Diplomado De Profundizacion Cisco

Actividad Final

Entregado Por:

Pablo Andres Tovar Guerra

Escuela De Ciencias Básicas Tecnología E Ingeniería

Programa De Ingeniería Electrónica/Telecomunicaciones

Ibague-Tolima

Noviembre 15 de 2017

Diplomado De Profundizacion Cisco

Actividad Final

Entregado Por:

Pablo Andres Tovar

Tutor:

Nilson Albeiro Ferreira

Escuela De Ciencias Básicas Tecnología E Ingeniería

Programa De Ingeniería Electrónica/Telecomunicaciones

Ibague-Tolima

Noviembre 15 de 2017

1. Introduccion.

Mediante la realización de este trabajo colaborativo se pretende realizar una conceptualización general de las temáticas desarrolladas en las unidades vistas durante el curso de diplomado como opción de grado, se trataron temas como el Modelo OSI y Direccionamiento IP, (Diseño e Implementación de Soluciones Integradas LAN / WAN), a la vez que se desarrollan una serie de actividades prácticas mediante la herramienta de simulación Packet Tracer según sea requerido. Las temáticas a tratar en este momento de evaluación corresponden a, Capa de transporte, Asignación de direcciones IP, División de redes en subredes, Capa de transporte y capa de aplicación.

A continuación se presenta un informe detallado de las actividades realizadas por los estudiantes del grupo de trabajo 203092_13, mediante los cuales se evidencia el desarrollo de cada una de los ejercicios prácticos correspondientes a la temática trabajada en cada uno de los capítulos de la unidad.

2. Objetivos

Objetivos General:

- Identificar y solucionar problemas propios de subredes y direccionamiento IP, mediante el uso adecuado de herramientas y estrategias basadas en comandos y características del IOS.

Objetivos Específicos:

- Conceptualizar la temática planteada para la unidad 2 en lo que respecta a direccionamiento IP, capa de transporte, división de redes en subredes, funcionalidad y estructura de la capa de aplicación, del curso de profundización.
- Aplicar dichas temáticas en cada uno de los ejercicios propuestos.
- Utilizar la herramienta de simulación Packet Tracer de acuerdo a requisitos establecidos.
- Participar activamente en el foro asignado para el desarrollo del trabajo colaborativo.

3. Desarrollo De La Actividad.

Informe Del Desarrollo De Las Tareas Prácticas Propuestas

2.1.1.6 Lab - Configuring Basic Switch Settings

Práctica de laboratorio: configuración de los parámetros básicos de un switch

Topología

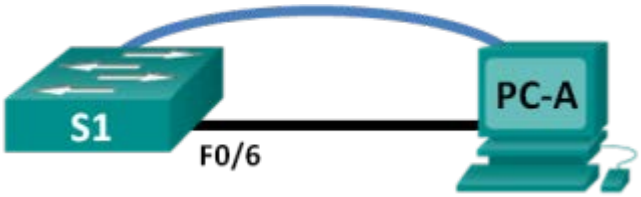


Tabla de direccionamiento

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

Objetivos

Parte 1: tender el cableado de red y verificar la configuración predeterminada del switch

Parte 2: configurar los parámetros básicos de los dispositivos de red

- Configurar los parámetros básicos del switch.
- Configurar la dirección IP de la computadora.

Parte 3: verificar y probar la conectividad de red

- Mostrar la configuración del dispositivo.
- Probar la conectividad de extremo a extremo con ping.
- Probar las capacidades de administración remota con Telnet.
- Guardar el archivo de configuración en ejecución del switch.

Parte 4: administrar la tabla de direcciones MAC

- Registrar la dirección MAC del host.

- Determine las direcciones MAC que el switch ha aprendido.
- Enumere las opciones del comando **show mac address-table**.
- Configure una dirección MAC estática.

Información básica/situación

Los switches Cisco se pueden configurar con una dirección IP especial, conocida como “interfaz virtual de switch” (SVI). La SVI o dirección de administración se puede usar para el acceso remoto al switch a fin de ver o configurar parámetros. Si se asigna una dirección IP a la SVI de la VLAN 1, de manera predeterminada, todos los puertos en la VLAN 1 tienen acceso a la dirección IP de administración de SVI.

En esta práctica de laboratorio, armará una topología simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto. Examinará la configuración predeterminada del switch antes de configurar los parámetros básicos del switch. Esta configuración básica del switch incluye el nombre del dispositivo, la descripción de interfaces, las contraseñas locales, el mensaje del día (MOTD), el direccionamiento IP, la configuración de una dirección MAC estática y la demostración del uso de una dirección IP de administración para la administración remota del switch. La topología consta de un switch y un host que solo usa puertos Ethernet y de consola.

Nota: el switch que se utiliza es Cisco Catalyst 2960 con IOS de Cisco versión 15.0(2) (imagen 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 el switch se haya borrado y no tenga una configuración de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term, y capacidad para Telnet)
- Cable de consola para configurar el dispositivo con IOS de Cisco mediante el puerto de consola
- Cable Ethernet, como se muestra en la topología

Part 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.

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

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

   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 el switch aún no tiene configuración de ip ni ningún parámetro correcto de conectividad establecido, ni tampoco un nombre único de host, por tanto no cumple con las configuraciones mínimas.

   Topología antes de la configuración de parámetros básicos

Step 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.

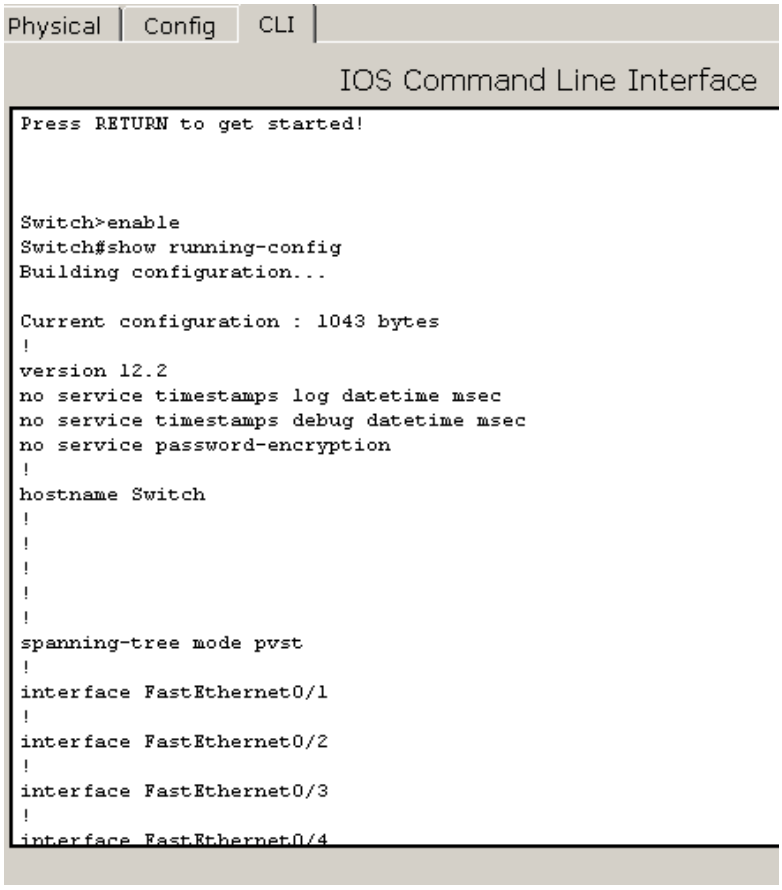
a. Si se parte de la suposición de que el switch no tenía ningún archivo de configuración almacenado en la memoria de acceso aleatorio no volátil (NVRAM), usted estará en la petición de entrada del modo EXEC del usuario en el switch, con la petición de entrada Switch>. Use el comando **enable** para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

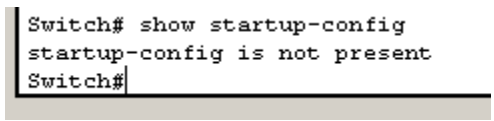
¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960? **2**

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

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 aún no hay parámetros configurados**

c. 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 0001.4368.9b4a (bia 0001.4368.9b4a)
  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#
```

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

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

```
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0001.4368.9b4a (bia 0001.4368.9b4a)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
```

¿Está activa esta interfaz? **La interfaz no está activa**

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

Switch# **show ip interface vlan1**

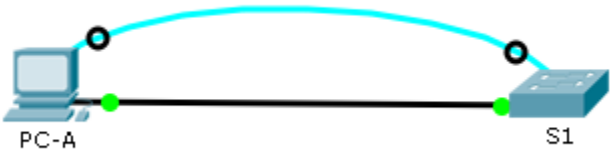
```
Switch#
Switch#show ip interface vlan1
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
Switch#
```

¿Qué resultado ve?

Este comando debería mostrarnos información sobre la IP configurada para la interfaz vlan1, pero no hay información porque aún no se ha configurado.

e. 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?

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

Vlan1 está administrativamente inactivo, el protocolo de línea está inactivo. Procesamiento de protocolo de Internet deshabilitado

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

Switch# **show versión**

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

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

System returned to ROM by power-on

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


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

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0001.4368.9B4A
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
 --More--
```

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

Versión 12.2 (25)FX

¿Cuál es el nombre del archivo de imagen del sistema?

C2960-LANBASE-M

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

0001.4368.9B4A

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

Switch# **show interface f0/6**

```
Switch#show interface f0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Lance, address is 0007.ec74.1506 (bia 0007.ec74.1506)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

¿La interfaz está activa o desactivada?

Esta activa

¿Qué haría que una interfaz se active?

El comando no shutdown o para este caso en específico que esté conectada.

¿Cuál es la dirección MAC de la interfaz?

0007.ec74.1506;

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

Full-duplex, 100Mb/s

Examine la configuración VLAN predeterminada del switch.

Switch# **show vlan**

```
Switch#show vlan

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

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

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


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

¿Cuál es el nombre predeterminado de la VLAN 1? **Por defecto (default**)

¿Qué puertos hay en esta VLAN? **Del Fa0/1 al Fa0/24 y Gig0/1 Gig0/2**

¿La VLAN 1 está activa? **Si esta activa**

¿Qué tipo de VLAN es la VLAN predeterminada? **TYPE SAID**

h. Examine la memoria flash.

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

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

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

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

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

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
```

Part 2: configurar los parámetros básicos de los dispositivos de red

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

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

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>
```

//Procedimiento realizado//

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sl
Sl(config)#service password-encryption
Sl(config)#enable secret class
Sl(config)#no ip domain-lookup
Sl(config)#banner motd #Prohibido el acceso no autorizado#
Sl(config)#exit
Sl#
%SYS-5-CONFIG_I: Configured from console by console

Sl#exit
```

Una vez que salimos y hacemos un enter podemos apreciar el mensaje que configuramos anteriormente igual que los parámetros de contraseña de acceso al modo privilegiado

```
Prohibido el acceso no autorizado

Sl>
```

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

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.

```
Prohibido el acceso no autorizado

Sl>enable
Password:
Sl#
```

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)#
```

//Procedimiento realizado//

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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)#
```

//Procedimiento realizado//

En éste primer pantallazo, se puede apreciar que los puertos aún están asignados a la vlan por defecto. Esto dado que se presentó un error de omisión de una línea de comando.

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/1-24,g0/1-2
S1(config-if-range)#exit
S1(config)#exit
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, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
99   VLAN0099                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
S1#show vlan99 brief
```

Una vez que se corrige, agregando la línea de comando (**S1(config-if-range)#switchport access vlan 99**) después de establecer los rangos de puerto, podemos verificar nuevamente:

```
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

S1#
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#
```

Y observamos que ya están asignados el rango de puertos a la vlan99.

```
%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
```

//Desarrollado en el enciso anterior.//

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
```

//Proceso desarollado //

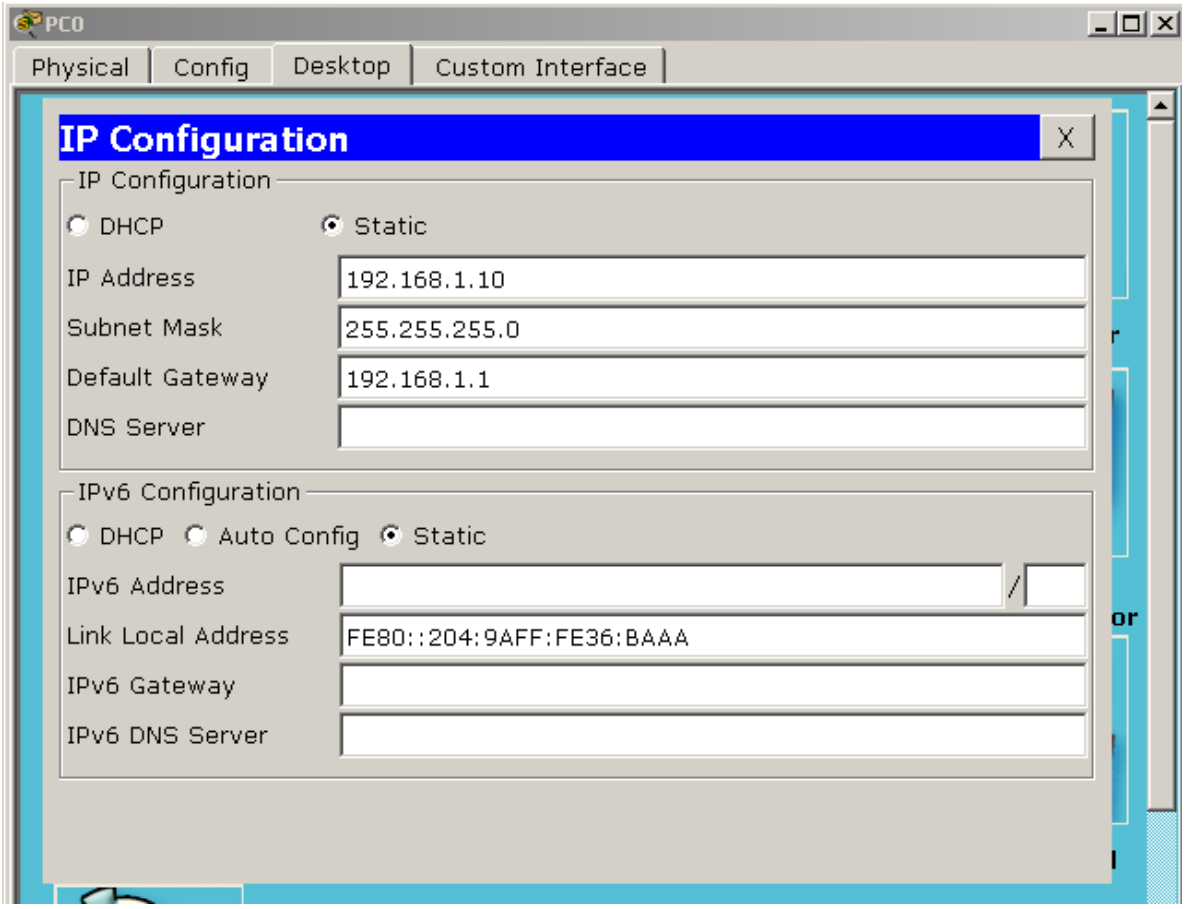
```
Prohibido el acceso no autorizado

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.1.1
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)#
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

¿Por qué se requiere el comando **login**? **Para que se aplique la configuración.**

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

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

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



Part 3: verificar y probar la conectividad de red

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

Step 1: mostrar la configuración del switch.

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

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

```
S1# show run
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#
```

//Verificando //

```
S1>enable
Password:
S1#show run
Building configuration...

Current configuration : 2048 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 99
 --More--
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
!
banner motd ^CProhibido el acceso no autorizado^C
!
!
 --More--

!
!
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
!
end

S1#
```

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

```
S1# show interface vlan 99
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? **BW 1000000 Kbit**

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

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

//Verificando//

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0001.4368.9b4a (bia 0001.4368.9b4a)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
S1#
```

¿Cuál es el ancho de banda en esta interfaz? **BW 100000 Kb o 100 MB**

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

¿Cuál es el estado del protocolo de línea? **is up o Activo**

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

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

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

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=15ms TTL=128
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128
Reply from 192.168.1.10: bytes=32 time=0ms TTL=128
Reply from 192.168.1.10: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 5ms

PC>
```

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`**

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

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.

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

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

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.

Se realizan todos los pasos anteriores. Primero accedemos mediante telnet para ello utilizamos el comando **telnet 192.168.1.2** y nos autenticamos con la contraseña. A continuación entramos al modo de EXEC privilegiado para lo cual también debemos proporcionar la contraseña. Finalmente utilizamos el comando **exit** para salir,

Step 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#
```

//verificacion//

```
Prohibido el acceso no autorizado

User Access Verification

Password:

S1>enable
Password:
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Part 4: Administrar la tabla de direcciones MAC

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

Step 1: registrar la dirección MAC del host.

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

```
PC> ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0004.9A36.BAAA
   Link-local IPv6 Address.........: FE80::204:9AFF:FE36:BAAA
   IP Address.......................: 192.168.1.10
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.1.1
   DNS Servers......................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID...............: 00-01-00-01-56-B5-74-81-00-04-9A-36-BA-AA


PC>
```

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

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

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

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

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

  99    0004.9a36.baaa    DYNAMIC     Fa0/6
S1#
```

¿Cuántas direcciones dinámicas hay? **1**

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

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

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

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

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

¿Cuántas opciones se encuentran disponibles para el comando **show mac address-table**? Dinamic, interfaces, static.

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

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**

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

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

  99    0004.9a36.baaa    DYNAMIC      Fa0/6
```

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>**

La respuesta es commando invalido.

```
Sl#show mac address-table address <0004.9a36.baaa>
                                  ^
% Invalid input detected at '^' marker.
```

Step 4: Configure una dirección MAC estática.

a. limpie la tabla de direcciones MAC.

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

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

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

S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay? Ninguna

¿Cuántas direcciones dinámicas hay? Ninguna

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

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

c. Examine nuevamente la tabla de direcciones MAC

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

S1# **show mac address-table**

¿Cuántas direcciones dinámicas hay? Ninguna

¿Por qué cambió esto desde la última visualización? **No cambio**

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**.

Se realiza el ping

```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=0ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255
Reply from 192.168.1.2: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Y repetimos el comando show mac address-table. Se visualiza nuevamente dirección MAC.

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

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

  99    0004.9a36.baaa    DYNAMIC     Fa0/6
```

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 0050.56BE.6C89 vlan 99 interface fastethernet 0/6`**

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#mac address-table static 0004.9a36.baaa vlan 99 interface
fastethernet 0/6
```

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

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

```
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
----    -----------       --------    -----

  99    0004.9a36.baaa    STATIC      Fa0/6
S1#
```

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

¿Cuántas direcciones estáticas hay? **1**

f. Elimine la entrada de MAC estática. Ingrese al modo de configuración global y elimine el comando escribiendo **no** delante de la cadena de comandos.

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`**

```
S1(config)#no mac address-table static 0004.9a36.baaa vlan 99 interface
fastethernet 0/6
S1(config)#
```

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

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

```
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
----    -----------       --------    -----
```

Ya no esta la dirección MAC estática.

¿Cuántas direcciones MAC estáticas hay en total? **Ninguna**

Reflexión

1. ¿Por qué debe configurar las líneas vty para el switch?

   Para que se pueda dar una conexión remota. En este caso específico la conexión telnet.

2. ¿Para qué se debe cambiar la VLAN 1 predeterminada a un número de VLAN diferente?

   Por seguridad.

3. ¿Cómo puede evitar que las contraseñas se envíen como texto no cifrado?

   Configurando la encriptación de las mismas.

4. ¿Para qué se debe configurar una dirección MAC estática en una interfaz de puerto?

Para especificar a qué puerto específico se debe conectar un host.

Apéndice A: inicialización y recarga de un router y un switch

Step 1: inicializar y volver a cargar el router. (No aplica)

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

```
Router> enable
Router#
```

b. Introduzca el comando **erase startup-config** para eliminar la 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?, presione Enter. (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 una petición de entrada para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **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. Aparece otra petición de entrada para finalizar la instalación automática. Responda escribiendo **yes** (sí) y presione Enter.

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

Step 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#
```

//se realiza el procedimiento//

```
Prohibido el acceso no autorizado

User Access Verification

Password:

Sl>enable
Password:
Sl#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    4  -rw-        2048          <no date>  config.text
    2  -rw-         616          <no date>  vlan.dat

64016384 bytes total (59598799 bytes free)
Sl#
```

Efectivamente se encuentra el archivo vlan.dat

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

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

Se procede a eliminarlo

d. Se le solicitará que verifique el nombre de archivo. Si introdujo el nombre correctamente, presione Enter; de lo contrario, puede cambiar el nombre de archivo.

e. Se le solicita que confirme la eliminación de este archivo. Presione Intro para confirmar.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

//Proceso//

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

Sl#
```

f. Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicita que elimine el archivo de configuración. Presione Intro para confirmar.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

//proceso//

```
Sl#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
Sl#
```

g. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Luego, recibirá una petición de entrada para confirmar la recarga del switch. Presione Enter para continuar.

```
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. Responda escribiendo **no** y presione Enter.

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

h. Una vez que se vuelve a cargar el switch, debe ver una petición de entrada del diálogo de configuración inicial. Responda escribiendo **no** en la petición de entrada y presione Enter.

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

//Una vez de reiniciado el Switch esta es la información que se evidencia//

```
Sl#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0001.4368.9B4A
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
################################################################################ [OK]
              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, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Image text-base: 0x80008098, data-base: 0x814129C4



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


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


63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0001.4368.9B4A
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


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

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

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to
up


Switch>
```

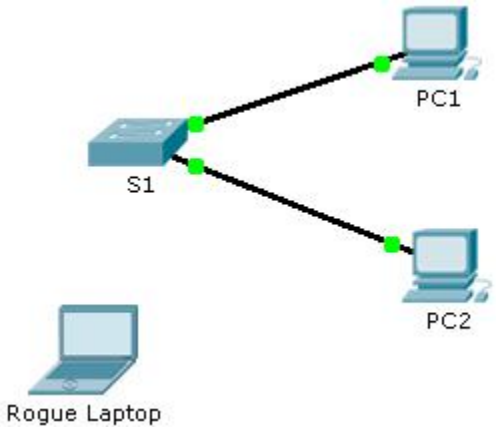
Nota: El archivo pka se conserva con las configuraciones de parámetros básicos con el fin de evidenciar el trabajo realizado. En lo que respecta a la asignación de la dirección MAC estática no se logra evidenciar dado que

uno de los pasos fue borrar esta dirección. Para verificar la dirección MAC dinámica basta con realizar un pin desde la PC-A al Switch y luego utilizar el comando **show mac address-table**

2.2.4.9 Packet Tracer - Configuring Switch Port Security Instructions – IG

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
```

//Realuizado//

```
Sl>enable
Sl#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sl(config)#
Sl(config)#interface range fa0/1 - 2
Sl(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
```

a. 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
```

b. 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
```

//Realizado//

```
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
```

Con el comando S1# show port-security interface fastethernet 0/1, verificamos el estado de la configuración realizada en esta interfaz.

```
S1#show port-security interface fastethernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.B027.2245:1
Security Violation Count   : 0
```

Con el comando S1# show port-security interface fastethernet 0/2, verificamos el estado de la configuración realizada es la interfaz fa0/2

```
S1#show port-security interface fastethernet 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.647C.697E:1
Security Violation Count   : 0

S1#
```

c. 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 ,
gi1/1 - 2 S1(config-if-range)# shutdown
```

//Realizado//

Primero deshabilitamos los puertos fastethernet del 3 al 24.

