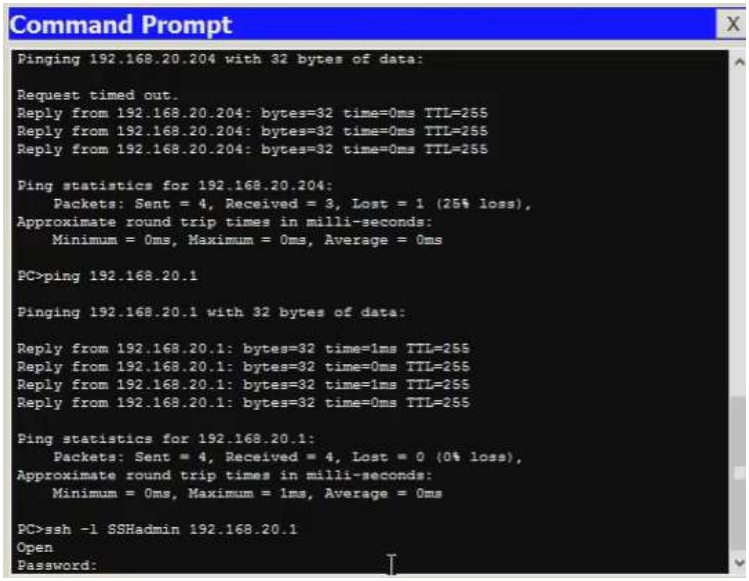
Example: (may vary from student configuration)
R1(config)# interface fa0/0.1
R1(config-subif)# ip access-group 101 in
R1(config-subif)# interface fa0/0.2
R1(config-subif)# ip access-group 101 in



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.



The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

b. From D1, ping the management PC. Were the pings successful? Explain.

The ping should have failed. This is because in order for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

Step 5: Check results.

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.

!!! Script for SW-1

```
conf t
interface fa0/23
switchport mode trunk
switchport trunk native vlan 15
switchport nonegotiate
no shutdown
vlan 20
exit
interface vlan 20
ip address 192.168.20.3 255.255.255.0
```

!!! Script for SW-2

```
conf t
interface fa0/23
switchport mode trunk
switchport trunk native vlan 15
switchport nonegotiate
no shutdown
vlan 20
exit
interface vlan 20
ip address 192.168.20.4 255.255.255.0
```

!!! Script for SW-A

```
conf t
vlan 20
exit
interface vlan 20
```

ip address 192.168.20.1 255.255.255.0
interface fa0/1
switchport access vlan 20
no shutdown

!!! Script for SW-B

conf t
vlan 20
exit
interface vlan 20
ip address 192.168.20.2 255.255.255.0

!!! Script for Central

conf t
vlan 20
exit
interface vlan 20
ip address 192.168.20.5 255.255.255.0

!!! Script for R1

conf t
interface fa0/0.3
encapsulation dot1q 20
ip address 192.168.20.100 255.255.255.0
access-list 101 deny ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
interface FastEthernet0/0.1
ip access-group 101 in
interface FastEthernet0/0.2
ip access-group 101 in

Conclusión

El desarrollo de las temáticas para esta tercera etapa como son Introducción a redes conmutadas, Configuración y conceptos básicos de Switching, VLANs, Conceptos de Routing, Enrutamiento entre VLANs, Enrutamiento Estático, En una red fueron de gran importancia para el aprendizaje individual y consecutivamente grupal, por medio de la simulación y conceptualización de cada uno de los temas que cuenta esta tercera unidad.

La iteración y socialización de los laboratorios en el foro propuesto para el desarrollo de las tareas fue de gran ayuda, pues nos fortalecimos unos a otros con el compromiso de adquirir nuevos conocimientos a partir de los informes expuestos por todos y cada uno de los miembros del grupo.

El desarrollo de la Unidad 3, es fundamental porque permite que el aprendiz adquiera la capacidad en desarrollar sistemas de redes, entendiendo la estructura física y lógica que deben tener, aplicando conocimientos básicos en el manejo de Configuración de Sistemas de red soportados en VLANs.

Con las prácticas de laboratorio y el manejo Configuración de Sistemas de red soportados en VLANs por medio de la aplicación Packet Tracer, los estudiantes pudieron entender y conocer el comportamiento de la red al aplicar los ejercicios ordenados para el desarrollo de la Unidad 3.

En general puede observarse el interés para lograr el aprendizaje a través del desarrollo de este curso por la importancia que tiene para la vida personal y en el ámbito profesional de cada uno de los participantes en este diplomado.

Bibliografía

- Unidad 3. https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1 Recuperado abril 2017

- Configuración de swiths. http://gonsystem.blogspot.com.co/2010/10/configurar-usuario-y-contrasena-cisco.html recuperado en abril 2017.

- Dhcp. http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html Recuperado en noviembre 2017.
- Guía de configuración. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html

- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html

- http://blog.capacityacademy.com/2014/06/06/cisco-ccna-como-configurar-vlan-en-switch-cisco/