```
Sl#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sl(config)#
Sl(config)#interface range f0/3 - 24
Sl(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

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

……

```
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
Sl(config-if-range)#
```

//Verificamos con el comando show ip interface brief//

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
```

//Ahora deshabilitamos los puertos G0/1 hasta el 2//

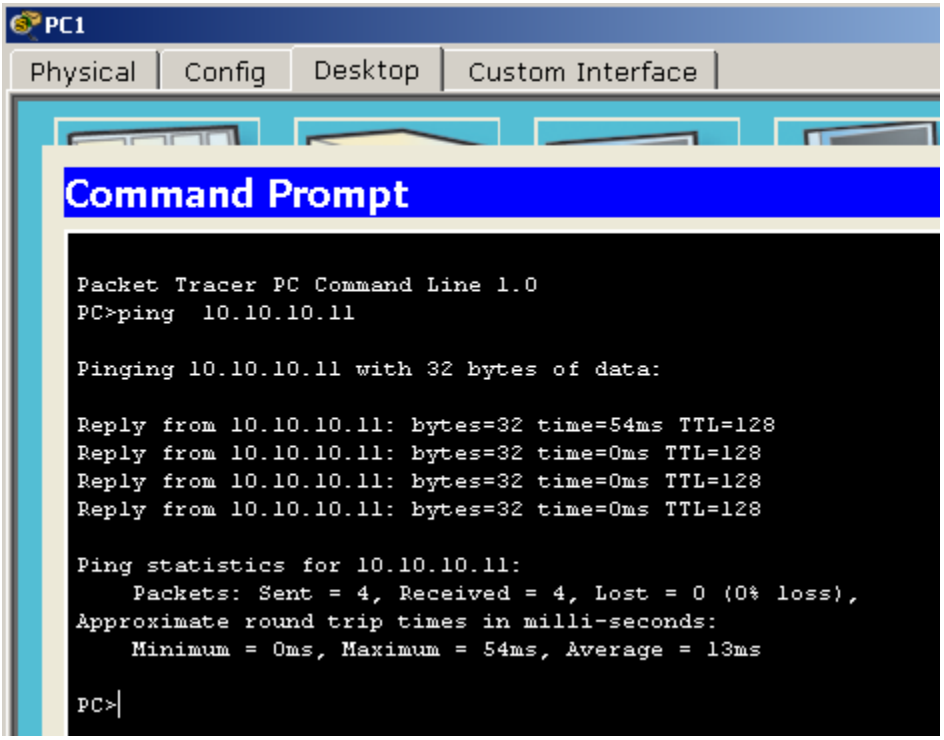
```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range g0/1 - 2
S1(config-if-range)#shutdown
S1(config-if-range)#end
S1#
```

//Verificamos con el comando show ip interface brief//

```
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
```

Part 2: Verify Port Security

d. From **PC1**, ping **PC2**.

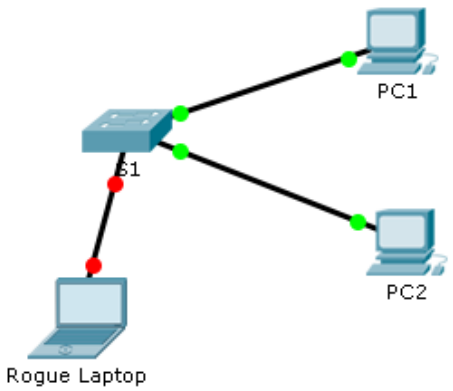


e. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

//Verificando//

```
S1>enable
S1#show port-security address
                                    Secure Mac Address Table
------------------------------------------------------------------------------
Vlan       Mac Address Type                                    Ports
Remaining Age

(mins)
----       -----------  ----                                   -----
-------------
1          00E0.B027.2245         SecureSticky
FastEthernet0/1                   -
1          0001.647C.697E         SecureSticky
FastEthernet0/2                   -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#
```

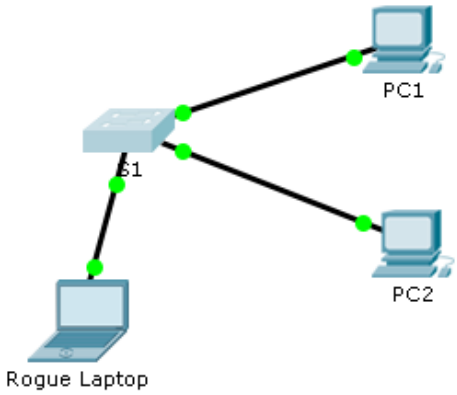
f. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

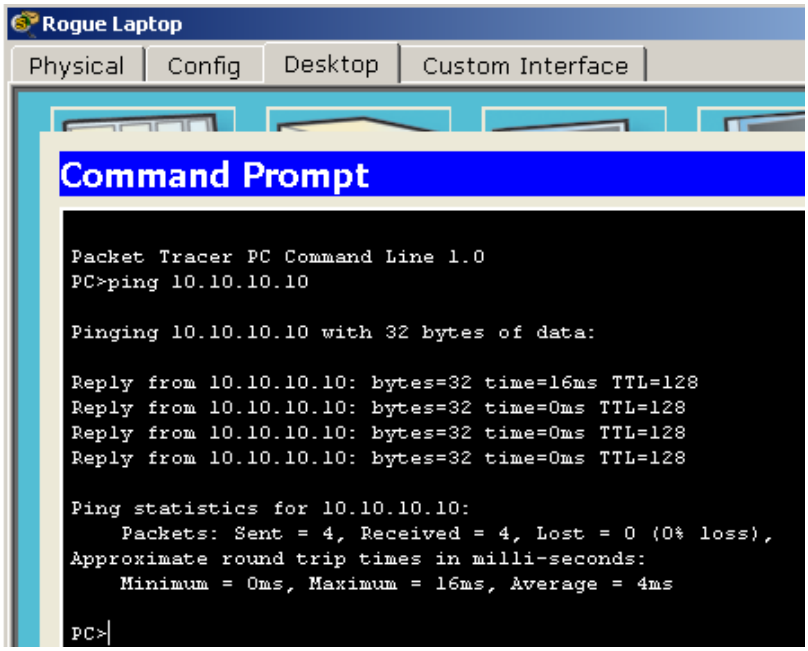


g. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

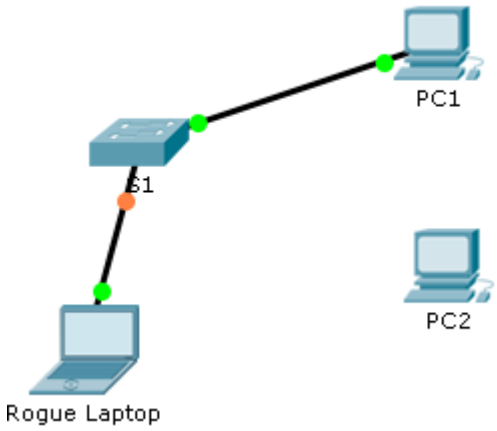
//Activamos el puerto//

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#interface fastethernet0/3
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up
```





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



El ping evidentemente no responde.

```
PC>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

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

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

`S1# show port-security interface fa0/2`

`//Verificamos con el comando anterior y evidenciamos la información de violación a la seguridad que se presenta//.`

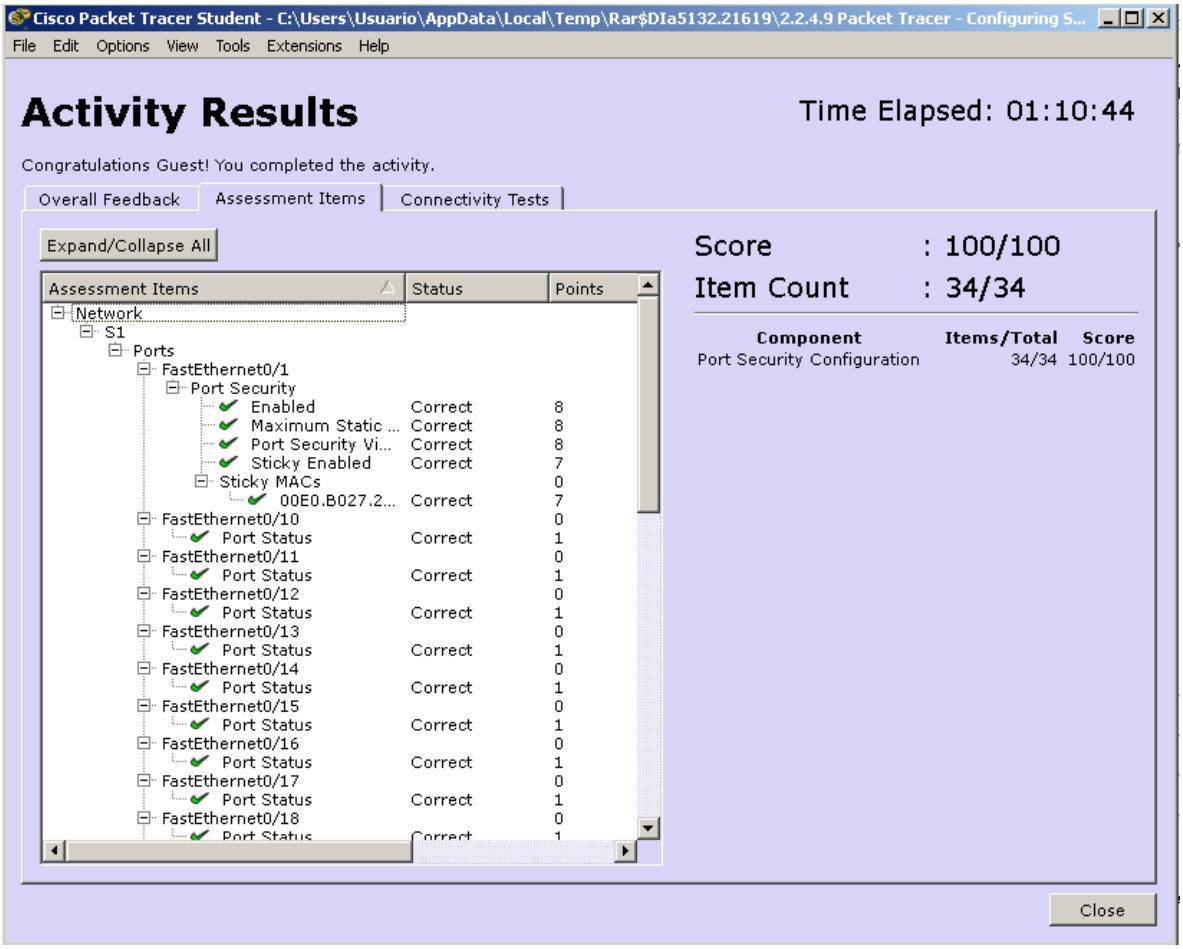
```
S1#show port-security interface fastethernet 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0002.4A42.C51C:1
Security Violation Count   : 4

S1#
```

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

```
PC>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=128
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Reply from 10.10.10.10: bytes=32 time=0ms TTL=128
Reply from 10.10.10.10: bytes=32 time=0ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

PC>
```

k. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?

R/ La seguridad del puerto que se habilitó en el puerto solo permitió que el dispositivo, cuyo MAC se aprendió primero, acceda al puerto y evite el acceso de todos los demás dispositivos.



2.2.4.11 Lab - Configuring Switch Security Features

Liliana Magaly Acosta Práctica de laboratorio: configuración de características de seguridad de switch

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

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 y verificar el acceso por SSH en el S1

- Configurar el acceso por SSH.
- Modificar los parámetros de SSH.
- Verificar la configuración de SSH.

Parte 4: configurar y verificar las características de seguridad en el S1

- Configurar y verificar las características de seguridad general.
- Configurar y verificar la seguridad del puerto.

Información básica/situación

Es muy común bloquear el acceso e instalar buenas características de seguridad en computadoras y servidores. Es importante que los dispositivos de infraestructura de red, como los switches y routers, también se configuren con características de seguridad.

En esta práctica de laboratorio, seguirá algunas de las prácticas recomendadas para configurar características de seguridad en switches LAN. Solo permitirá las sesiones de SSH y de HTTPS seguras. También configurará y verificará la seguridad de puertos para bloquear cualquier dispositivo con una dirección MAC que el switch no reconozca.

Nota: el router que se utiliza en las prácticas de laboratorio de CCNA es un router de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). El switch que se utiliza es 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. Si no está seguro, solicite ayuda al instructor o consulte las prácticas de laboratorio anteriores para conocer los procedimientos de inicialización y recarga de 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)
- 1 computadora (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

Part 5: 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.

Part 6: 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. **//hosname R1//**

b. Desactive la búsqueda del DNS. **//no ip domain-lookup//**

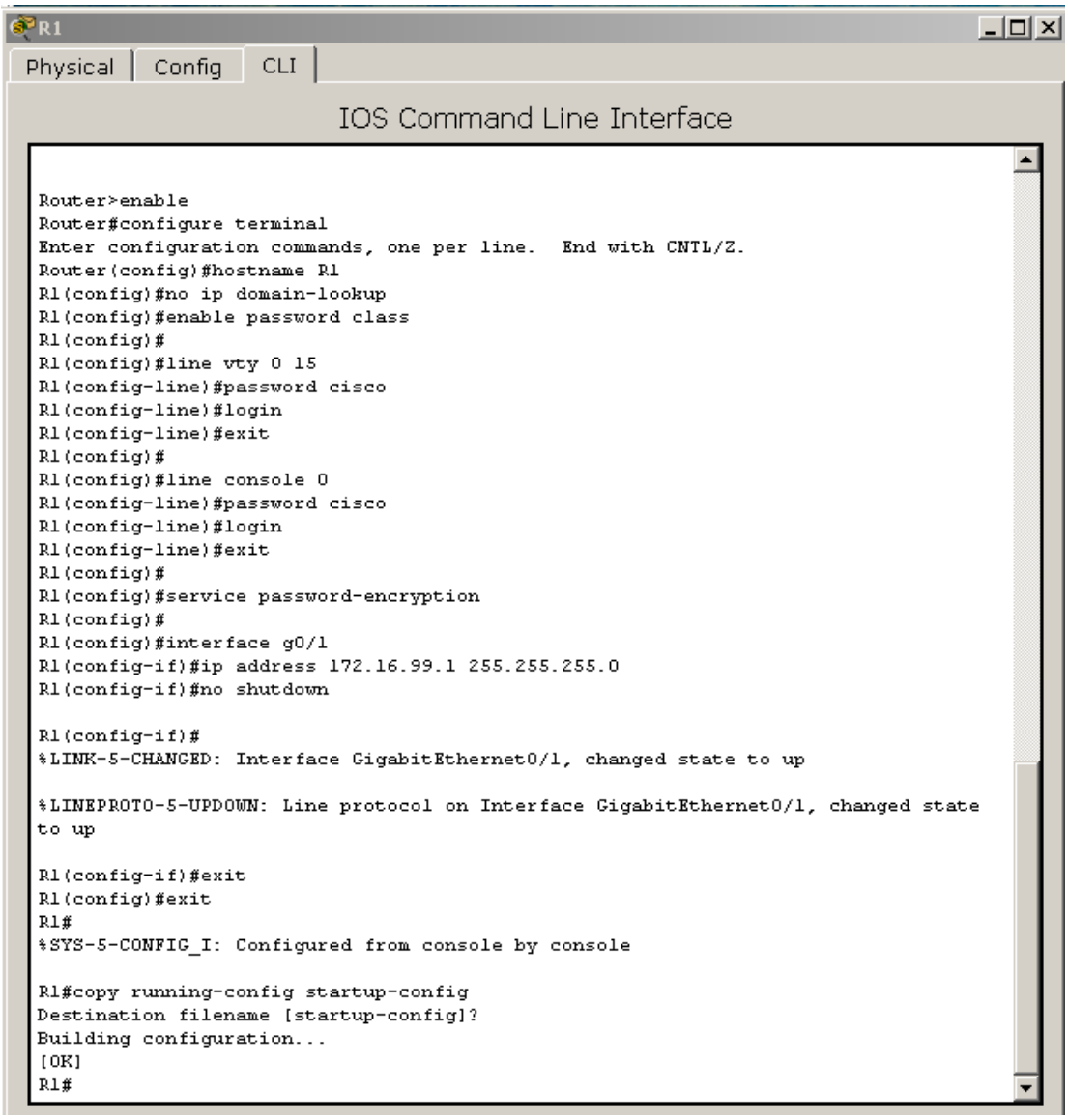
c. Configure la dirección IP de interfaz que se muestra en la tabla de direccionamiento. **//ip address 172.16.99.1 255.255.255.0// //no shutdown//**

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

e. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión. //line **vty 0 15// //password cisco// //login//**

f. Cifre las contraseñas de texto no cifrado. **//service password-encryption//**

g. Guarde la configuración en ejecución en la configuración de inicio. **//copy running-config-startup-config//**



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.

h. Configure el nombre del dispositivo. //**Switch(config)#hostname S1** //

i. Desactive la búsqueda del DNS. **//S1(config)#no ip domain-lookup//**

j. Asigne **class** como la contraseña del modo EXEC privilegiado**. //S1(config)#enable password class//**

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

//S1(config)#line vty 0 15
S1(config-line)#
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 //

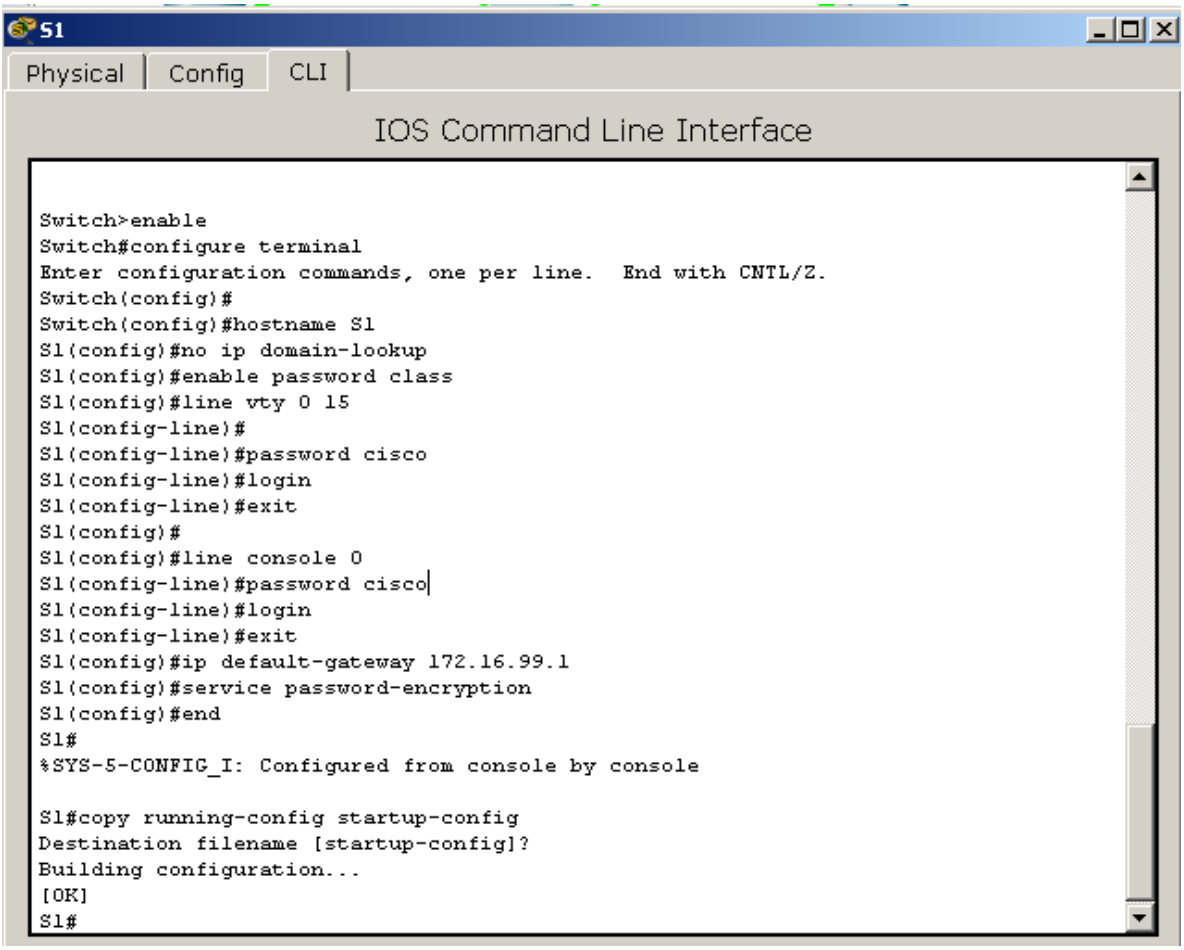
l. Configure un gateway predeterminado para el S1 con la dirección IP del R1.

//S1(config)#ip default-gateway 172.16.99.1//

m. Cifre las contraseñas de texto no cifrado.

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

n. Guarde la configuración en ejecución en la configuración de inicio**. //S1#copy running-config startup-config//**



o. 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)#
```

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

```
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#
```

//Desarrollado//

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 172.16.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
S1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
99   management                        active
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
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More--
```

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

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

Su estado es activo pero su protocolo caído, dado que aún no tiene ningún puerto asignado y por ende activo.

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

R/Como se mencionó anteriormente porque aún no se le han asignado puertos, y es la VLAN 1 quien por defecto tiene todos los puertos asignados.

s. 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
```

t. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99? **R/ Ambos están activos, dado que ya tiene asignados dos puertos.**

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

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

Agregue los puertos Fa/01, Fa/05 y Fa/6.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#interface f0/5
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)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

//Verificamos//

```
S1#show vlan

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
99   management                        active    Fa0/1, Fa0/5, Fa0/6
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Paso 4. verificar la conectividad entre los dispositivos.

u. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1 (**172.16.99.1**). ¿Los pings se realizaron correctamente? **R/Correcto**

```
Pinging 172.16.99.1 with 32 bytes of data:

Reply from 172.16.99.1: bytes=32 time=155ms TTL=255
Reply from 172.16.99.1: bytes=32 time=0ms TTL=255
Reply from 172.16.99.1: bytes=32 time=0ms TTL=255
Reply from 172.16.99.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.16.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 155ms, Average = 38ms
```

v. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente? **R/Correcto**

```
PC>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

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

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

w. En el S1, haga ping a la dirección de gateway predeterminado en el R1 (**172.16.99.1**). ¿Los pings se realizaron correctamente?

```
S1#ping 172.16.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/4/18 ms

S1#
```

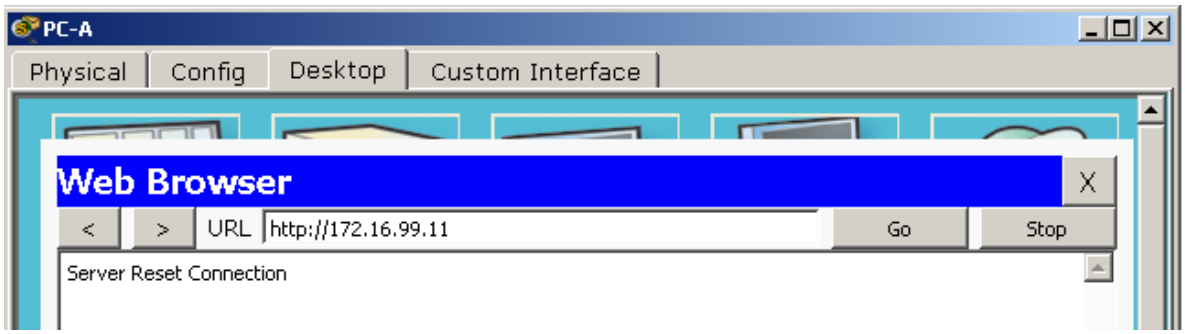
Esto nos indica que:

El envío de 5, 100-byte ICMP Echos a 172.16.99.1, tiempo de espera es de 2 segundos:

La tasa de éxito es del 80 por ciento (4/5), ida y vuelta min / avg / max = 0/4/18 ms

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

Esta es la respuesta obtenida



y. 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.

Part 7: 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.

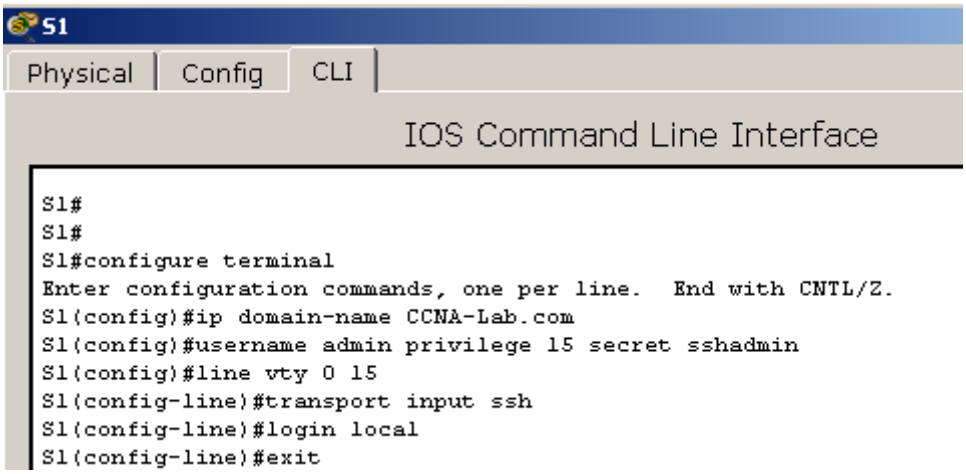
Nota: la contraseña que se utiliza aquí NO es una contraseña segura. Simplemente se usa a los efectos de esta práctica de laboratorio.

```
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.

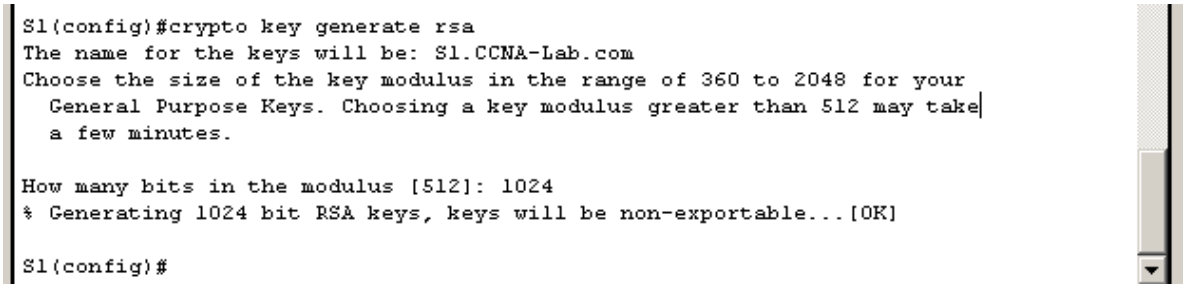
```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

//Realizado//



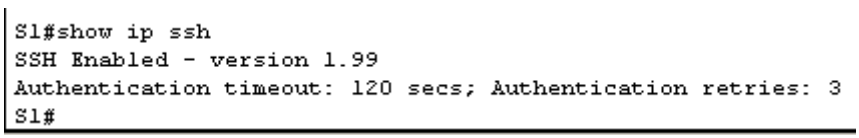
d. Genere una clave criptográfica RSA con un módulo de 1024 bits.

```
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
```



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

```
S1# show ip ssh
```



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

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

¿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
```

//Realizado//

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

```
S1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
S1#
```

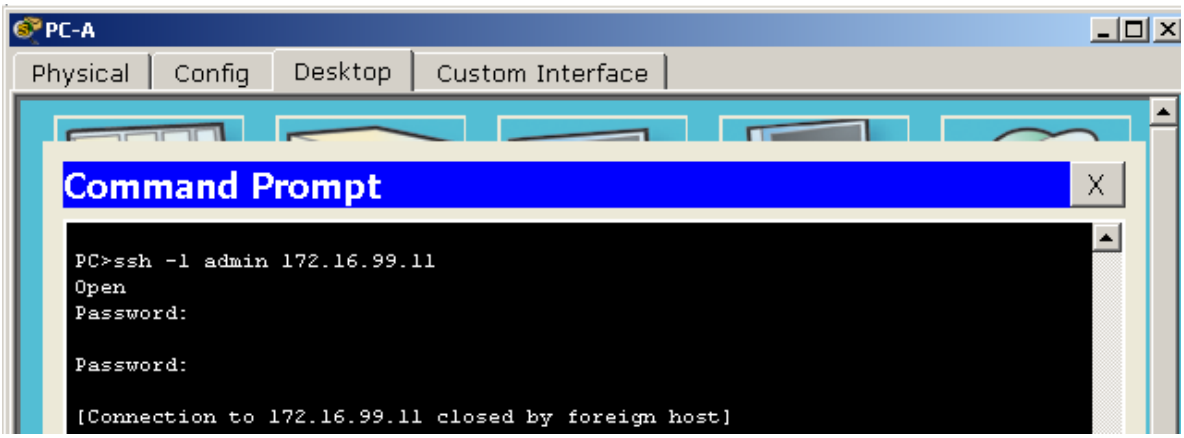
¿Cuántos intentos de autenticación permite SSH? **Ahora permite 2 intentos**

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

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**.

//Se utiliza el comando ssh -l admin 172.16.99.11 para establecer la conexión desde la PC-A//



¿La conexión se realizó correctamente? **R/Si**

¿Qué petición de entrada se mostró en el S1? ¿Por qué? **R/Se solicitó usuario y contraseña para el ingreso, dado que esos parámetros de seguridad se establecieron con anterioridad y constituyen requisitos básicos para la conexión.**

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

Part 8: 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.

```
User Access Verification

Password:
Password:

S1>enable
Password:
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#banner motd #Prohibido el acceso no autorizado#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

R/Están activos los puertos 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#
```

//Realizado//

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#interface range f0/1 - 4
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%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
S1(config-if-range)#
```

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

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES manual administratively down down

FastEthernet0/2        unassigned      YES manual administratively down down

FastEthernet0/3        unassigned      YES manual administratively down down

FastEthernet0/4        unassigned      YES manual administratively down down
```

e. Emita el comando **show ip http server status**. (**Este comando es invalido**)

```
S1#show ip http server status
           ^
% Invalid input detected at '^' marker.
```

¿Cuál es el estado del servidor HTTP?

¿Qué puerto del servidor utiliza?

¿Cuál es el estado del servidor seguro de HTTP?

¿Qué puerto del servidor seguro utiliza?

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

`S1(config)# no ip http server`

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

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

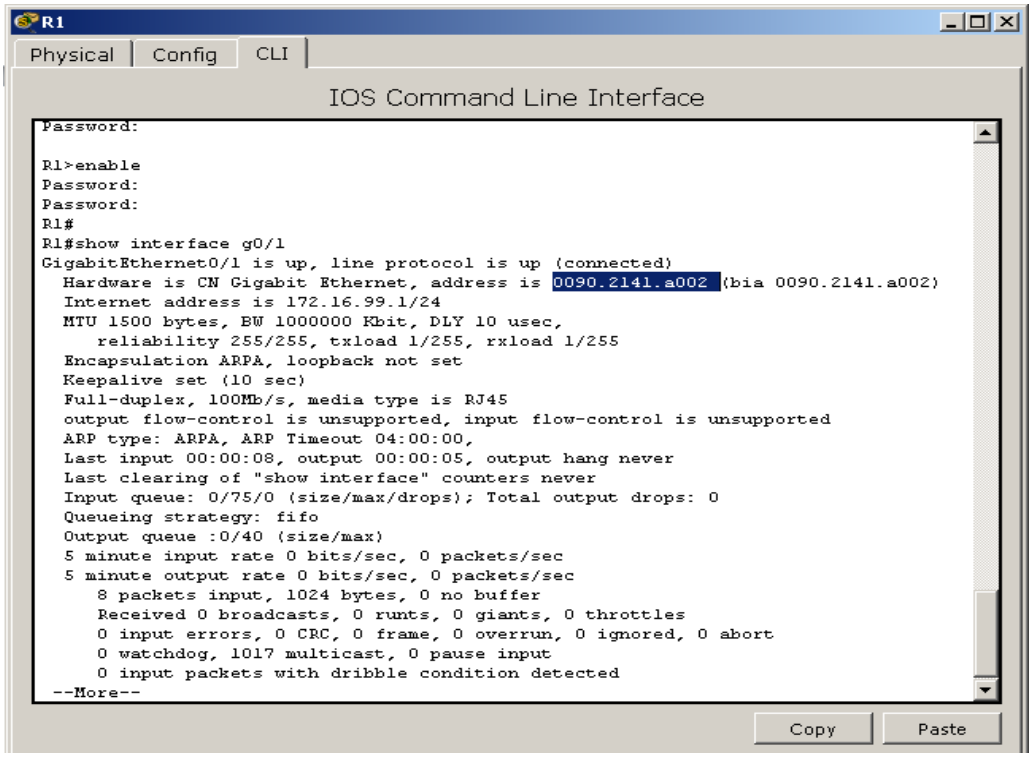
i. Cierre la sesión web en la PC-A.

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

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

`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?

R/ 0090.2141.a002

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.

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

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

  99    0090.2141.a002    DYNAMIC     Fa0/5
  99    00e0.b011.256b    DYNAMIC     Fa0/6
S1#
```

Dirección MAC de F0/5: **Mac Address 0090.2141.a002**

Dirección MAC de F0/6: **Mac Address 00e0.b011.256b**

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.

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

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

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

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

4) Configure una entrada estática para la dirección MAC de la interfaz G0/1 del R1 registrada en el paso 2a. (**0090.2141.a002**)

```
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
```

```
S1(config-if)#switchport port-security mac-address 0090.2141.a002
S1(config-if)#no shutdown

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

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

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

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? **Seguridad activada**

//Realizado//

```
S1#show port-security interface f0/5
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0090.2141.A002:99
Security Violation Count    : 0

S1#
```

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 = 0/0/0 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**

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, no se realiza correctamente**, **dado que al presentarse una violación de la seguridad los puertos se desactivan.**

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
```

//Realizado//

```
Prohibido el acceso no autorizado

User Access Verification

Password:

Sl>enable
Password:
Sl#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/5        1           1                1         Shutdown
---------------------------------------------------------------------
Sl#
```

```
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
```

//Realizado//

```
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#
```

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>
```

//Realizado//

```
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0060.7002.d105 (bia 0060.7002.d105)
 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
  --More--
```

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
```

//Realizado//

```
S1#show port-security address
                                  Secure Mac Address Table
------------------------------------------------------------------------------
Vlan       Mac Address Type                              Ports
Remaining Age

(mins)
----       -----------  ----                             -----
-------------
99         0090.2141.A002         SecureConfigured       FastEthernet0/5
-
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#
```

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.**

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

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.

//Realizado//

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

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
S1(config-if)#
S1(config-if)#no shutdown

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

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

S1(config-if)#
```

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
```

//Realizado//

```
S1#show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.7002.d105 (bia 0060.7002.d105)
 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
```

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

```
R1#ping 172.16.99.3

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

R1#
```

Reflexión

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

   Para garantizar parámetros de seguridad en los cuales se especifique que cierta cantidad de pc tengan acceso a ese Puerto y que dado el caso en que se infrinja la norma estos se deshabiliten automáticamente.

2. **¿Por qué deben deshabilitarse los puertos no utilizados en un switch? Porque evitar que usuarios no autorizados tengan acceso a nuestros recursos de red.**

Tabla de resumen de interfaces del router

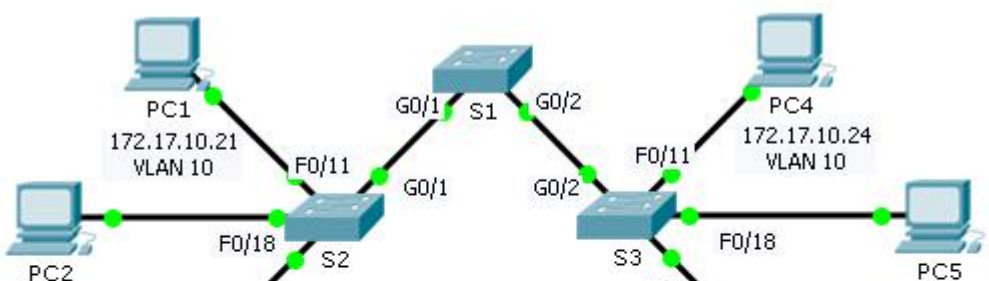
Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet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

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

3.2.1.7 Packet Tracer - Configuring VLANs.

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

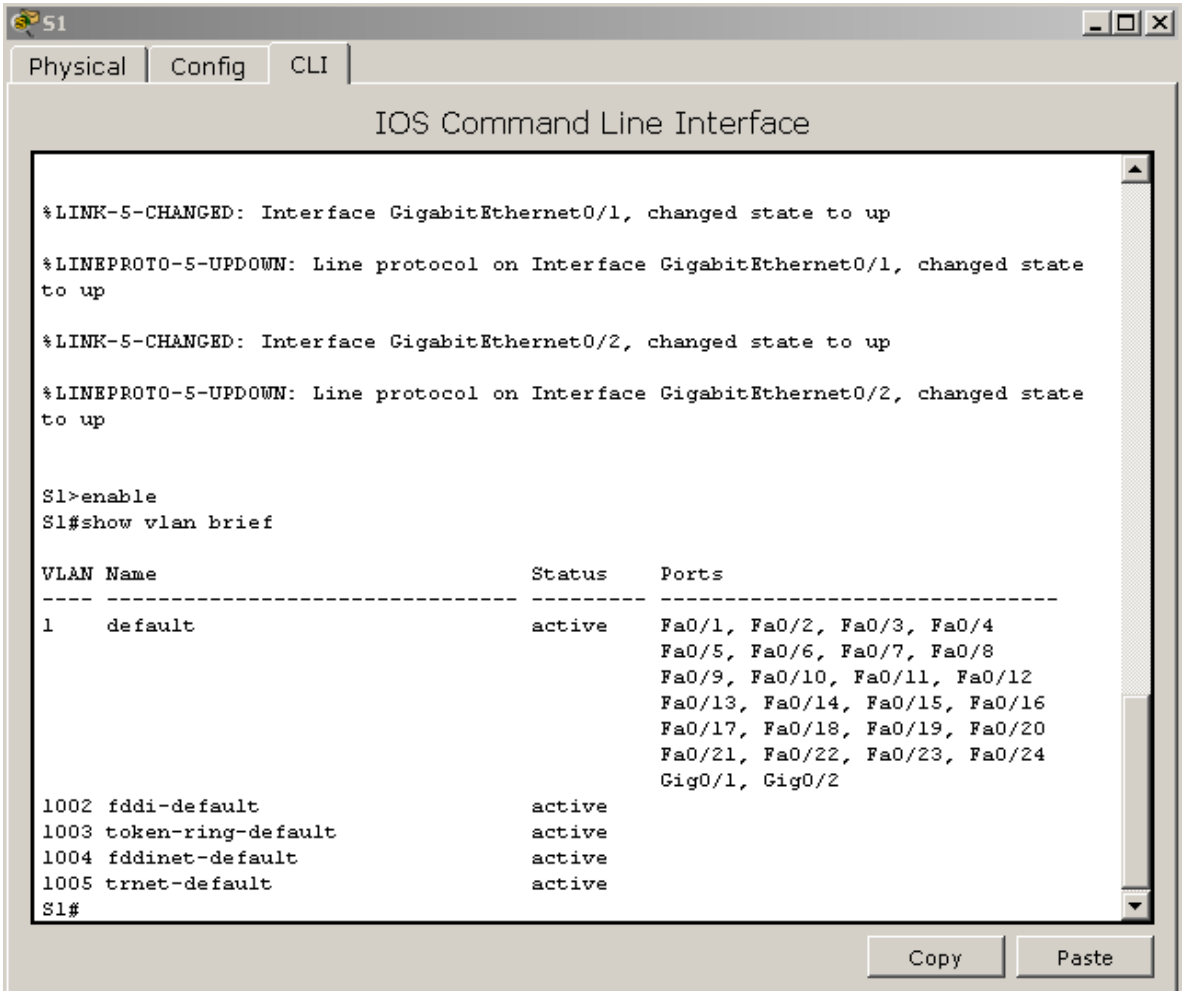
Background

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.

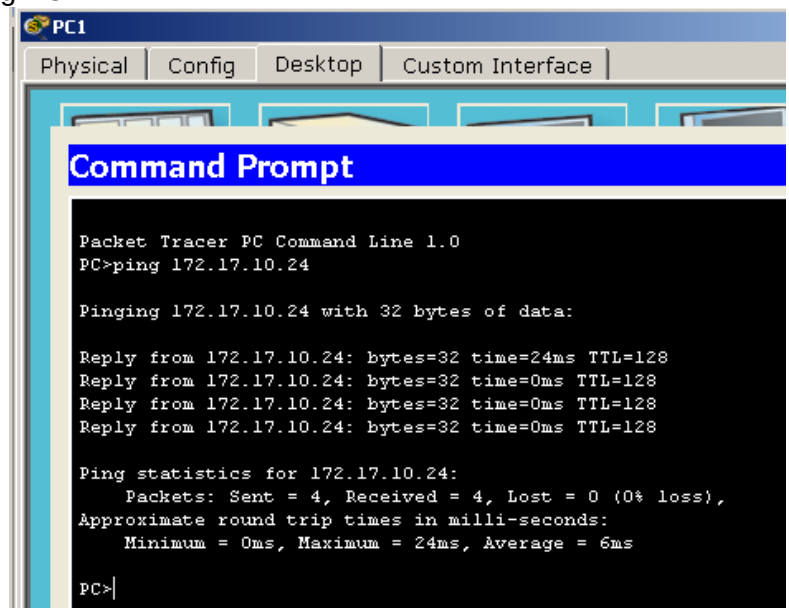
On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.



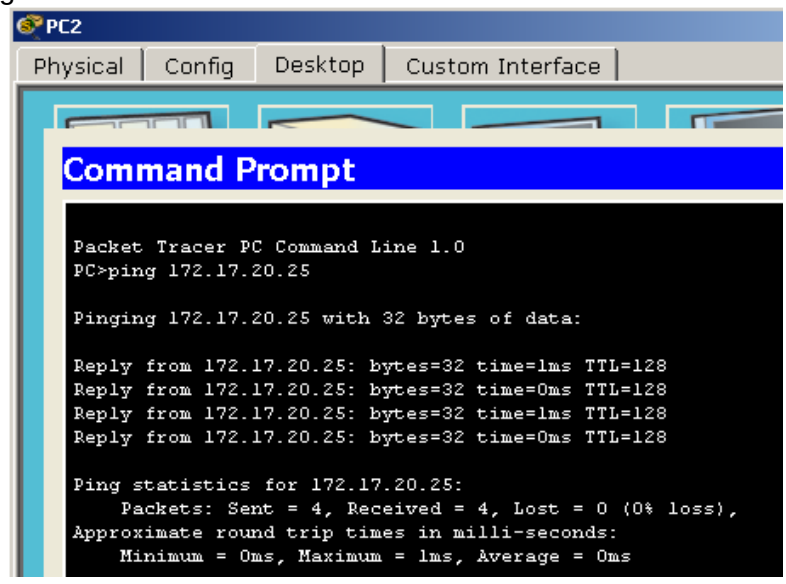
Step 2: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network.

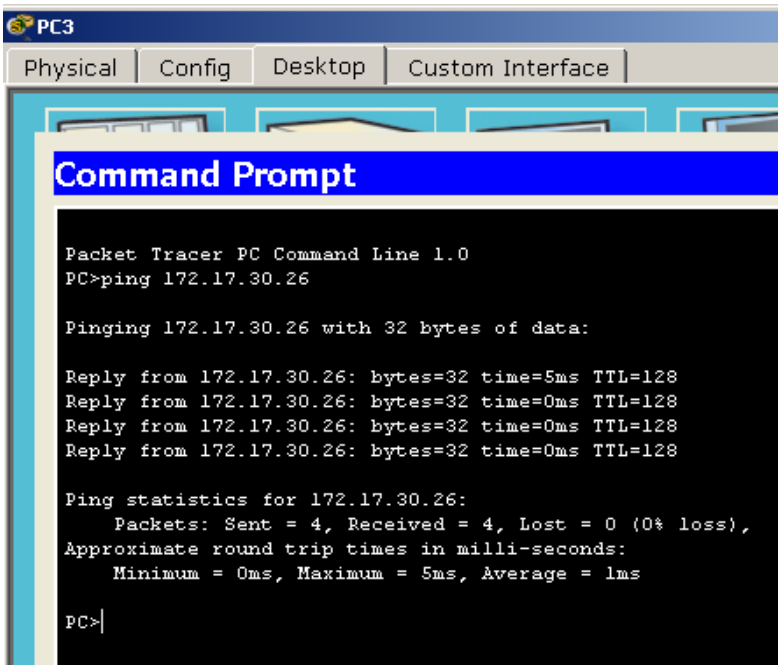
χ PC1 can ping PC4



δ PC2 can ping PC5



ε PC3 can ping PC6



Pings to PCs in other networks fail. **Si son de diferentes redes no se pueden comunicar**.

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.

Los principales beneficios del uso de VLAN son los siguientes: seguridad, reducción de costos, mayor rendimiento, mitigación de tormentas de difusión, mejor eficiencia del personal de TI y administración más simple de proyectos y aplicaciones.

Part 2: Configure VLANs

Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

δ. VLAN 10: Faculty/Staff

ε. VLAN 20: Students

ϕ. VLAN 30: Guest(Default)

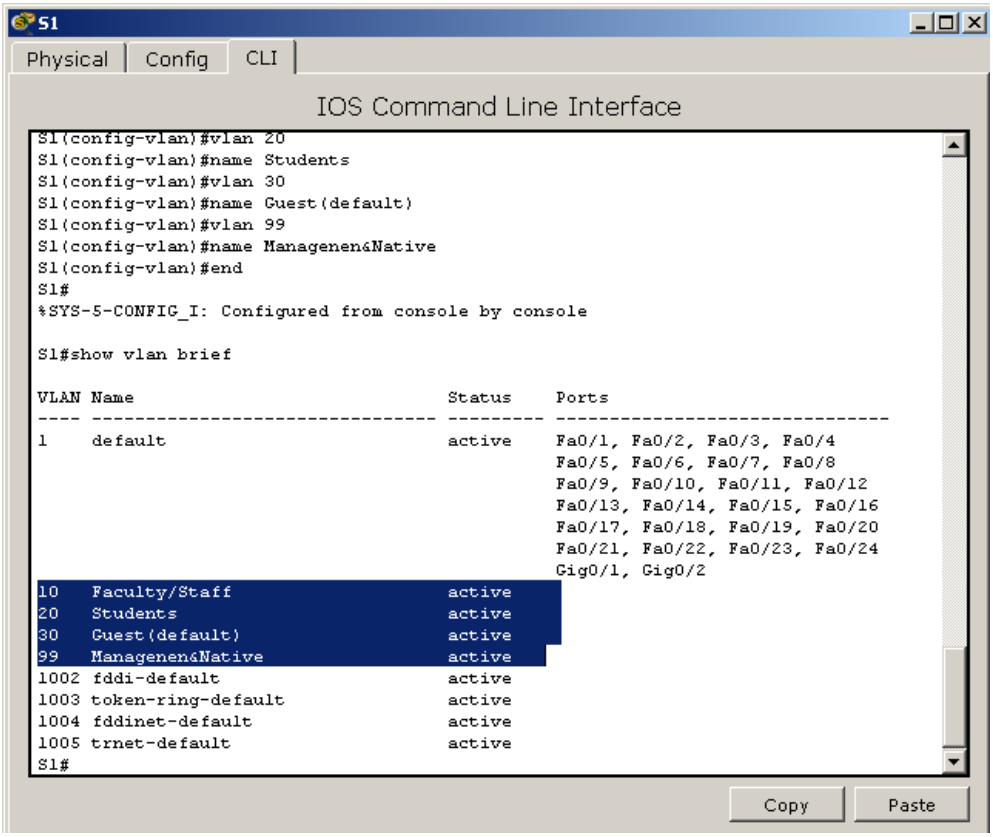
γ. VLAN 99: Management&Native

```
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
anagement&Native
```

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest(default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Managenen&Native
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 2: Verify the VLAN configuration.

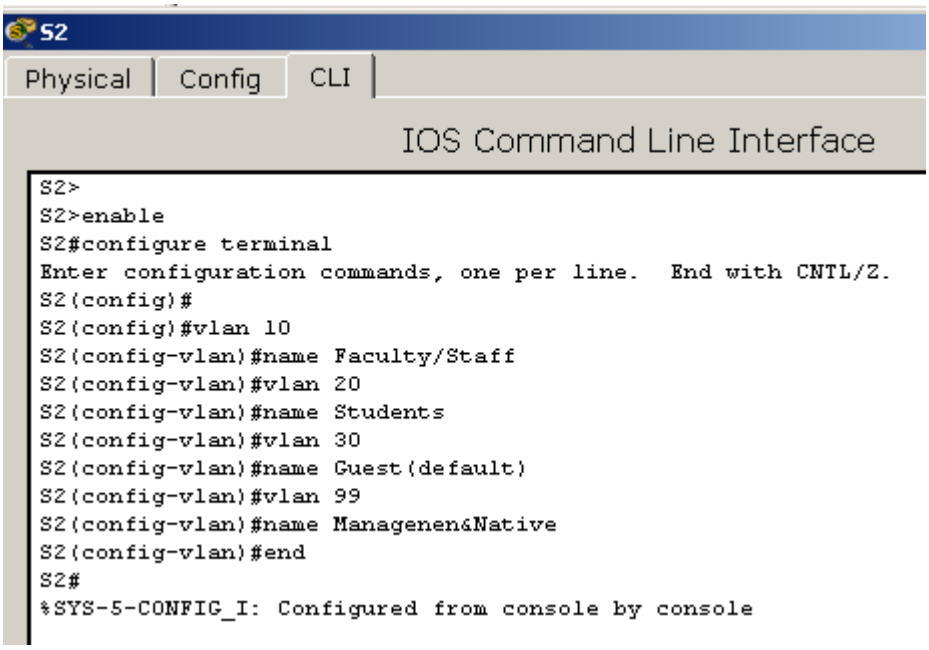
Which command will only display the VLAN name, status, and associated ports on a switch? `S1# show vlan brief`



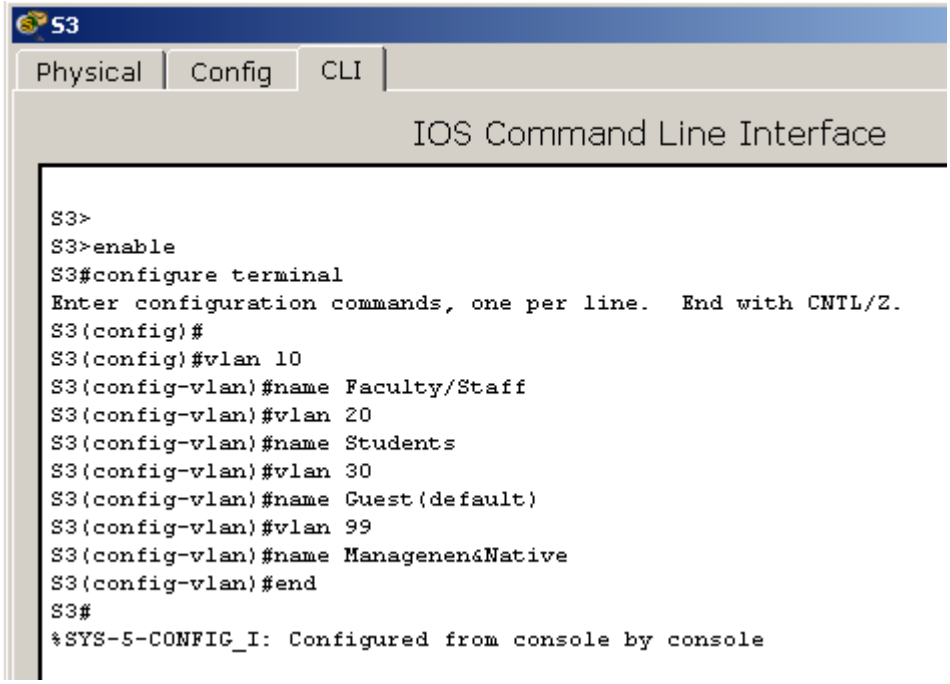
Step 3: Create the VLANs on S2 and S3.

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

//Configuración el S2//



//Configuración el S3//



Step 4: Verify the VLAN configuration.

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(default)                    active
99   Managenen&Native                  active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
```

```
S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(default)                    active
99   Managenen&Native                  active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S3#
```

Part 3: Assign VLANs to Ports

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

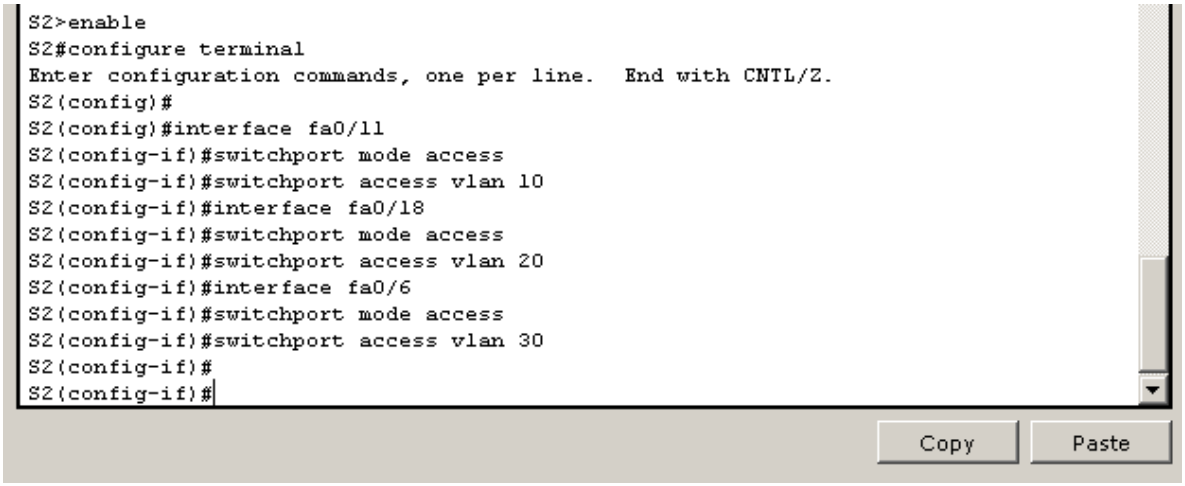
Assign the VLANs to the following ports:

λ. VLAN 10: Fast Ethernet 0/11

μ. VLAN 20: Fast Ethernet 0/18

v. VLAN 30: Fast Ethernet 0/6

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

S2(config-if)#  switchport  mode
access

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.

```
S3>
S3>enable
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#
S3(config)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
S3(config-if)#
S3(config-if)#
```

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. **No, los pings fallaron porque los puertos entre los switches están en VLAN 1 y PC1 y PC4 petenecen a la VLAN 10.**

What could be done to resolve this issue? Configure the ports between the switches as trunk ports.

//Necesitamos configurar los puertos como troncales//

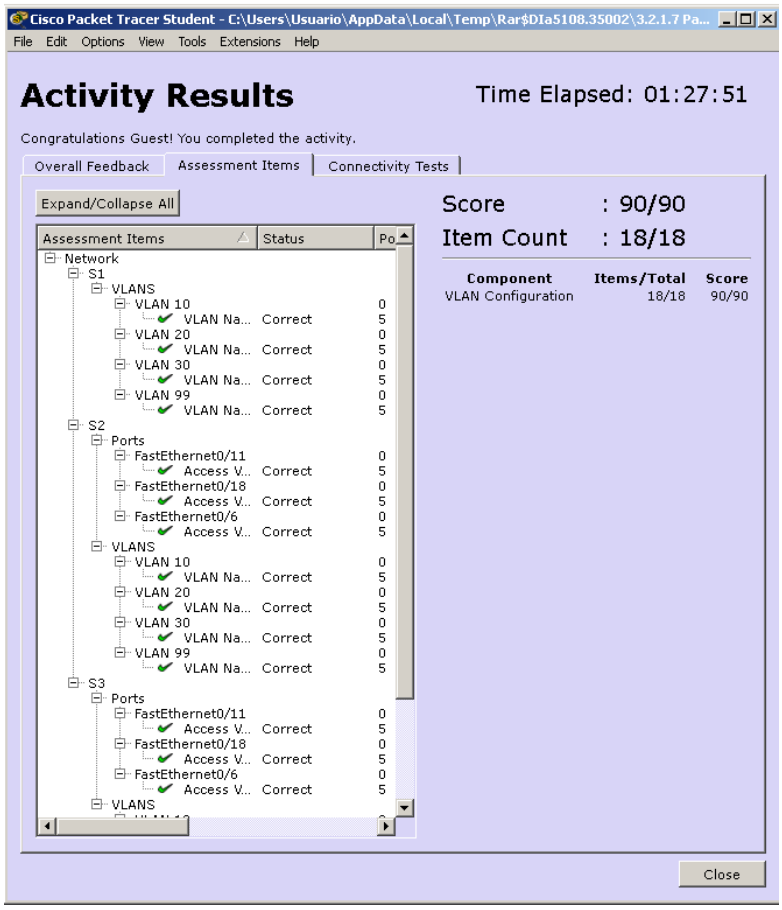
```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface g0/1
S1(config-if)#switchport mode trunk
S1(config-if)#interface g0/2
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state
to up

S1(config-if)#
```

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface g0/1
S2(config-if)#switchport mode trunk

S2(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

S2(config-if)#
```

```
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#
S3(config)#interface g0/2
S3(config-if)#switchport mode trunk
S3(config-if)#exit
S3(config)#
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

//Ahora verificamos con ping nuevamente y se evidencia la comunicación entro los host//

```
Pinging 172.17.10.24 with 32 bytes of data:

Reply from 172.17.10.24: bytes=32 time=0ms TTL=128
Reply from 172.17.10.24: bytes=32 time=1ms TTL=128
Reply from 172.17.10.24: bytes=32 time=0ms TTL=128
Reply from 172.17.10.24: bytes=32 time=0ms TTL=128

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```



3.2.2.4 Packet Tracer - Configuring Trunks.

Packet Tracer: configuración de enlaces troncales

Topología

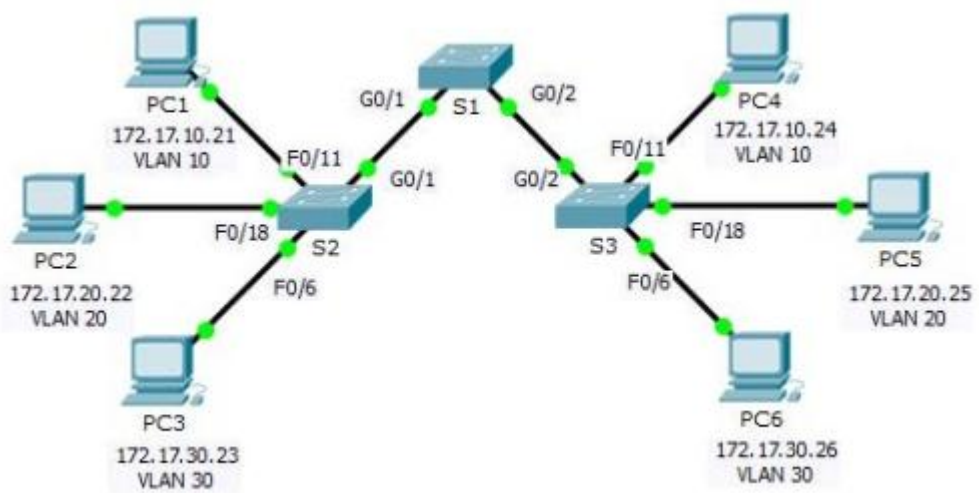


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerto del switch	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S1 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S1 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S1 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S2 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S2 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S2 F0/6	30

Objetivos

Parte 1: verificar las VLAN

Parte 2: configurar enlaces troncales

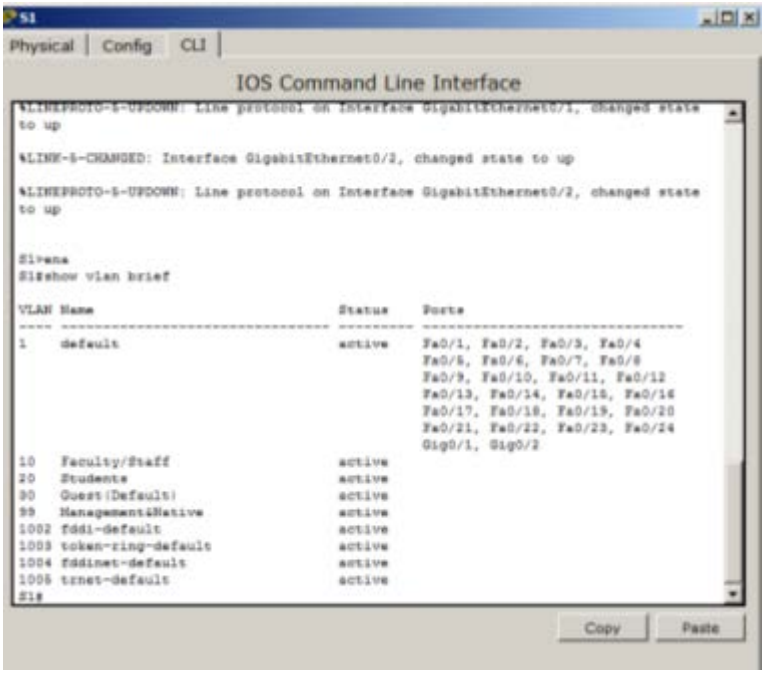
Información básica

Se requieren enlaces troncales para transmitir información de VLAN entre switches. Un puerto de un switch es un puerto de acceso o un puerto de enlace troncal. Los puertos de acceso transportan el tráfico de una VLAN específica asignada al puerto. Un puerto de enlace troncal pertenece a todas las VLAN de manera predeterminada; por lo tanto, transporta el tráfico para todas las VLAN. Esta actividad se centra en la creación de puertos de enlace troncal y en la asignación a una VLAN nativa distinta de la predeterminada.

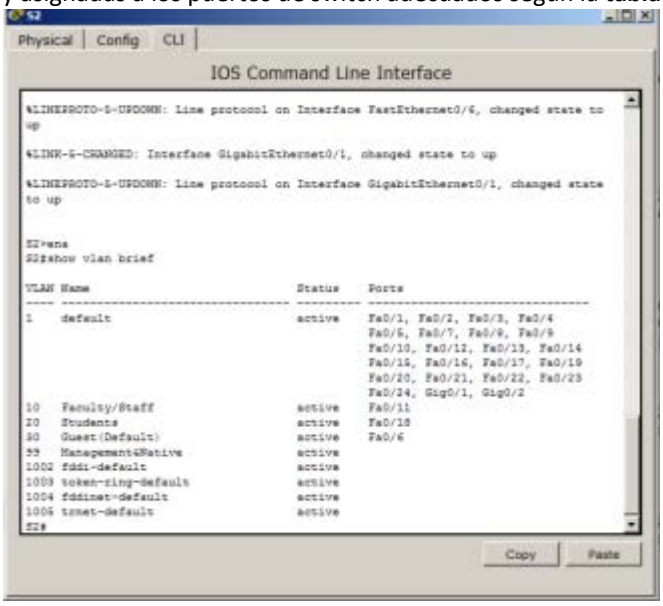
Parte 1: verificar las VLAN

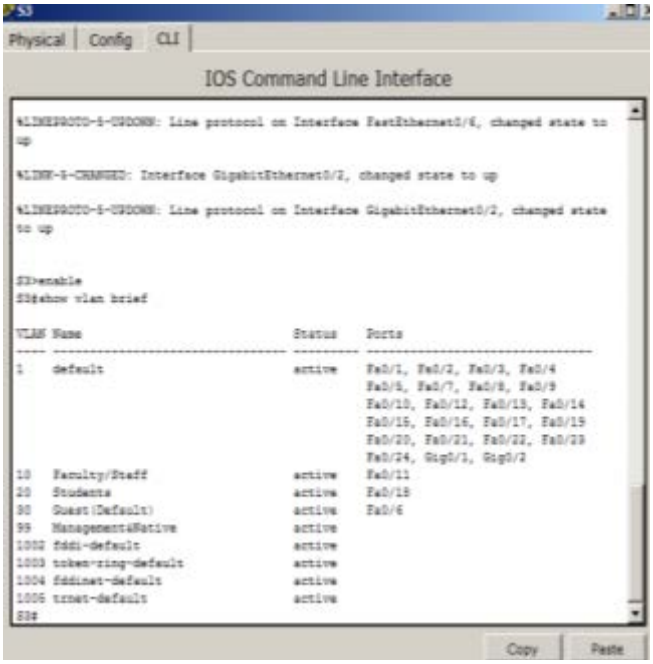
Paso 1: mostrar las VLAN actuales.

a. En el **S1**, emita el comando que muestra todas las VLAN configuradas.Debe haber nueve VLAN en total. Observe de qué manera los 26 puertos del switch se asignan a un puerto o a otro.



b. En el **S2** y el **S3**, muestre la información y verifique que todas las VLAN estén configuradas y asignadas a los puertos de switch adecuados según la **tabla de direccionamiento**.





Paso 2: verificar la pérdida de conectividad entre dos computadoras en la misma red.

Aunque la **PC1** y la **PC4** estén en la misma red, no pueden hacer ping entre sí. Esto es porque los puertos que conectan los switches se asignaron a la VLAN 1 de manera predeterminada. Para proporcionar conectividad entre las computadoras en la misma red y VLAN, se deben configurar enlaces troncales.

Parte 2: configurar los enlaces troncales

Paso 1: configurar el enlace troncal en el S1 y utilizar la VLAN 99 como VLAN nativa.

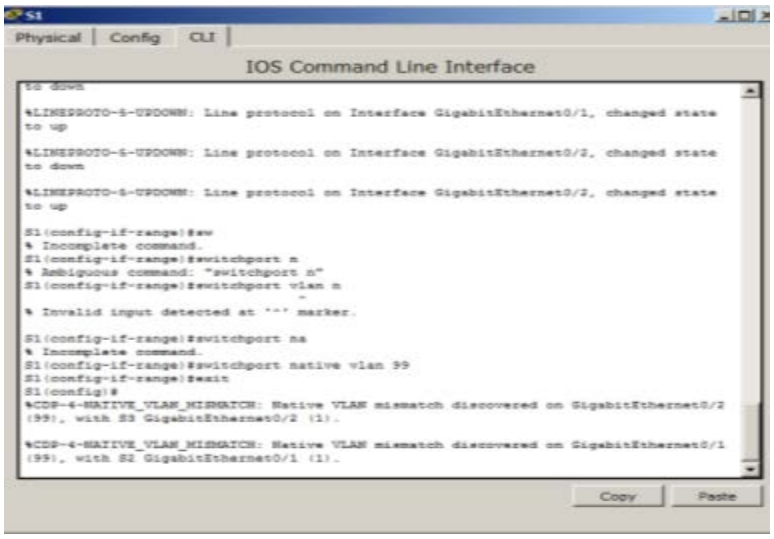
a. Configure las interfaces G0/1 y G0/2 en el S1 para el uso de enlaces troncales.

b. Configure la VLAN 99 como VLAN nativa para las interfaces G0/1 y G0/2 en el **S1**.

El puerto de enlace troncal demora aproximadamente un minuto en activarse debido al árbol de expansión, sobre lo que aprenderá en los próximos capítulos. Haga clic en **Fast Forward Time (Adelantar el tiempo)** para acelerar el proceso. Una vez que los puertos se activan, recibirá de forma periódica los siguientes mensajes de syslog:

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

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

Configuró la VLAN 99 como VLAN nativa en el S1. Sin embargo, y según lo indicado por el mensaje de syslog, el S2 y el S3 utilizan la VLAN 1 como VLAN nativa predeterminada.

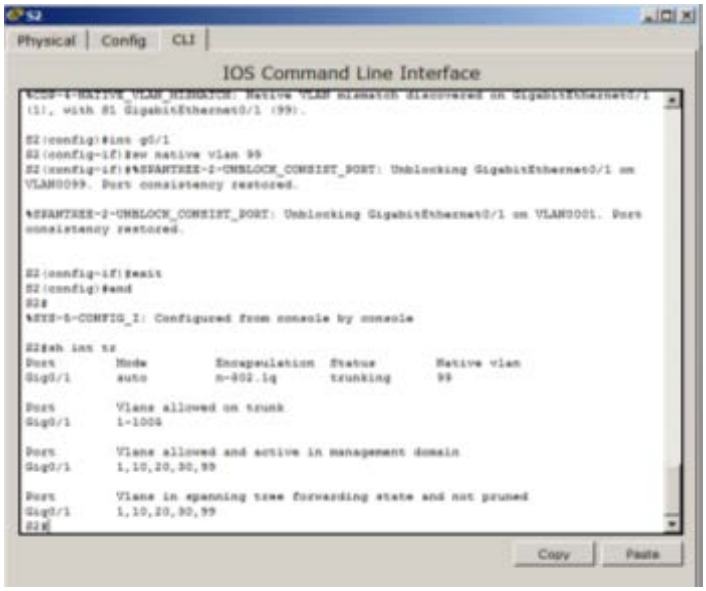


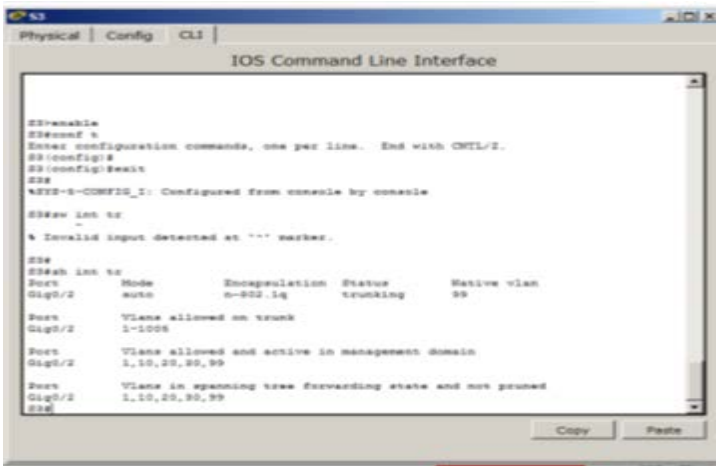
Si bien hay una incompatibilidad de VLAN nativa, los pings entre las computadoras de la misma VLAN ahora se realizan de forma correcta. ¿Por qué?

- Se ha habilitado en S1. El protocolo de enlace dinámico (DTP) ha negociado automáticamente el otro lado de los enlaces troncales.

Paso 2: verificar que el enlace troncal esté habilitado en el S2 y el S3.

En el **S2** y el **S3**, emita el comando **show interface trunk** para confirmar que el DTP haya negociado de forma correcta el enlace troncal con el S1 en el S2 y el S3. El resultado también muestra información sobre las interfaces troncales en el S2 y el S3.





¿Qué VLAN activas se permiten a través del enlace troncal?

Paso 3: corregir la incompatibilidad de VLAN nativa en el S2 y el S3.

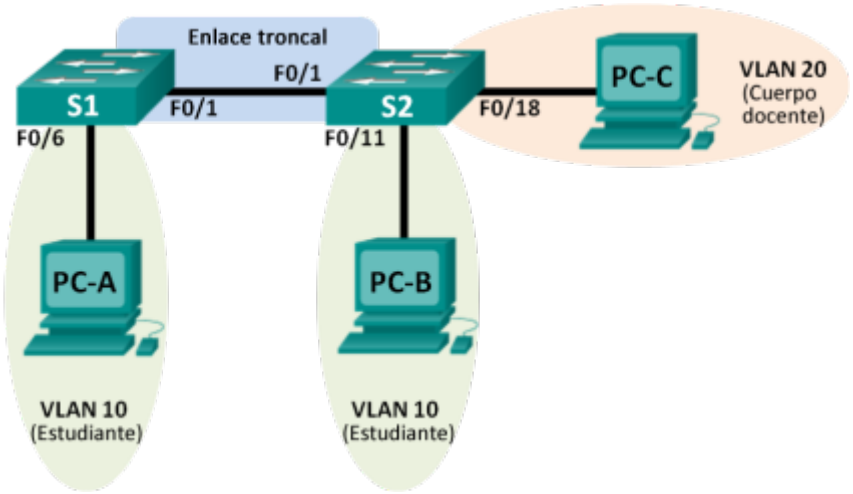
a. Configure la VLAN 99 como VLAN nativa para las interfaces apropiadas en el S2 y el S3.

b. Emita el comando **show interface trunk** para verificar que la configuración de la VLAN sea correcta.

3.2.2.5 Lab - Configuring VLANs and Trunking

Práctica de laboratorio: configuración de redes VLAN y enlaces troncales

Topología



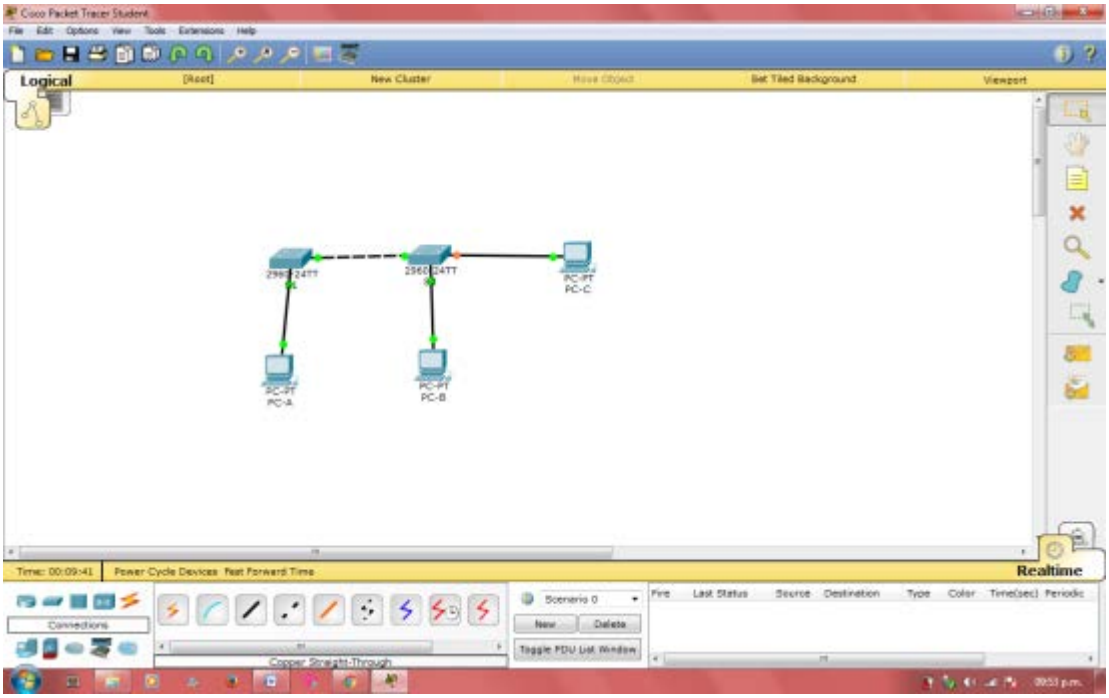


Tabla de direccionamiento

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

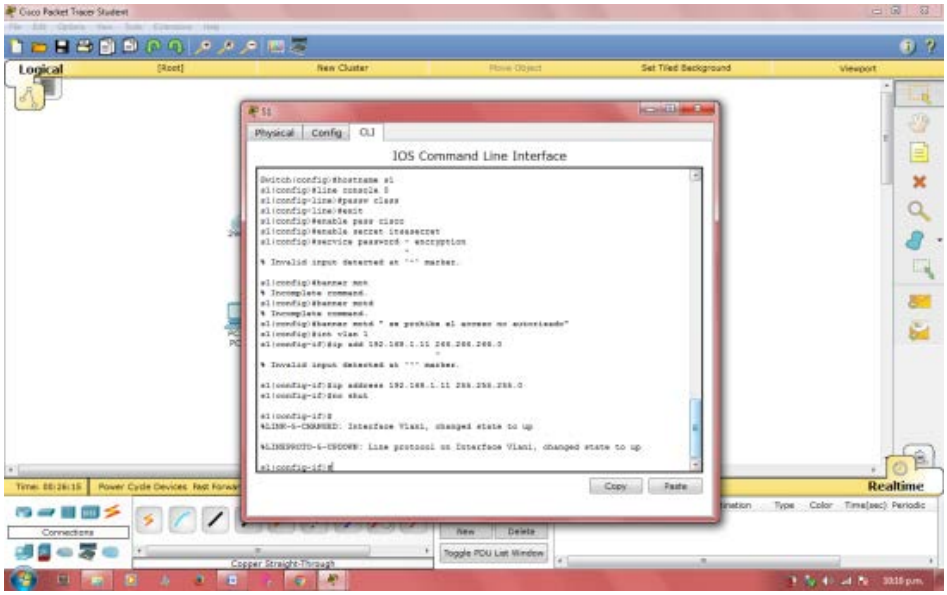
Part 9: armar la red y configurar los parámetros básicos de los dispositivos

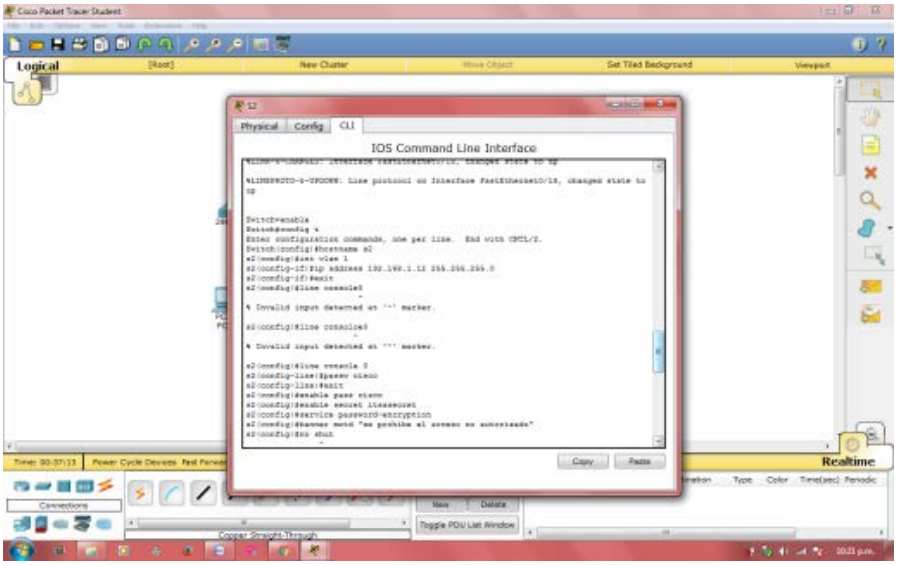
En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

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

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

Step 2: 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.

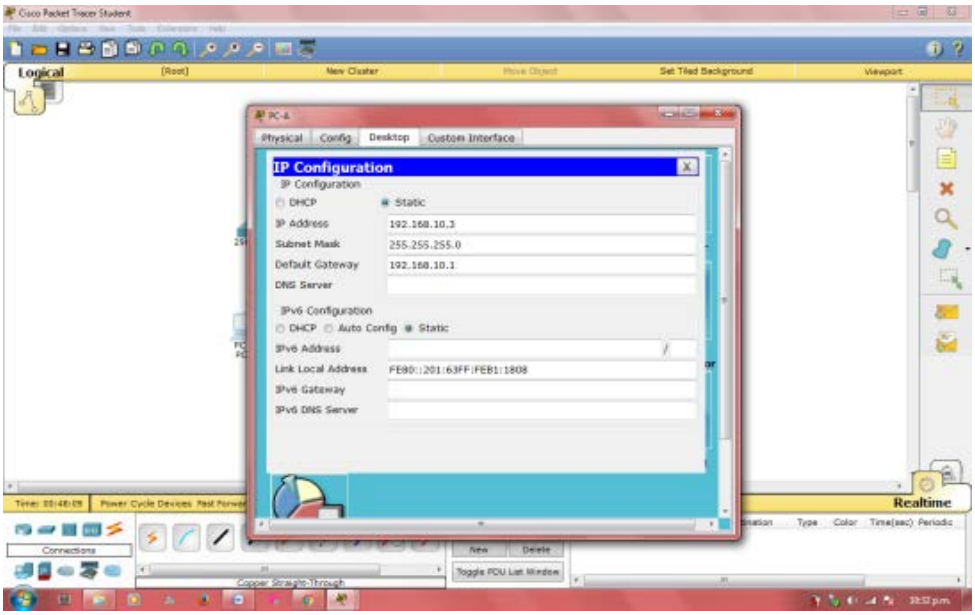
g. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

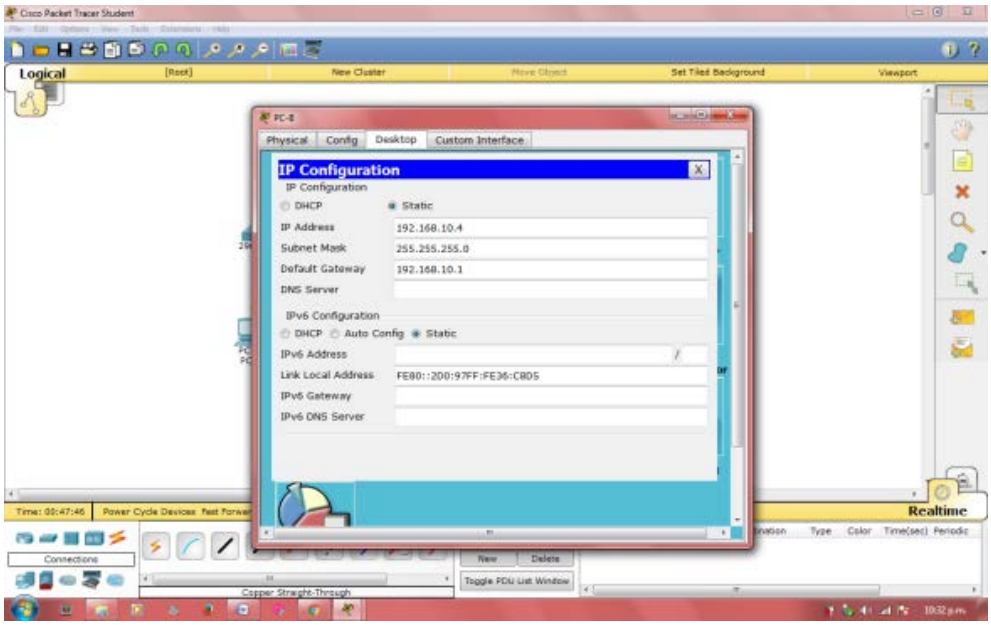
h. Desactive administrativamente todos los puertos que no se usen en el switch.

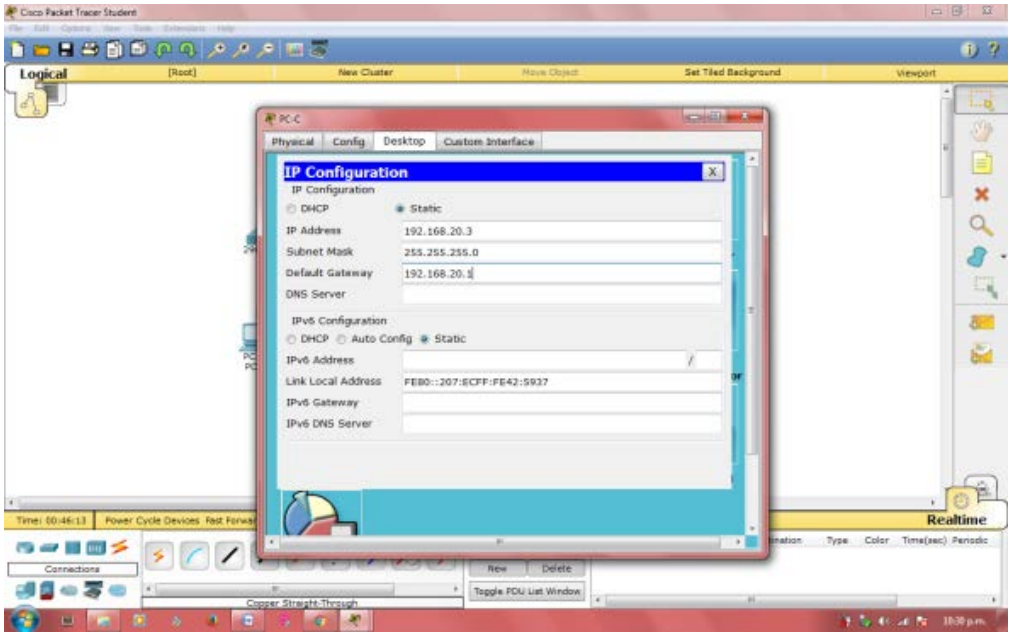
i. Copie la configuración en ejecución en la configuración de inicio

Step 3: configurar los equipos host.

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





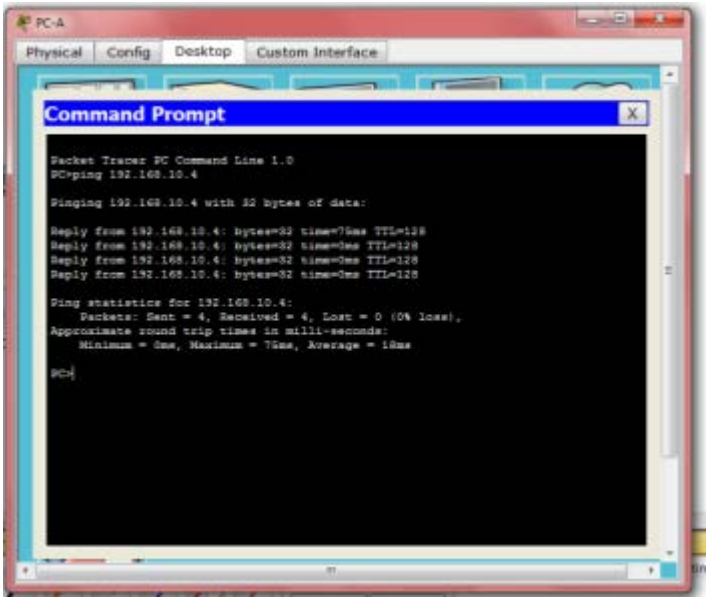


Step 4: Probar la conectividad.

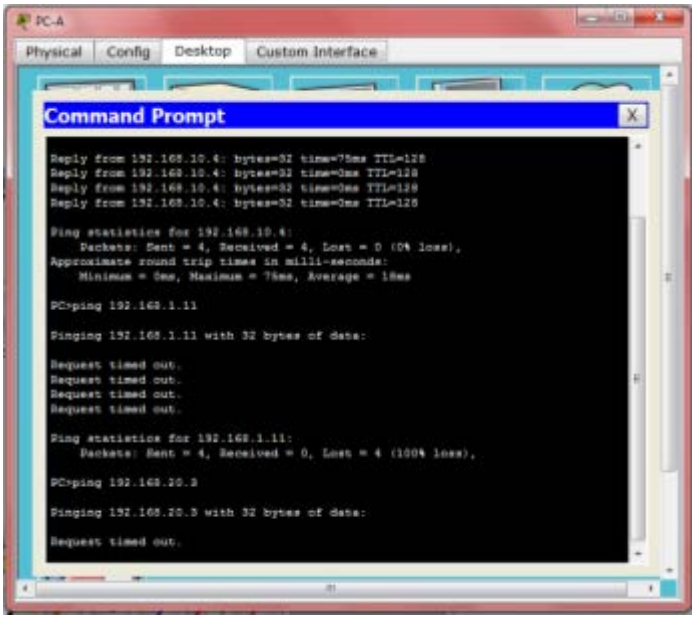
Verifique que los equipos host puedan hacer ping entre sí.

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

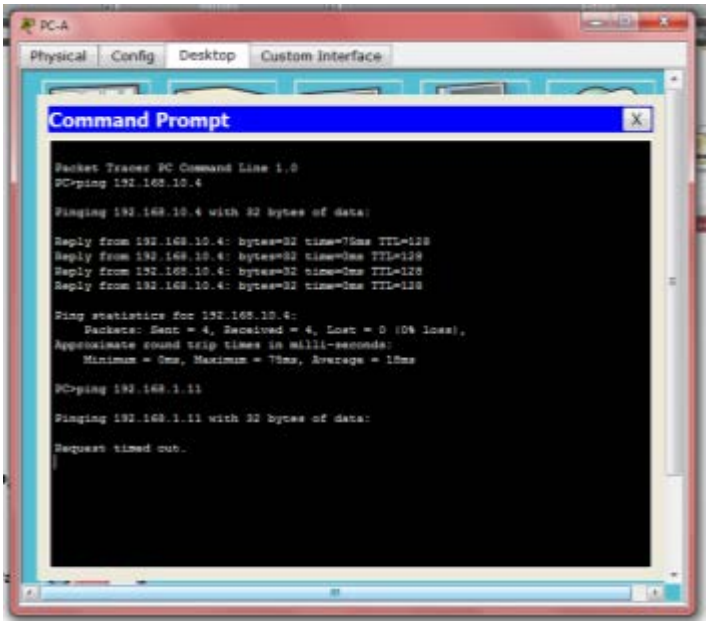
¿Se puede hacer ping de la PC-A a la PC-B? _____ si



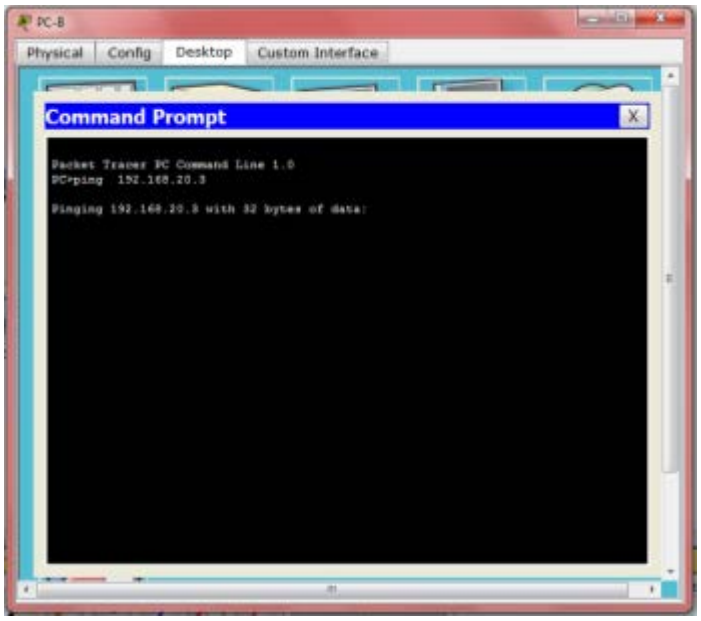
¿Se puede hacer ping de la PC-A a la PC-C? _____ NO



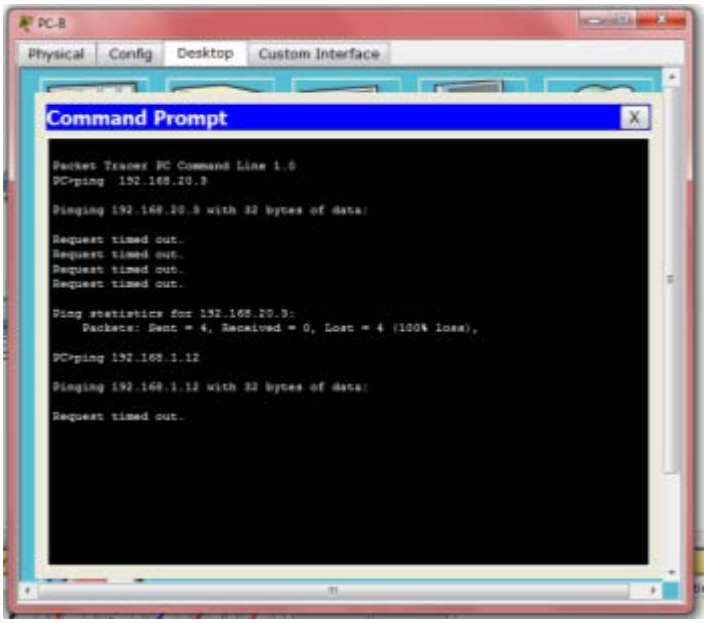
¿Se puede hacer ping de la PC-A al S1? _____ NO



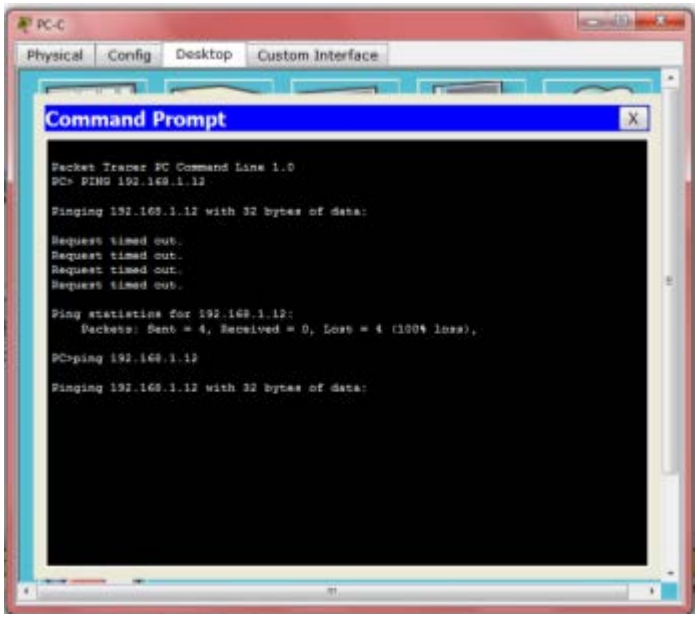
¿Se puede hacer ping de la PC-B a la PC-C? _____ NO



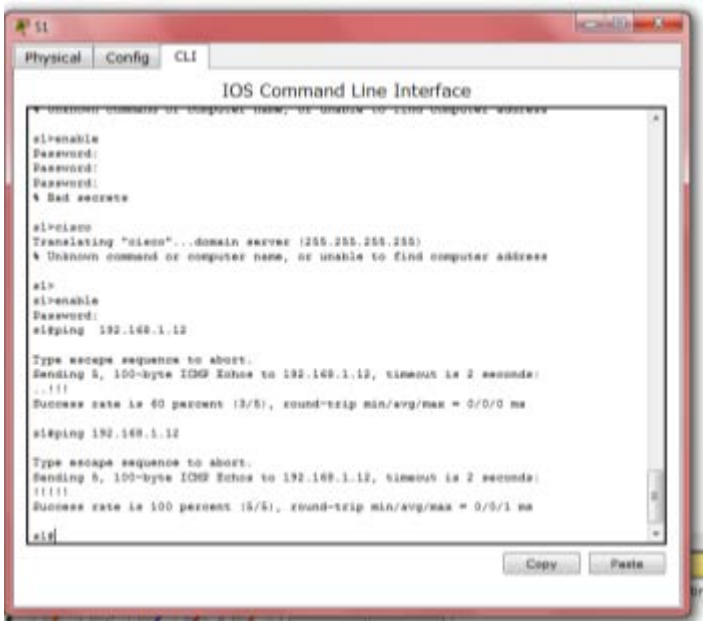
¿Se puede hacer ping de la PC-B al S2? _____ NO



¿Se puede hacer ping de la PC-C al S2? _____ NO



¿Se puede hacer ping del S1 al S2? _____ SI



Si la respuesta a cualquiera de las preguntas anteriores es no, ¿por qué fallaron los pings?

Los pings fallaron cuando se intentó hacer ping a un dispositivo en una subred diferente. Para que esos pings se realicen correctamente, debe existir un gateway predeterminado para enrutar el tráfico de una subred a otra.

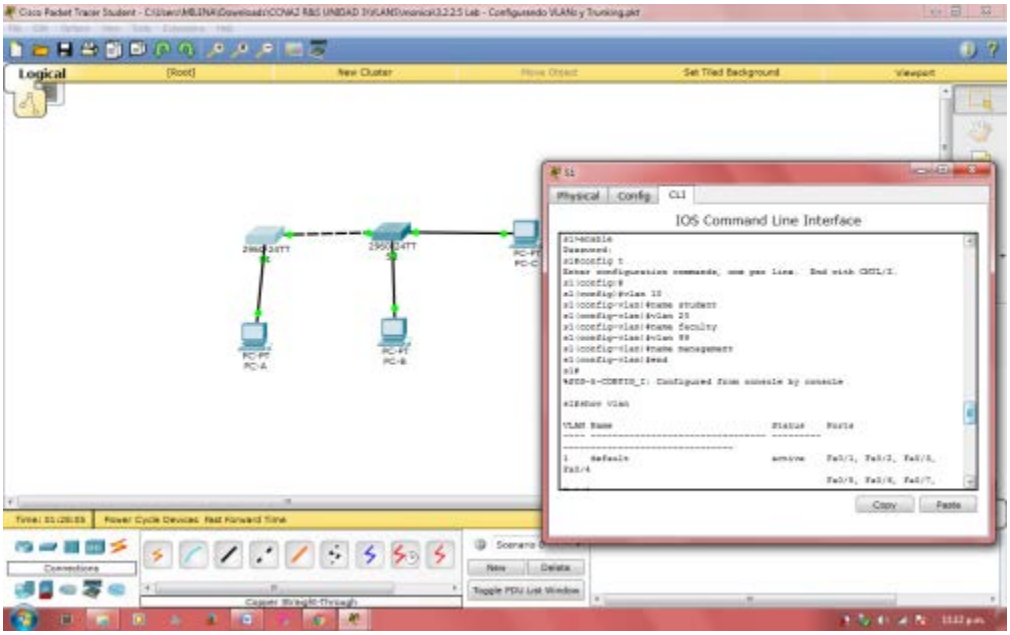
Part 10: crear redes VLAN y asignar puertos de switch

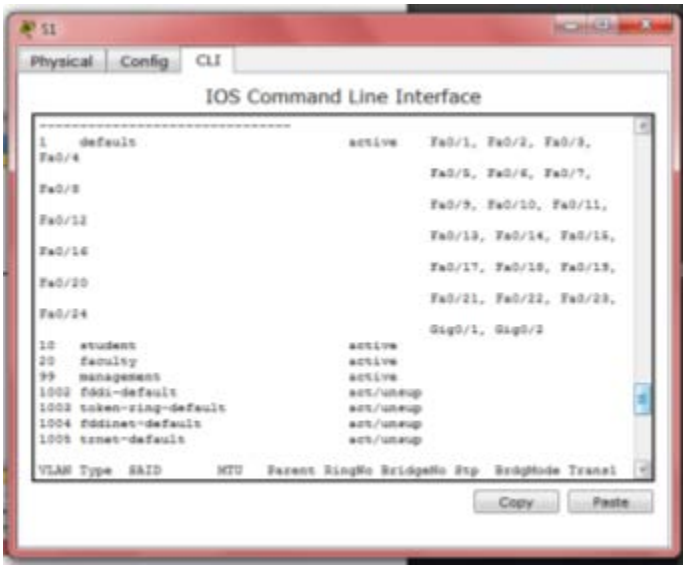
En la parte 2, creará redes VLAN para los estudiantes, el cuerpo docente y la administración en ambos switches. A continuación, asignará las VLAN a la interfaz correspondiente. El comando **show vlan** se usa para verificar las opciones de configuración.

Step 1: crear las VLAN en los switches.

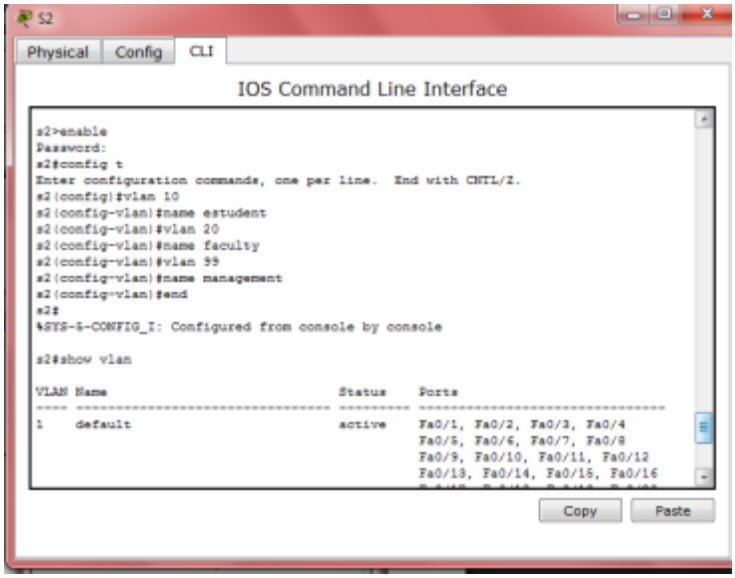
a. Cree las VLAN en S1.

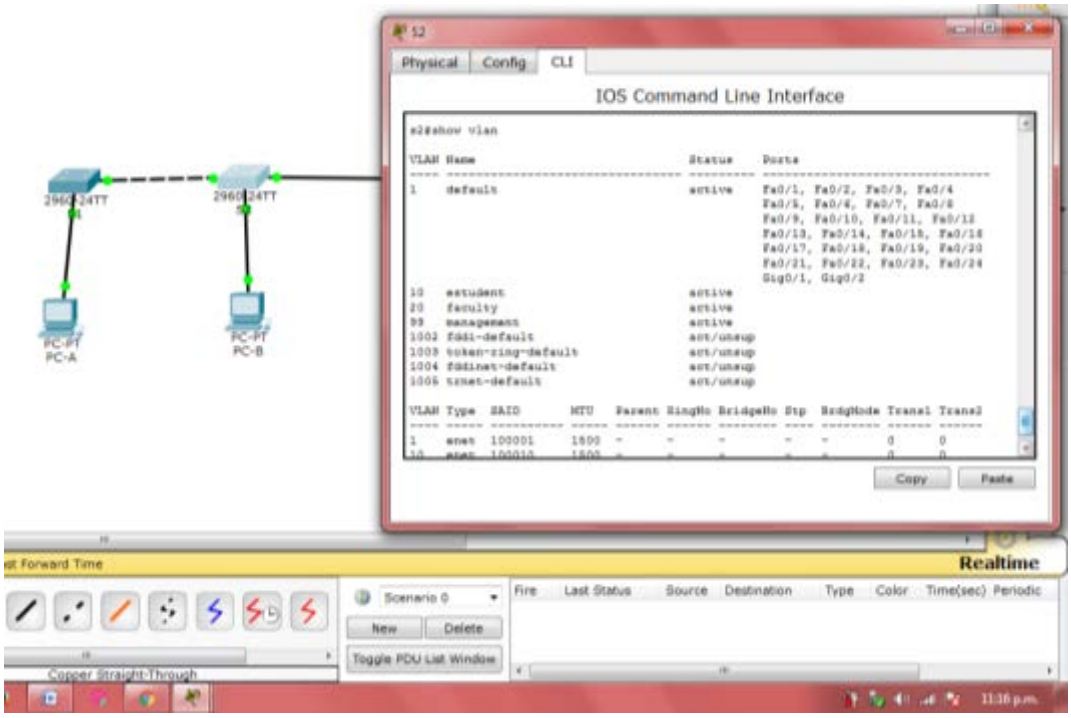
```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```





b. Cree las mismas VLAN en el S2.



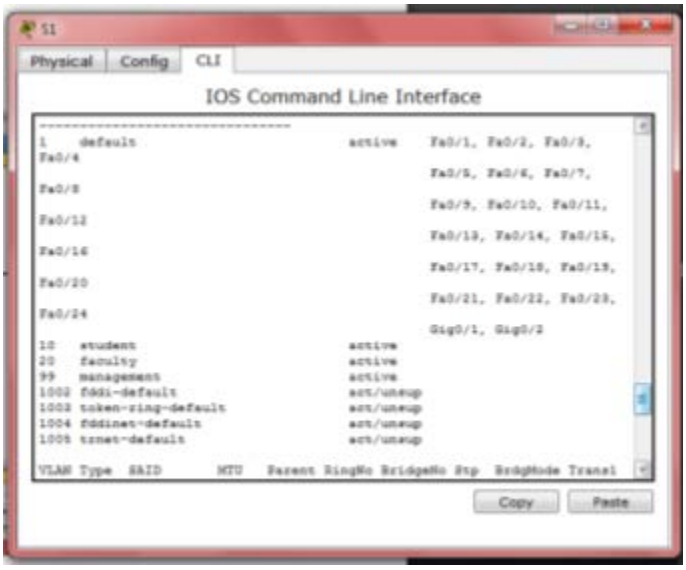


c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.

S1# **show vlan**

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

```
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gi0/1, Gi0/2
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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -----
-
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
------- --------- ----------------- ------------------------------------------
-
```



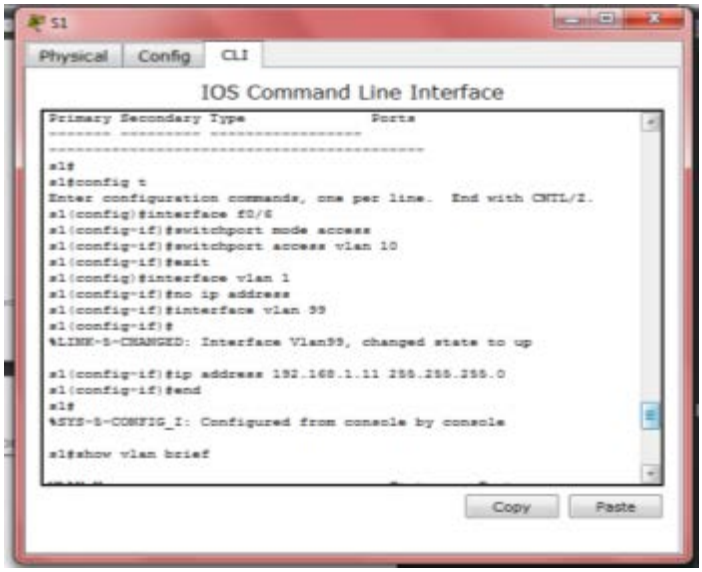
¿Cuál es la VLAN predeterminada? _____ LA VLAN 1

¿Qué puertos se asignan a la VLAN predeterminada?

Todos los puertos del switch se asignan a la VLAN 1 de manera predeterminada.

asignar las VLAN a las interfaces del switch correctas.

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



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

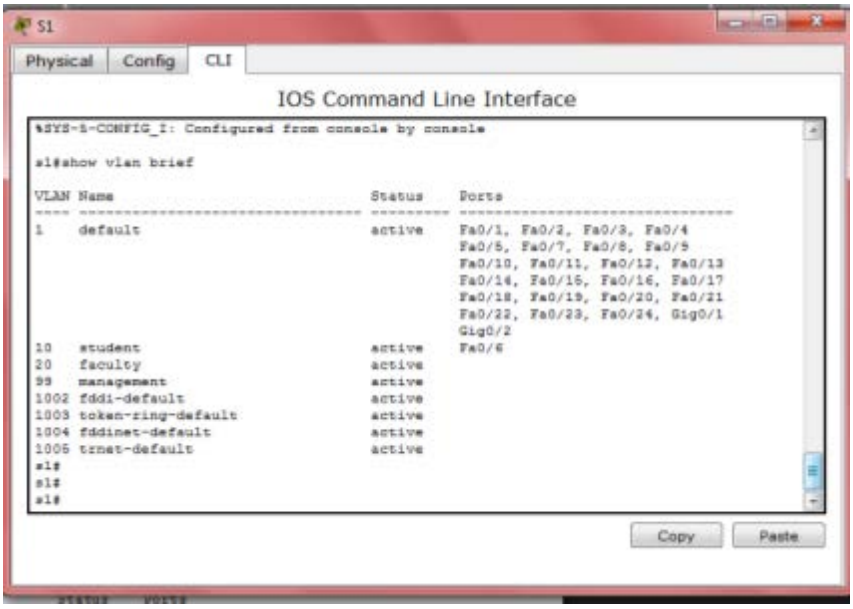
```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

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
```

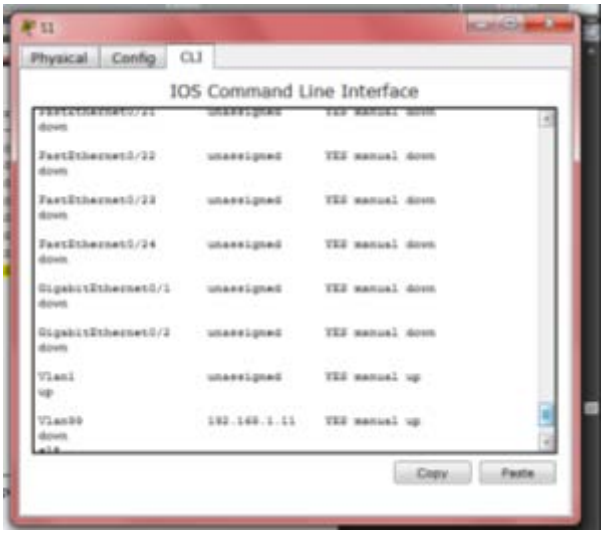
e. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
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, Gi0/1
                                                 Gi0/2
10   Student                           active    Fa0/6
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
```

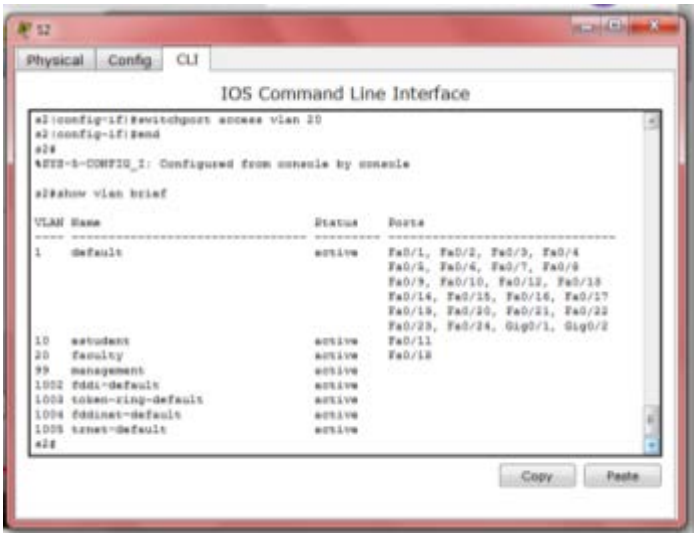
f. Emita el comando **show ip interface brief**.



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

El estado de la VLAN 99 es up/Down, porque todavía no se asignó a ningún puerto activo

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



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

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

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

```
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, Gi0/1, Gi0/2
10   Student                          active    Fa0/11
20   Faculty                          active    Fa0/18
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

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

No. La interfaz F0/1 no se asignó a la VLAN 10, de modo que el tráfico de la VLAN 10 no se envía a través de esta interfaz

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

No. Las direcciones IP de los switches ahora residen en la VLAN 99. El tráfico de la VLAN 99 no se envía a través de la interfaz F0/1

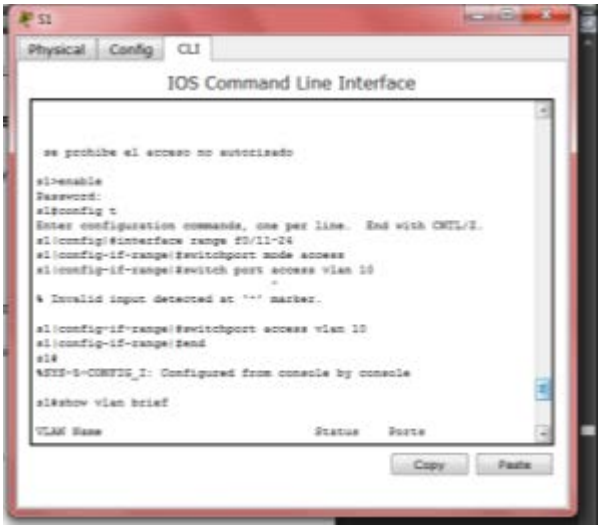
Part 11: mantener las asignaciones de puertos de VLAN y la base de datos de VLAN

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

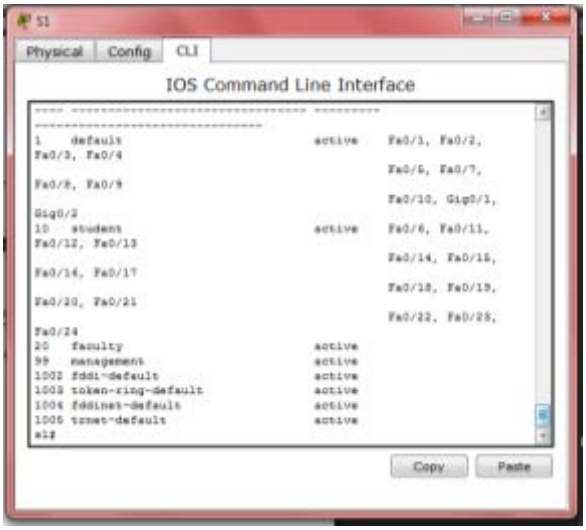
Step 1: asignar una VLAN a varias interfaces.

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

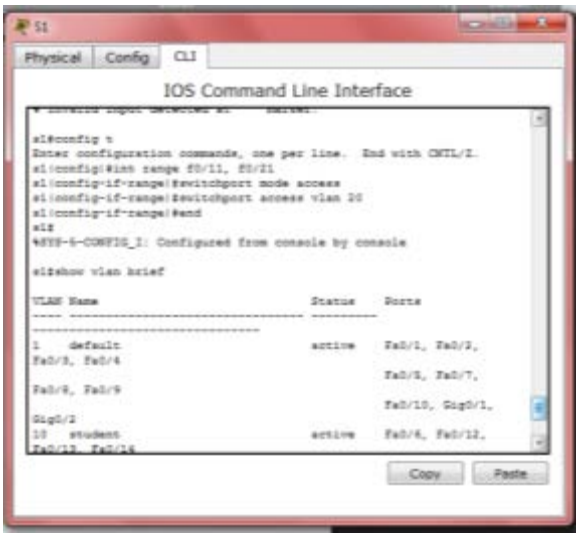
```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```



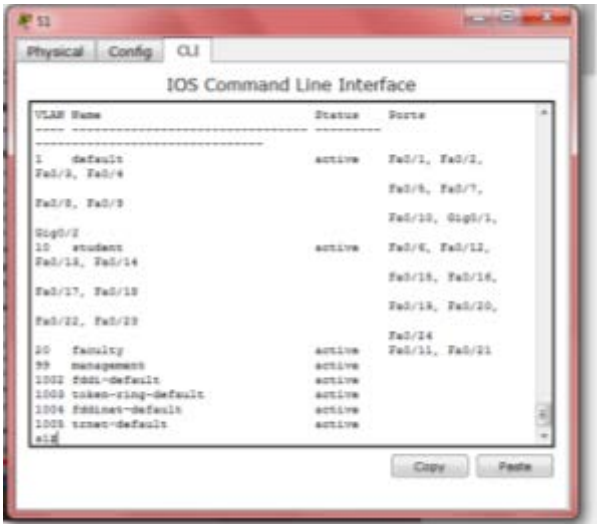
b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.



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



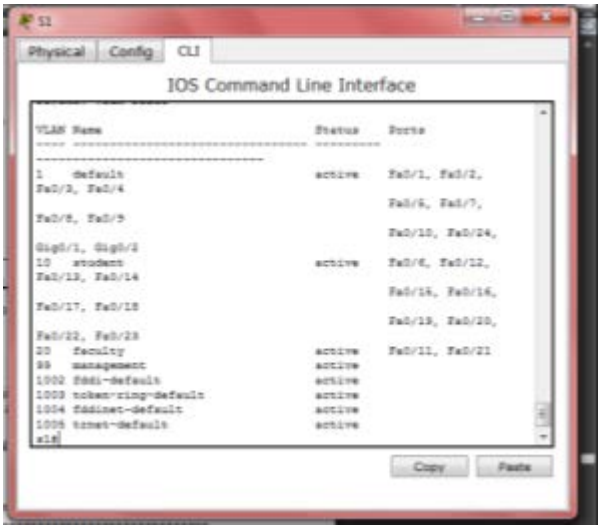
d. Verifique que las asignaciones de VLAN sean las correctas.



Step 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?

VLAN 1, la VLAN predeterminada

_____

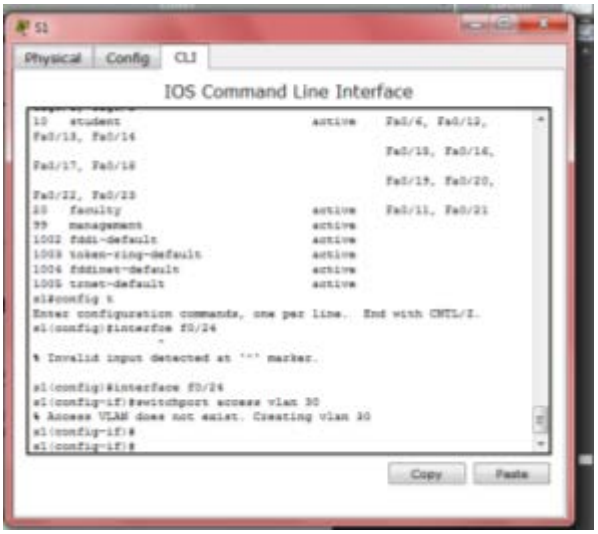
_____

Step 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.

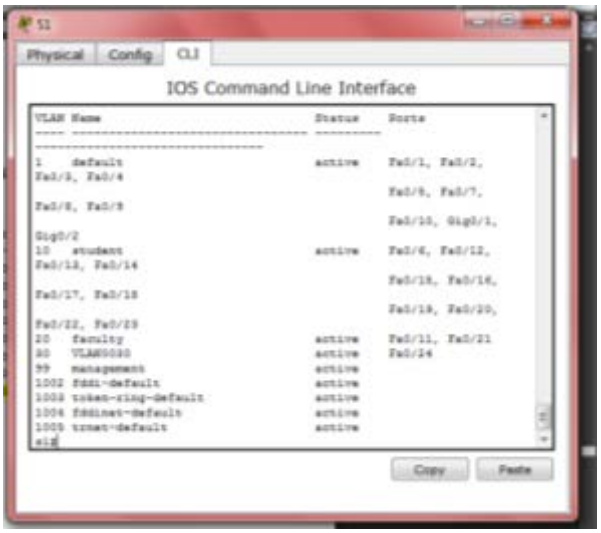
```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

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

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, Gi0/1, Gi0/2
10   Student                           active    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                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```



¿Cuál es el nombre predeterminado de la VLAN 30?

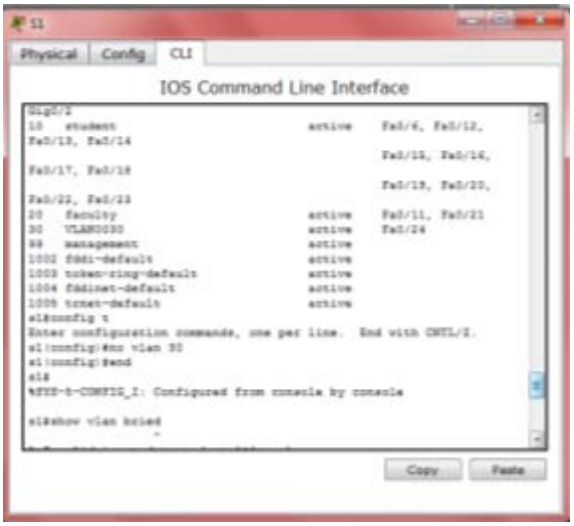
VLAN0030

_____

_____

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?

_El puerto F0/24 no se asigna a ninguna VLAN. Este puerto no transfiere tráfico

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
--
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                           active    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                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

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

_____

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?

_Las interfaces asignadas a una VLAN que se eliminó de la base de datos de VLAN no están disponibles para usar hasta que se reasignen a otra VLAN. Este problema puede ser difícil de resolver, ya que las interfaces de enlace troncal tampoco aparecen en la lista de puertos (en la parte 4, se incluye más información sobre las interfaces de enlace tronca

_____

Part 12: 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.

Step 1: usar DTP para iniciar el enlace troncal en F0/1.

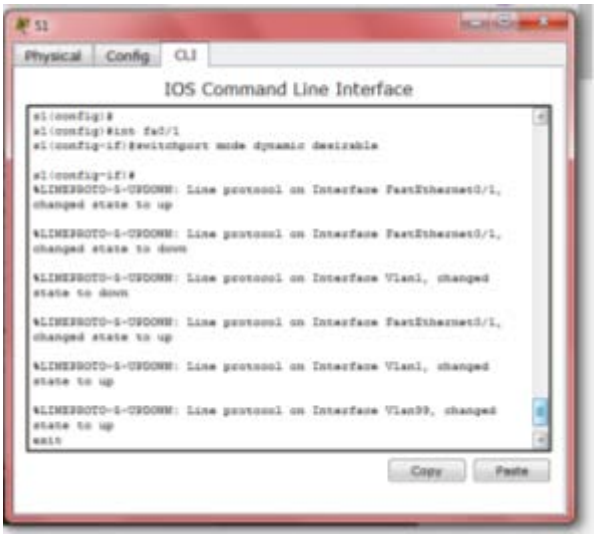
El modo de DTP predeterminado de un puerto en un switch 2960 es dinámico automático. Esto permite que la interfaz convierta el enlace en un enlace troncal si la interfaz vecina se establece en modo de enlace troncal o dinámico deseado.

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

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S1(config-if)#
*Mar  1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1(config-if)#
*Mar  1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar  1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

También debe recibir mensajes del estado del enlace en el S2.

```
S2#
*Mar  1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S2#
*Mar  1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S2#
*Mar  1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar  1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

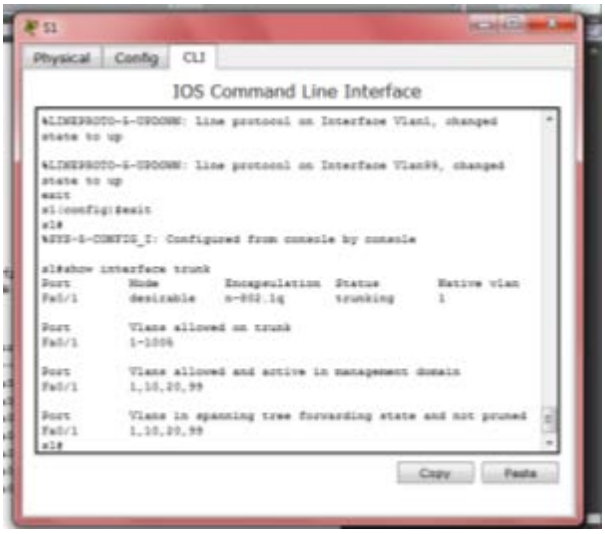


b. Emita el comando **show vlan brief** en el S1 y el S2. La interfaz F0/1 ya no está asignada a la VLAN 1. Las interfaces de enlace troncal no se incluyen en la tabla de VLAN.

```
S1# show vlan brief

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, Gi0/1, Gi0/2
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                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

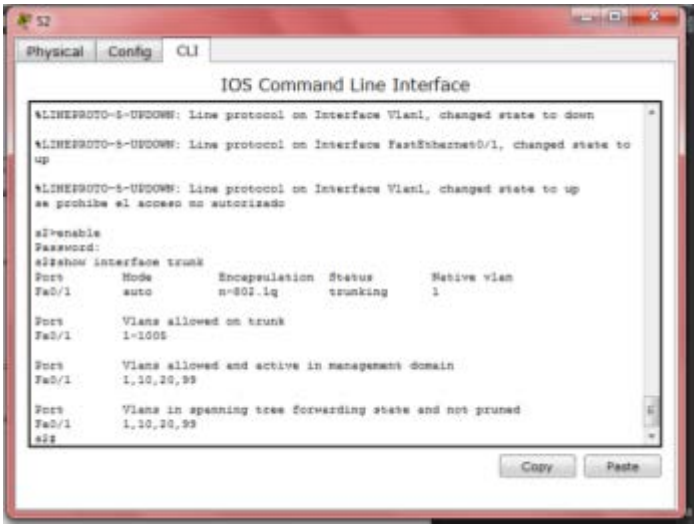
c. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

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

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



S2# **show interfaces trunk**

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

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

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



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

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

No se puede hacer ping de la PC-C a la PC-A o a la PC-B debido a que la PC-C está en una VLAN diferente. Los switches están en diferentes VLAN que las computadoras; por este motivo, los pings fallaron.

_____
_____

_____
_____

Step 2: configurar manualmente la interfaz de enlace troncal F0/1.

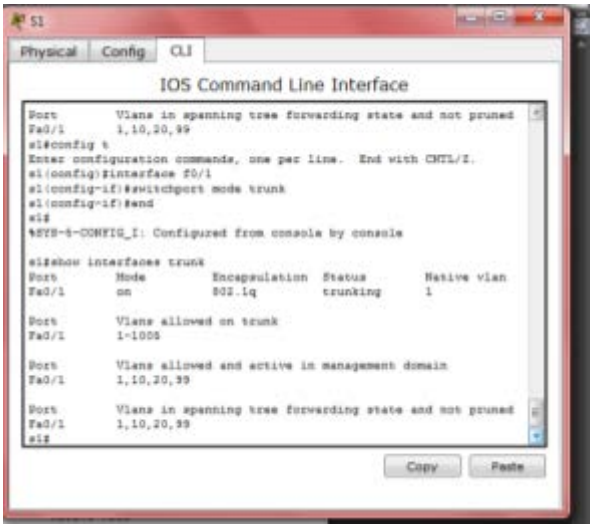
El comando **switchport mode trunk** se usa para configurar un puerto manualmente como enlace troncal. Este comando se debe emitir en ambos extremos del enlace.

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

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

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

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



¿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. Con el comando

switchport mode trunk

, se garantiza que el puerto se convierta en un enlace troncal, independientemente del tipo de equipo conectado al otro extremo del enlace

_____

Part 13: Eliminar la base de datos de VLAN

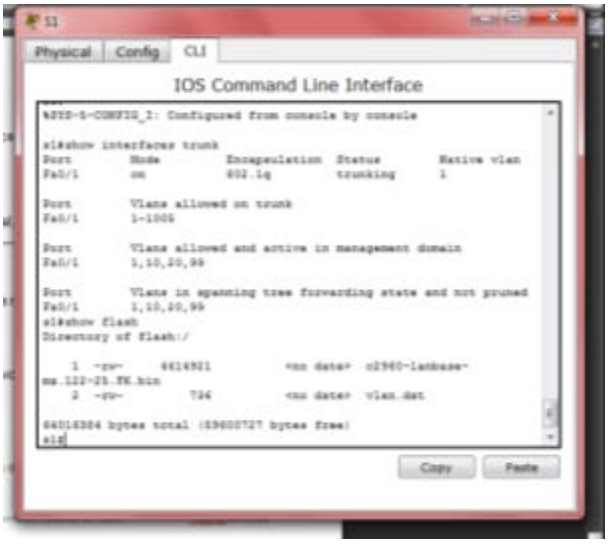
En la parte 5, eliminará la base de datos de VLAN del switch. Es necesario hacer esto al inicializar un switch para que vuelva a la configuración predeterminada.

Step 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

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
    6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

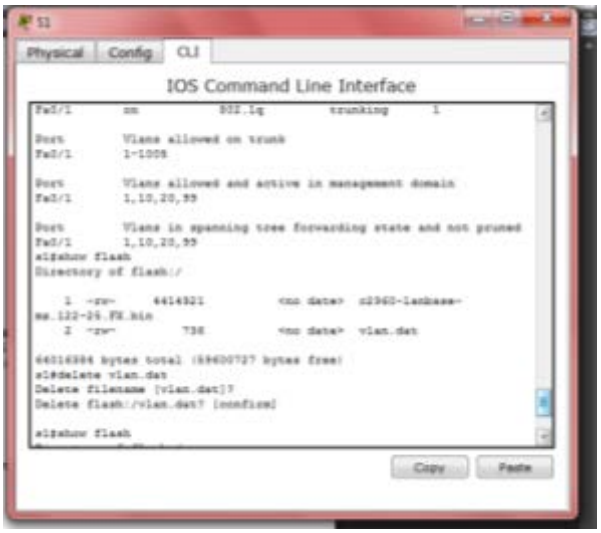
Nota: si hay un archivo **vlan.dat** en la memoria flash, la base de datos de VLAN no contiene la configuración predeterminada.



Step 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.

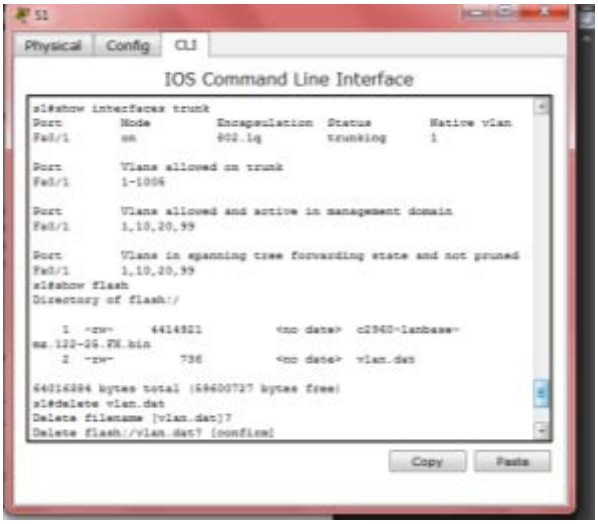
```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```



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

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
```

```
32514048 bytes total (20859904 bytes free)
```



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

Para que un switch vuelva a la configuración predeterminada, se deben emitir los comandos erase startup-config y reload después de emitir el comando delete vlan.da

Reflexión

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

   Las respuestas varían, pero se necesita el routing de capa 3 para enrutar el tráfico entre redes VLAN.

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

   Las respuestas varían, pero algunos de los beneficios de las VLAN incluyen lo siguiente: aumento de la seguridad, ahorro de costos (uso eficaz del ancho de banda y los uplinks), aumento del rendimiento (dominios de difusión más pequeños), mitigación de las tormentas de difusión, aumento de la eficiencia del personal de TI, simplificación de la administración de proyectos y aplicaciones

3.3.2.2 Lab - Implementing VLAN Security

Práctica de laboratorio: implementación de seguridad de VLAN

Topología

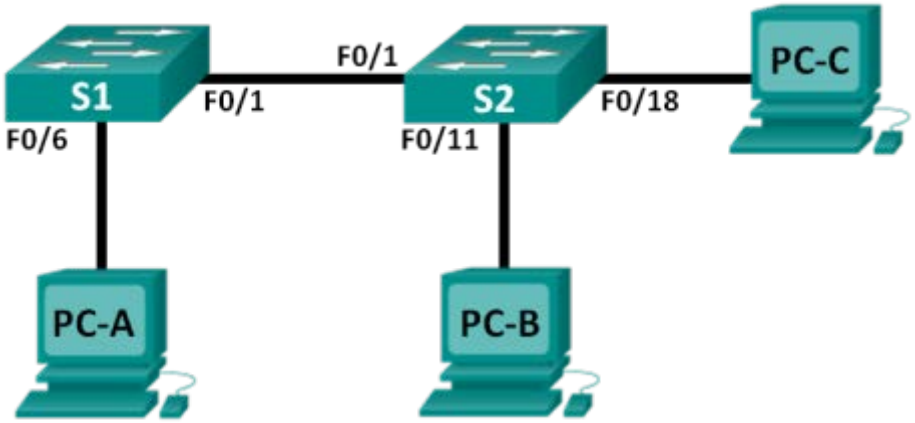


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

Objetivos

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

Parte 2: implementar seguridad de VLAN en los switches

Información básica/situación

La práctica recomendada indica que se deben configurar algunos parámetros básicos de seguridad para los puertos de enlace troncal y de acceso en los switches. Esto sirve como protección contra los ataques de VLAN y la posible detección del tráfico de la red dentro de esta.

En esta práctica de laboratorio, configurará los dispositivos de red en la topología con algunos parámetros básicos, verificará la conectividad y, a continuación, aplicará medidas de seguridad más estrictas en los switches. Utilizará varios comandos **show** para analizar la forma en que se comportan los switches Cisco. Luego, aplicará medidas de seguridad.

Nota: los switches que se utilizan en esta práctica de laboratorio son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

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

Recursos necesarios

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

Part 14: 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.

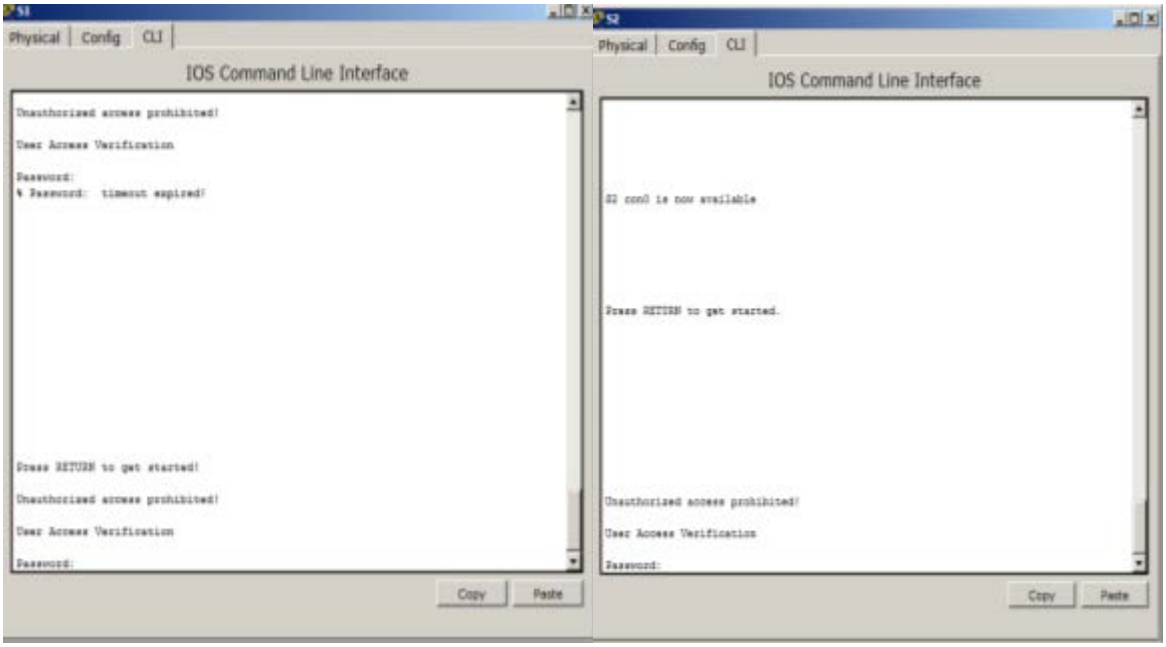
c. Asigne **class** como la contraseña del modo EXEC privilegiado.

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.

Contraseña: **boriscartagena**

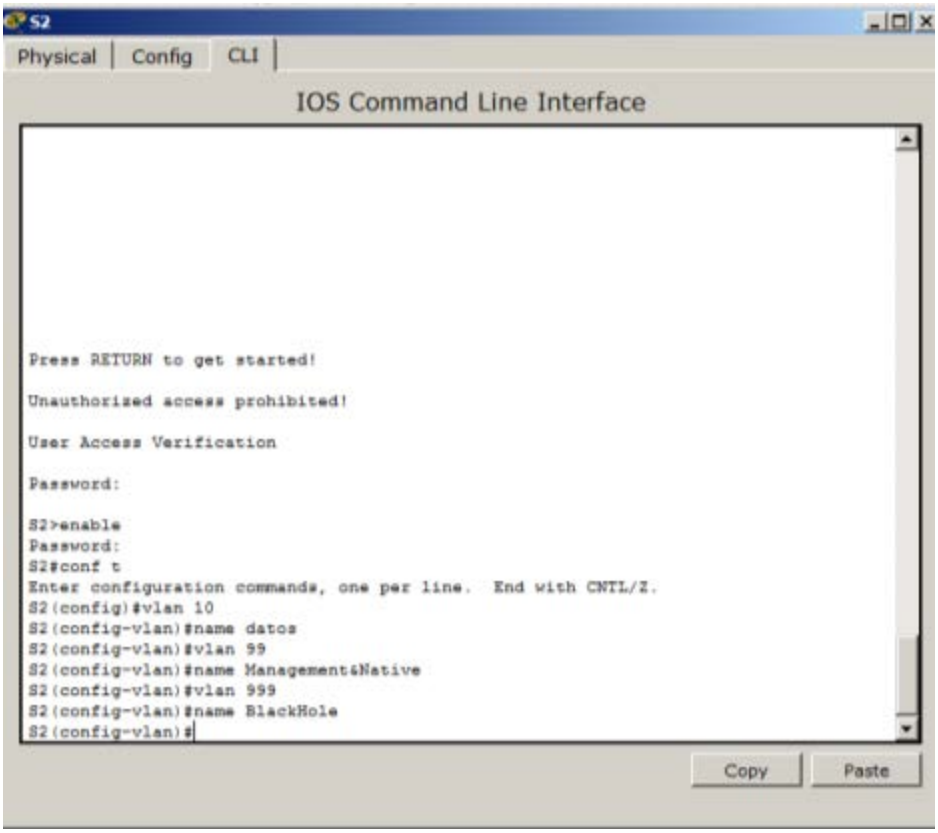
Contraseña:**cisco12345**



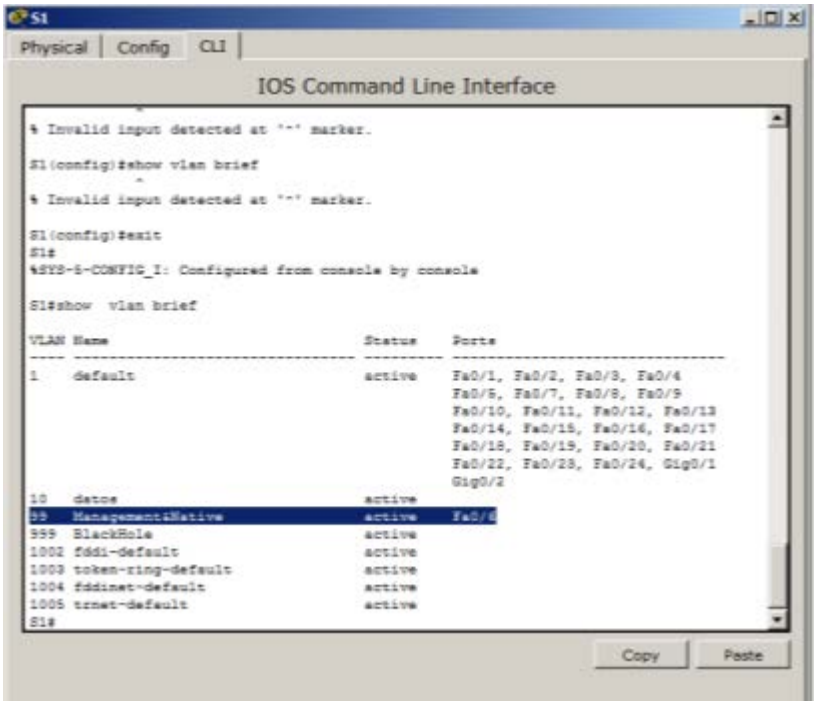
Paso 5. configurar las VLAN en cada switch.

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

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

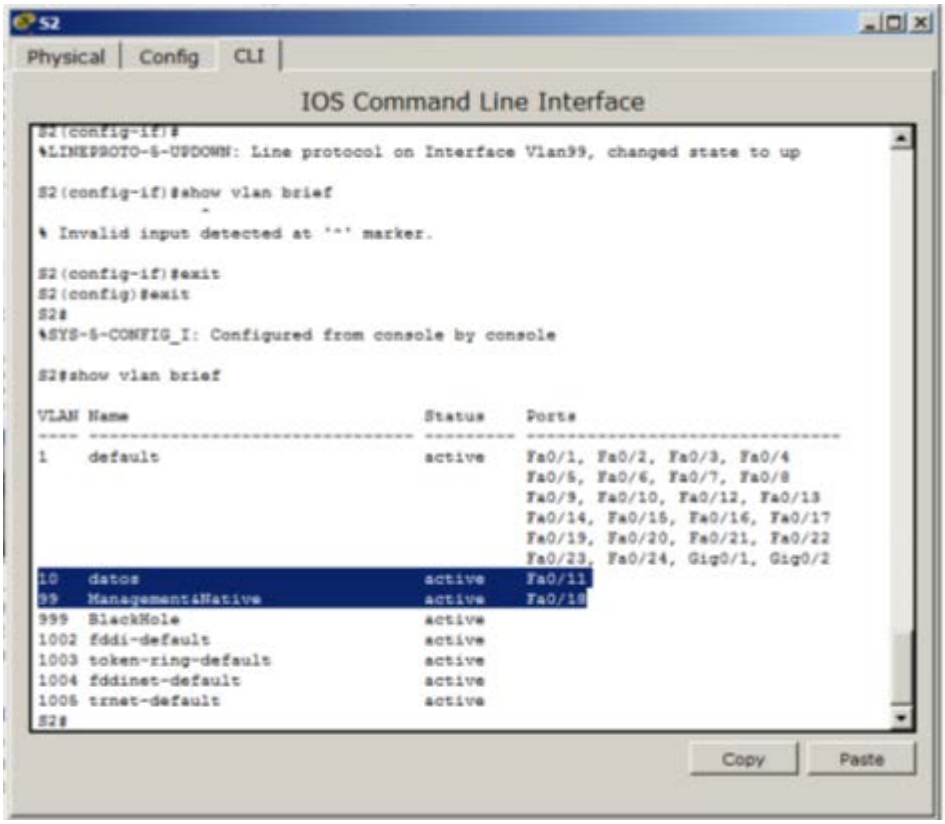


c. Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.



d. Configure F0/11 en el S2 como puerto de acceso y asígnelo a la VLAN 10.

e. Configure F0/18 en el S2 como puerto de acceso y asígnelo a la VLAN 99.



f. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN y de puertos.

¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2? **Está en la vlan 1**

Paso 6. configurar la seguridad básica del switch.

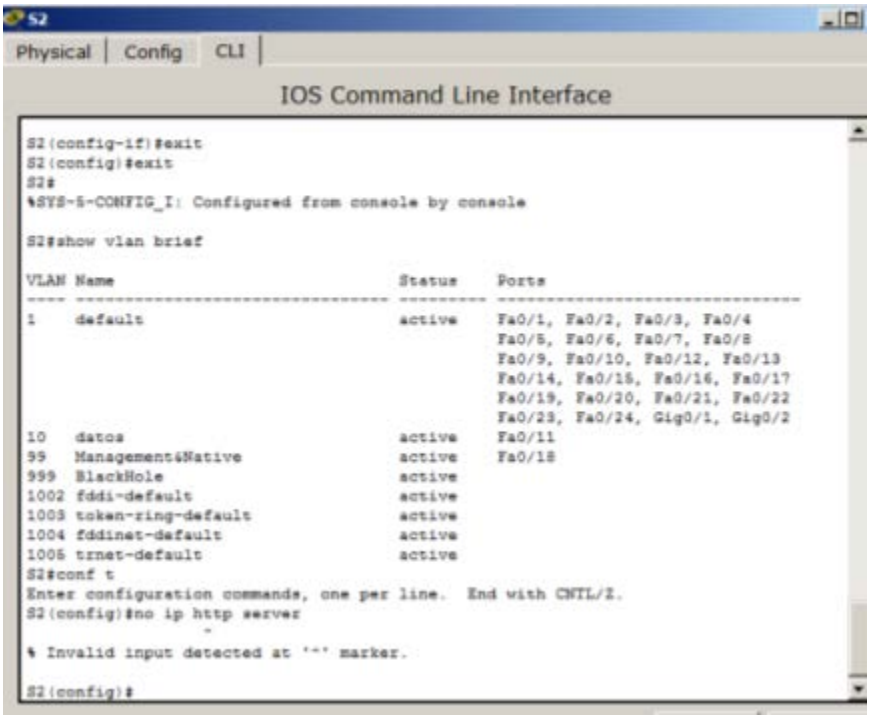
g. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

h. Encripte todas las contraseñas.

i. Desactive todos los puertos físicos sin utilizar.

j. Deshabilite el servicio web básico en ejecución.

```
S1(config)# no ip http server
S2(config)# no ip http server
```



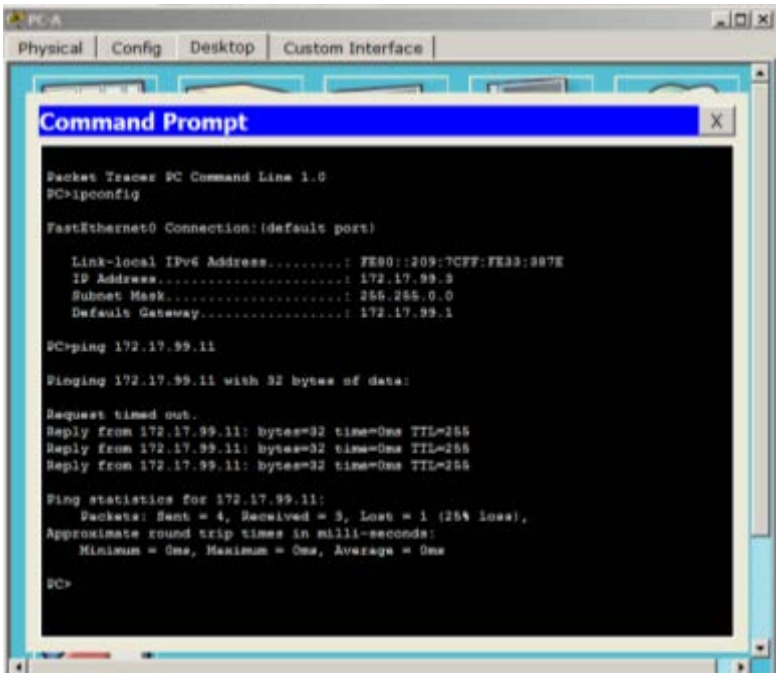
- **No corre la instrucion en el packet tracer**

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

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

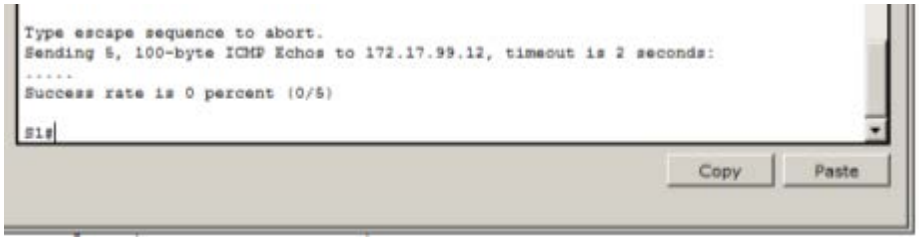
l. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

- **Si hay comunicacion entre el PC-A y S1 por que estan en la misma red**



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

- **No se pudo hacer ping porque no tienen asignación de la troncal**



n. 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?

- En el pc-a con el s2 no hacen ping por que no estan en la misma vlan
- En la pc-c con el s1 no hacen ping por que no estan en la misma vlan

o. 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?

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

Part 15: implementar seguridad de VLAN en los switches

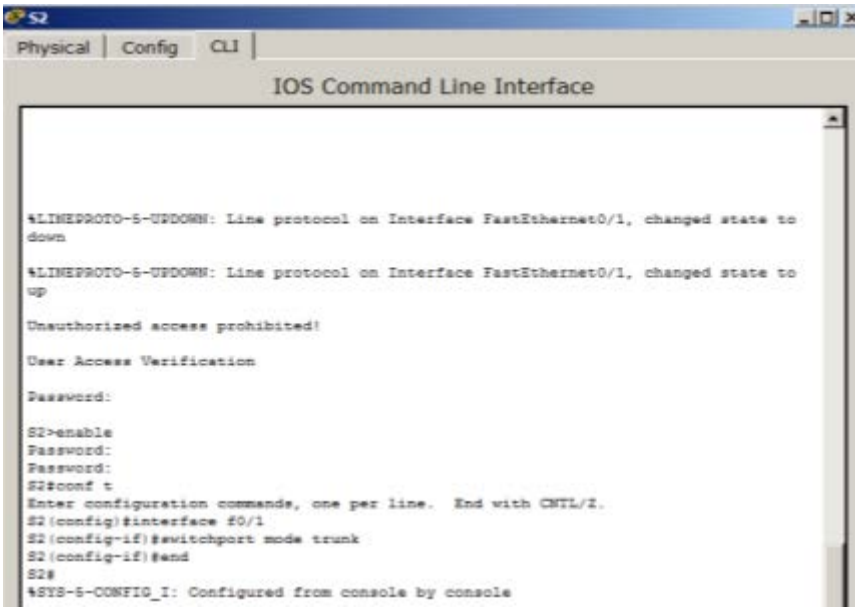
Paso 1. configurar puertos de enlace troncal en el S1 y el S2.

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
```

b. Configure el puerto F0/1 en el S2 como puerto de enlace troncal.

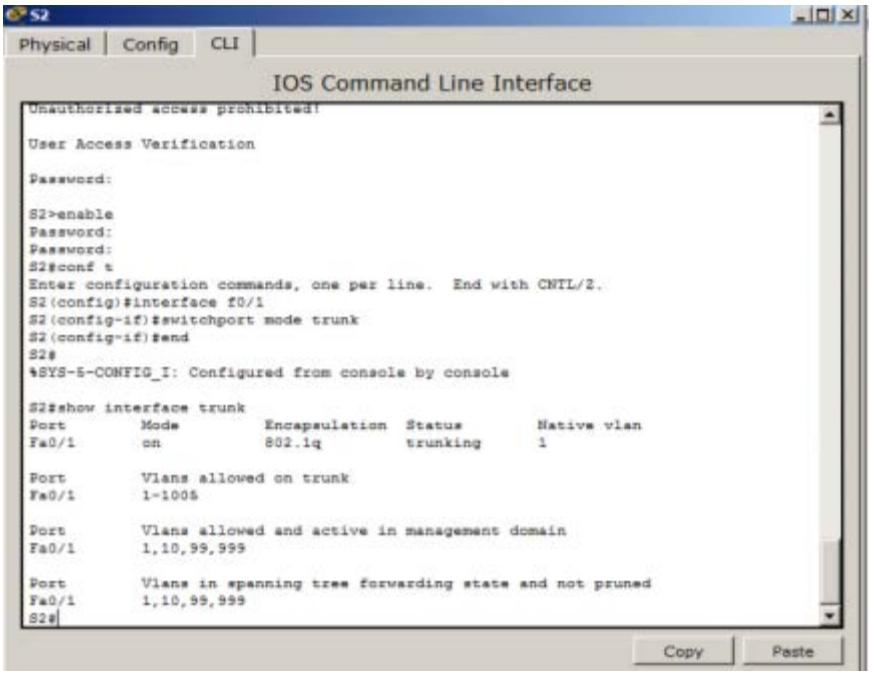
```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```



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**

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```



Paso 2. cambiar la VLAN nativa para los puertos de enlace troncal en el S1 y el S2.

Es aconsejable para la seguridad cambiar la VLAN nativa para los puertos de enlace troncal de la VLAN 1 a otra VLAN.

d. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?

- **Vlan 1**

e. 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
```

f. 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:?

_____
___

g. 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
```

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

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Paso 3. verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.

i. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

- **si**

j. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

- **El ping si se realiza ya que creamos una troncal**

_____
_____

k. 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?

- **No funciona por que esta en la capa 2 de la red**

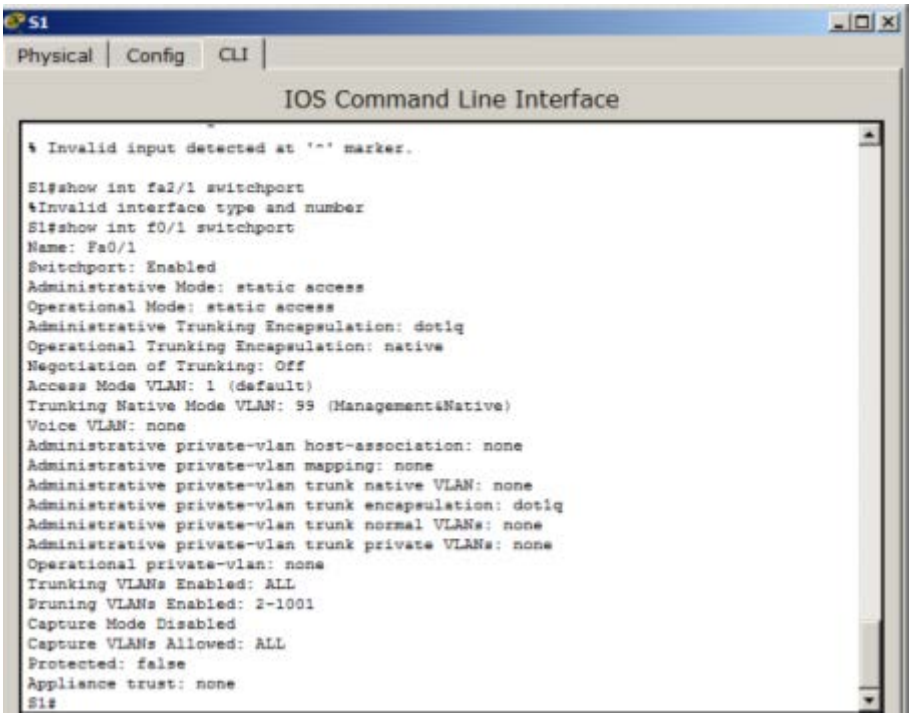
l. En el símbolo del sistema de la PC-C, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A. ¿Tuvo éxito? ¿Por qué?

- **Si hace ping**

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>
```



m. Desactive la negociación en el S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

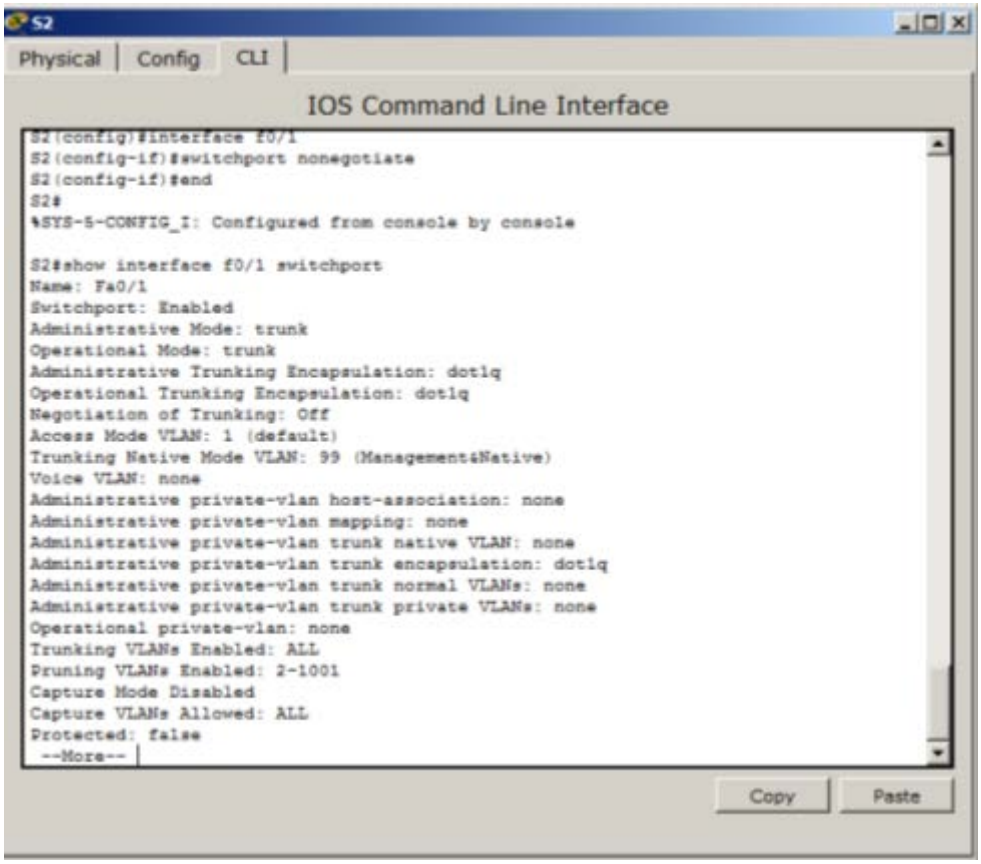
n. Desactive la negociación en el S2.

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

o. 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.

p. 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>
```

q. Deshabilite los enlaces troncales en los puertos de acceso del S1.

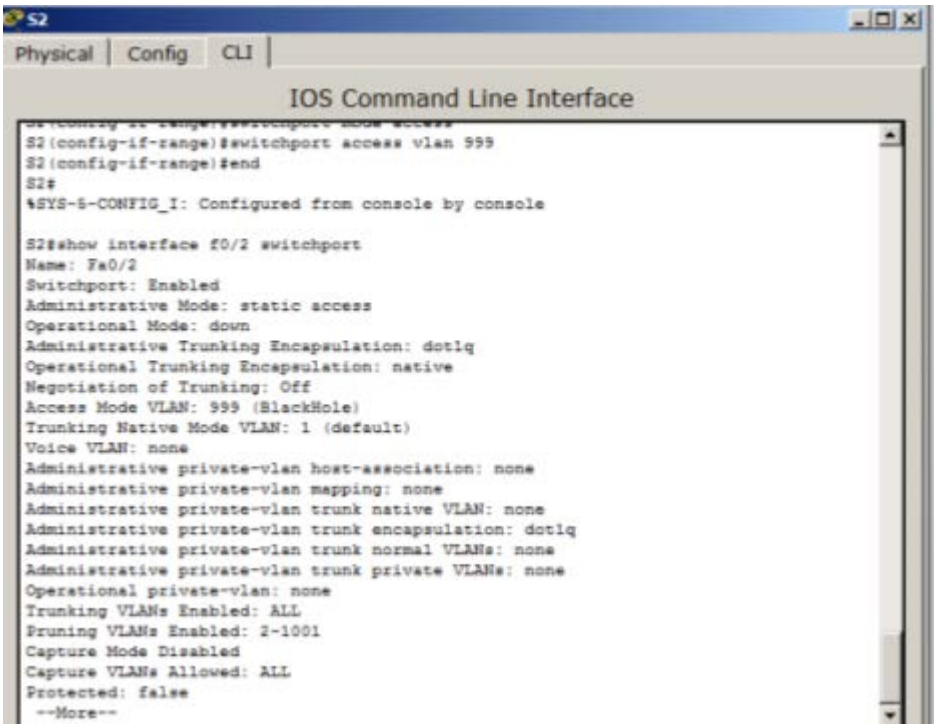
```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

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

s. 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>
```

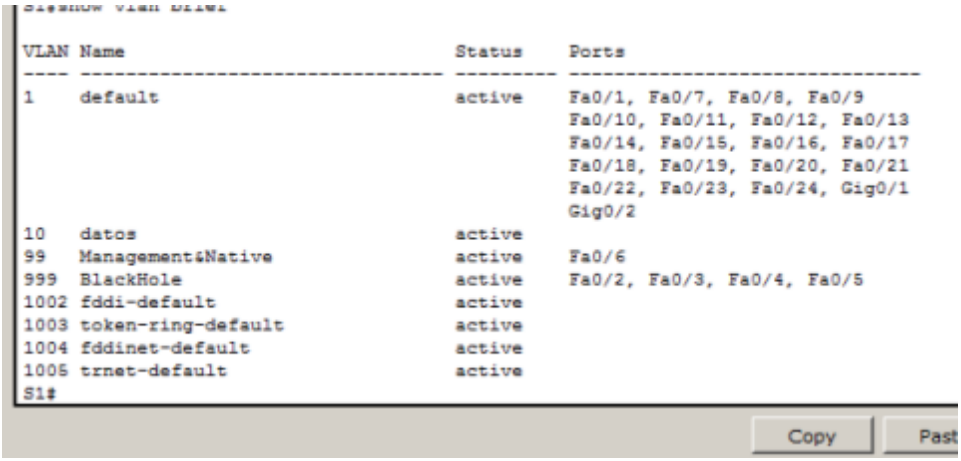


t. Verifique que las asignaciones de puertos de VLAN en ambos switches sean las correctas. A continuación, se muestra el S1 como ejemplo.

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.
```

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.



```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, 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#
```

Copy Past

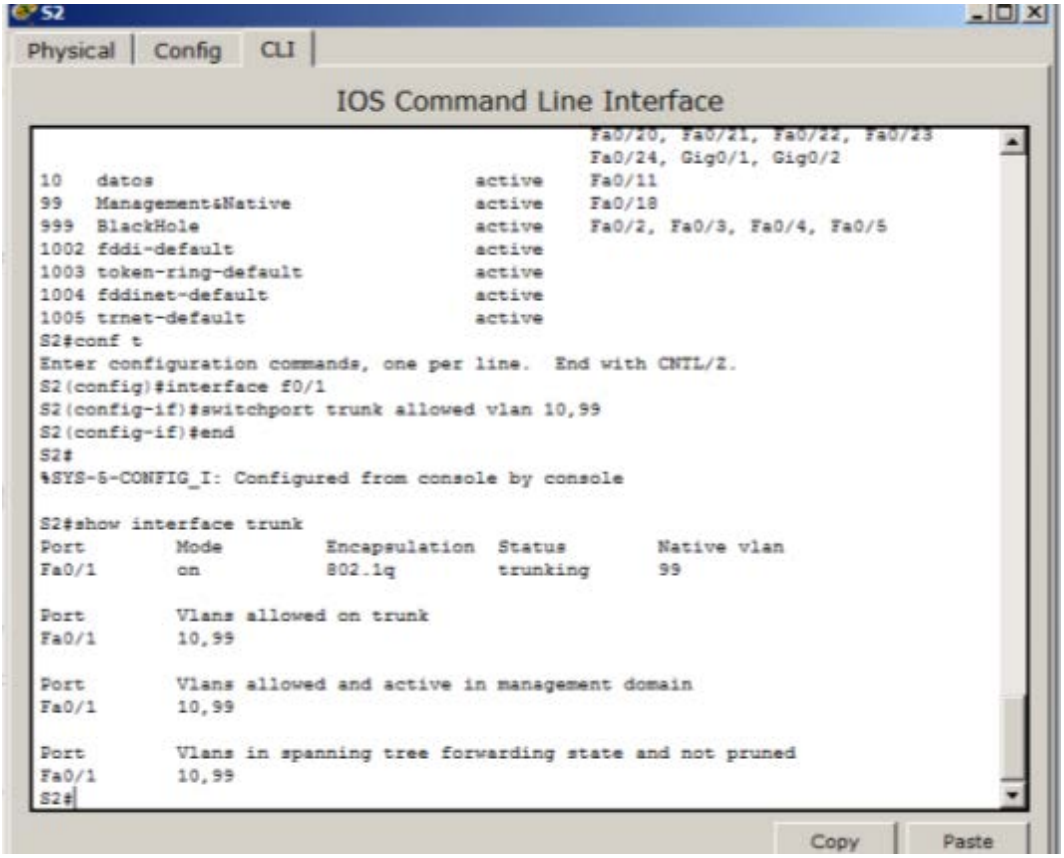
u. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10 y 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

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

w. Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo EXEC privilegiado en el S1 y el S2

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

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

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


S2
Physical
Config
CLI
IOS Command Line Interface
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 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
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport trunk allowed vlan 10,99
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
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#
Copy
Paste

4.1.4.6 Lab - Configuring Basic Router Settings with IOS CLI

Boris Arnaldo Cartgena

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

Topología

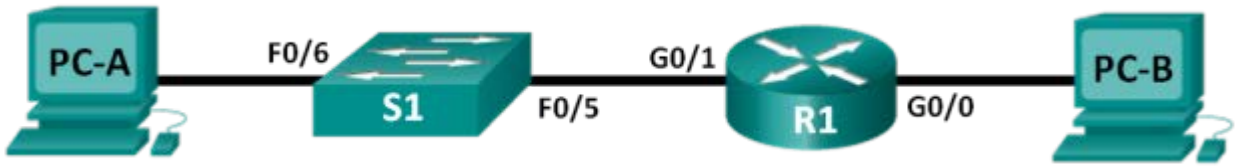


Tabla de direccionamiento

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

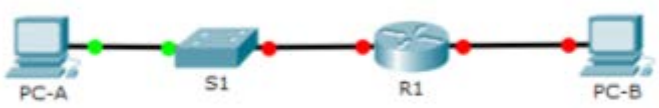
Nota: las interfaces Gigabit Ethernet en los ISR Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: establecer la topología e inicializar los dispositivos

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

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

y. Encienda todos los dispositivos de la topología.



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

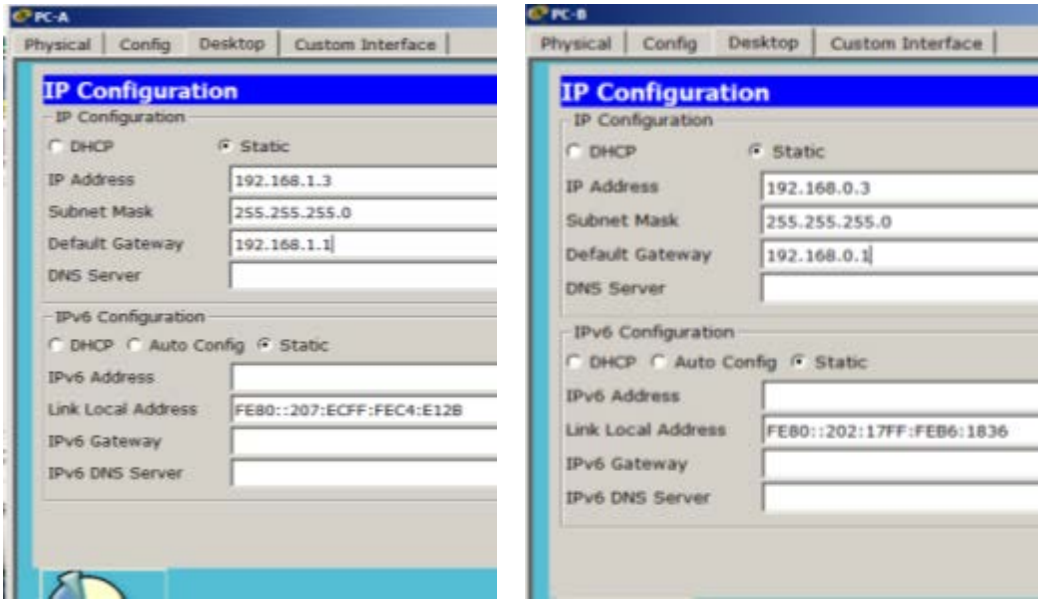
Nota: en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

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**?

- El tiempo de espera en consola para ser digitada la contraseña

_____
_____

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#
```

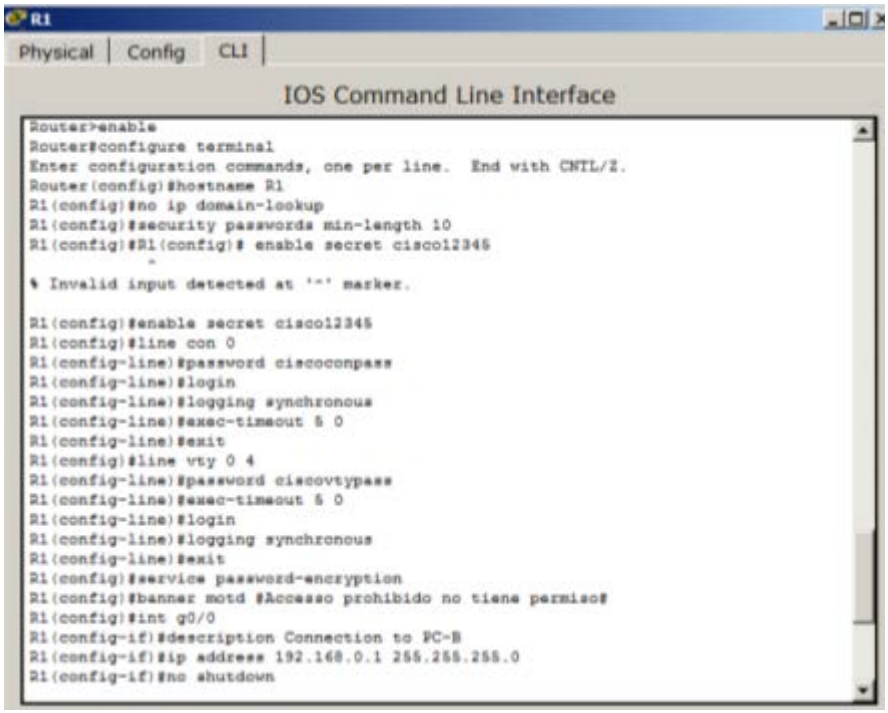
l. Configure el reloj en el router, por ejemplo:

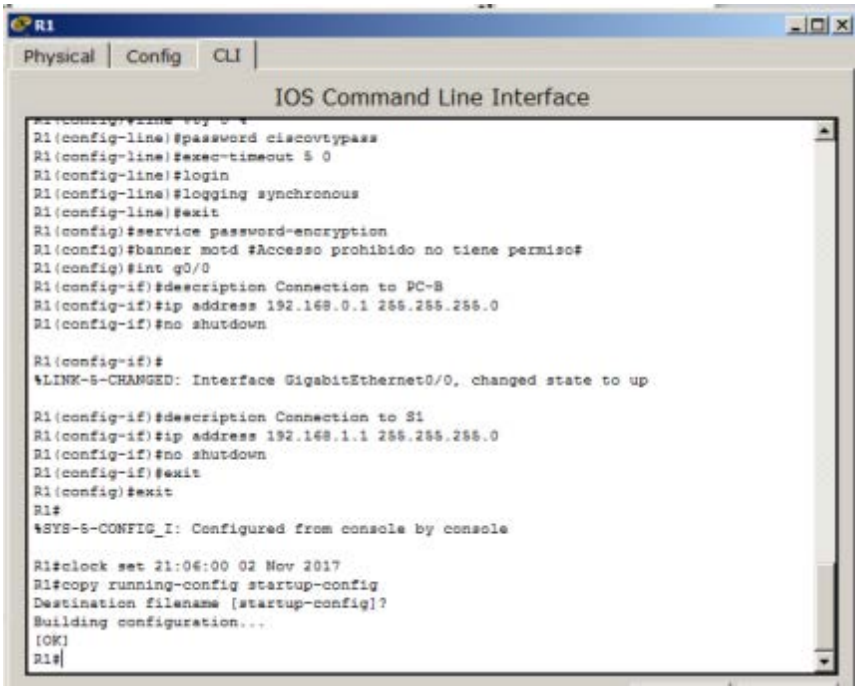
```
R1# clock set 17:00:00 18 Feb 2013
```

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

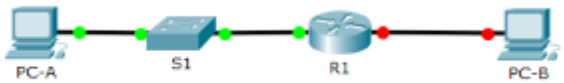
```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

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





Se establece conexión entre el S1 Y R1



Se borraría toda la configuración que se realice, ya que el router no tendría una configuración de inicio.

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.

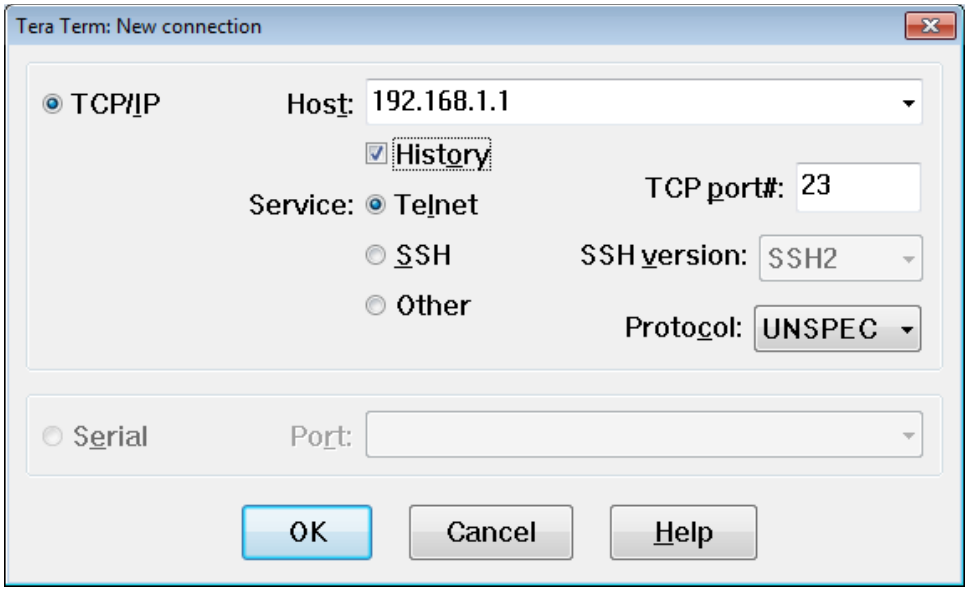
¿Tuvieron éxito los pings? si

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

Telnet

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? **si**

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

- Por qué puede conocerse la contraseñas e información por terceros

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

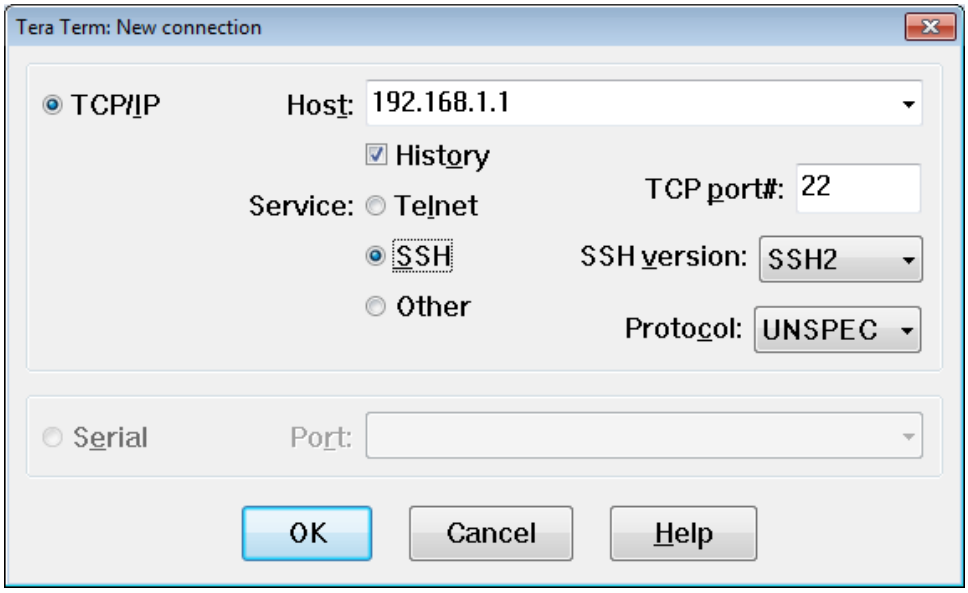
a. Habilite las conexiones SSH y cree un usuario en la base de datos local del router.

```
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.

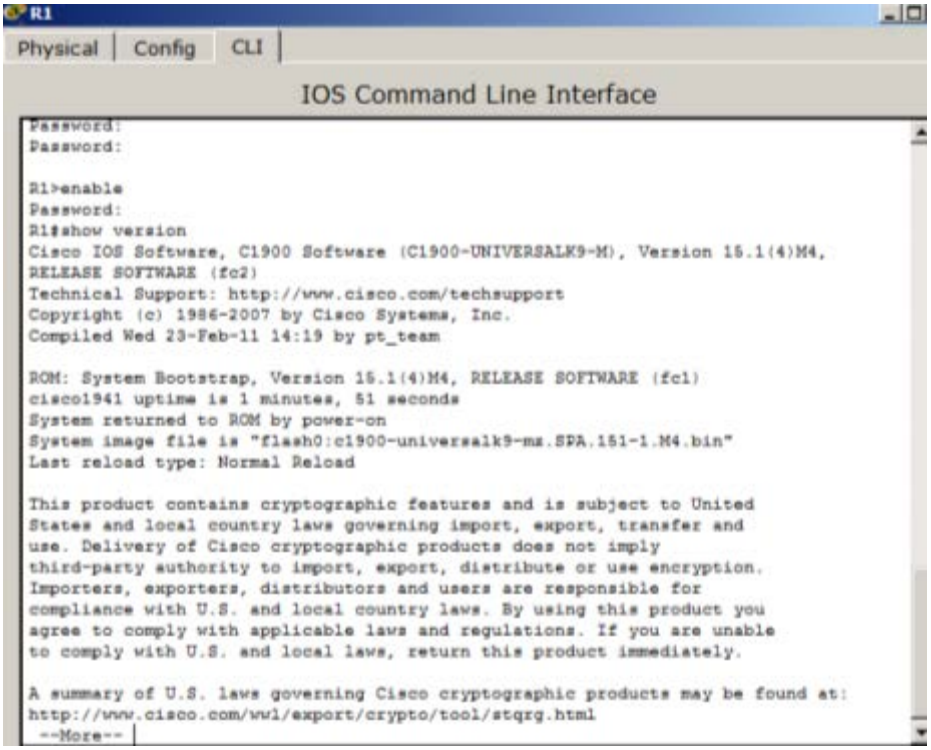
Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: nueva conexión). Asegúrese de que el botón de opción **SSH** esté seleccionado y después haga clic en **OK** para conectarse al router.



¿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?

- **System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"**

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

- **255K bytes of non-volatile configuration memory.**

¿Cuánta memoria flash tiene el router?

- **249856K bytes of ATA System CompactFlash 0 (Read/Write)**

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?

- **No se puede realizar simulando con el Packet Tracer, no ejecuta el comando.**

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?

- enable secret 5 1mERr$WvpW0n5HghRrqnrwXCUUl. **Están encriptados**

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

¿Qué resultado se obtiene al usar este comando?

- **No se puede realizar simulando con el Packet Tracer, no ejecuta el 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?

- **C 192.168.0.0/24 is directly connected, GigabitEthernet0/0**

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

- **2**

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?

- **no shutdown**

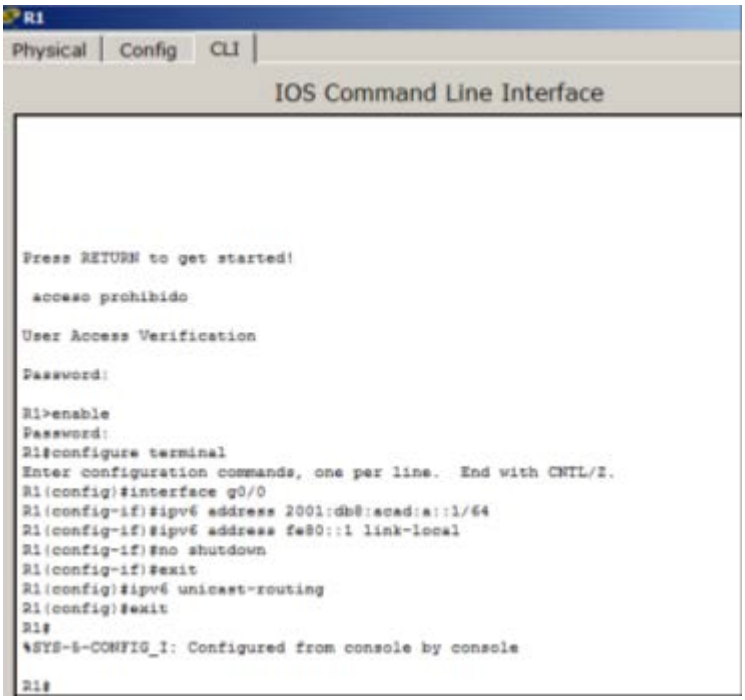
Parte 4: configurar IPv6 y verificar la conectividad

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]?

- **la capa 1 y la capa 2 de la interfaz y no depende de la capa 3.**

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?

- **Link-local IPv6 Address.....: FE80::202:17FF:FEB6:1836**

¿Cuál es el gateway predeterminado asignado a la PC-B?

- **Default Gateway.....: 192.168.0.1**

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 interface brief o show startup-config**
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 interface brief o 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?
   - **Falla porque g0/1 ipv6 no tiene configuración y el pc-a solo tiene ipv4**

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.

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

```
Router> enable
```

```
Router#
```

e. 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#
```

f. 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.

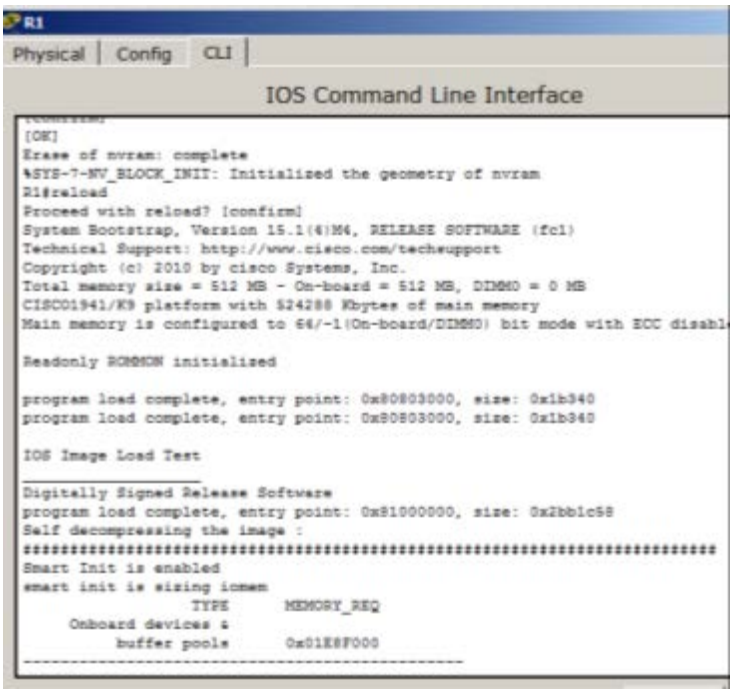
```
System configuration has been modified. Save? [yes/no]: no
```

g. 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
```

h. 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).

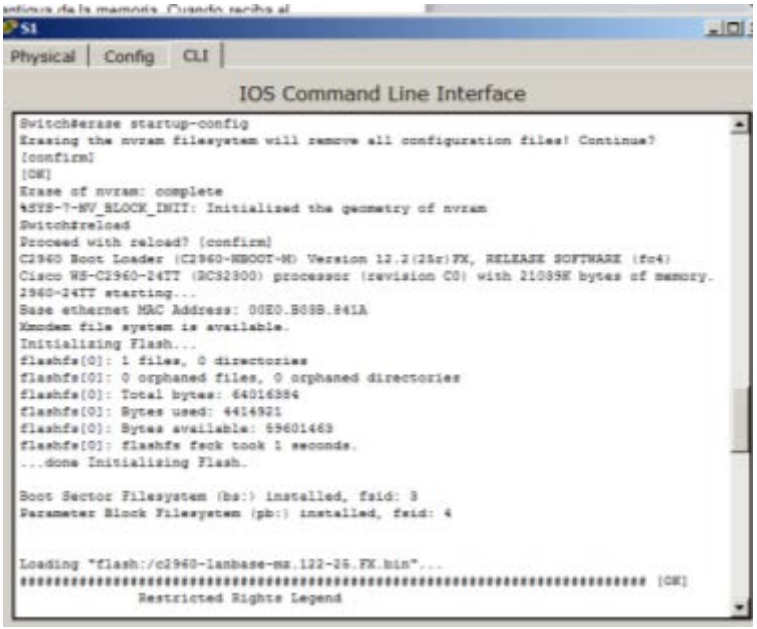
```
Switch# reload
Proceed with reload? [confirm]
```

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>
```



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

Ingrid Yalile Rodriguez

Configuring Router-on-a-Stick Inter-VLAN Routing

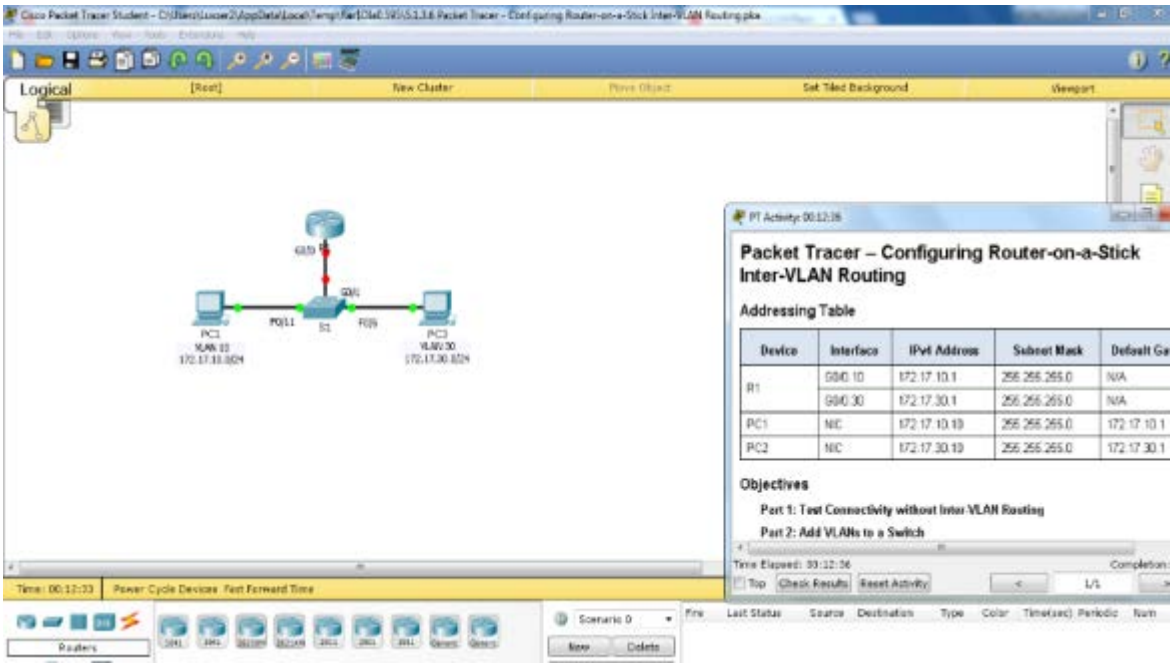
Addressing Table

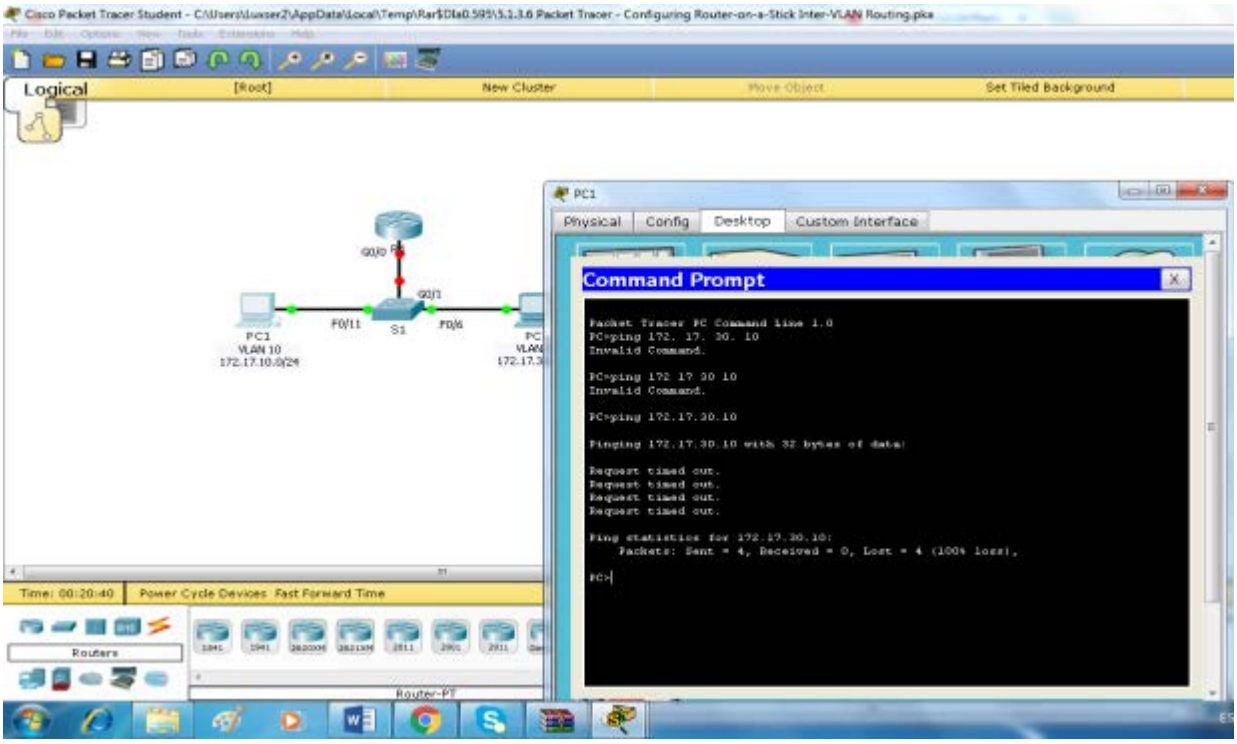
Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

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.

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.

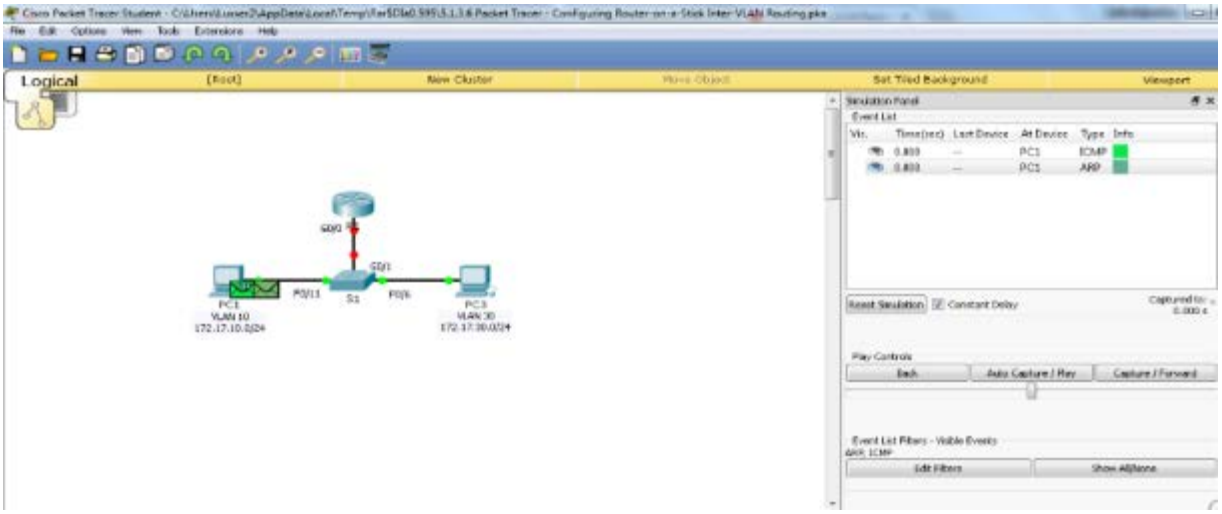


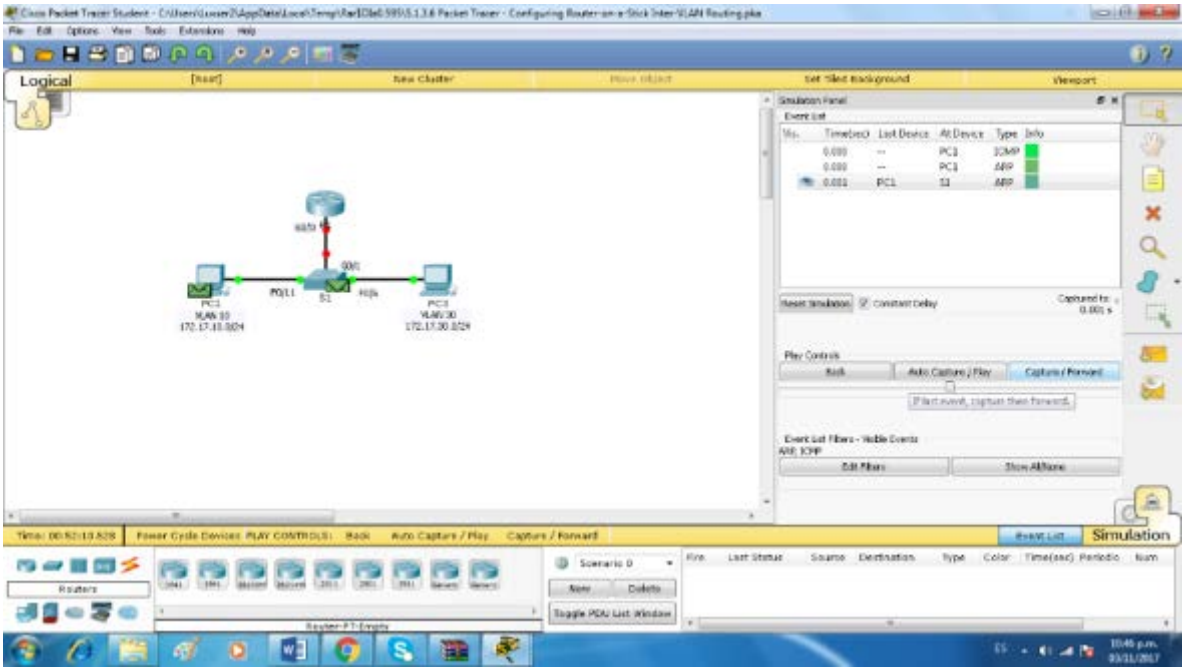


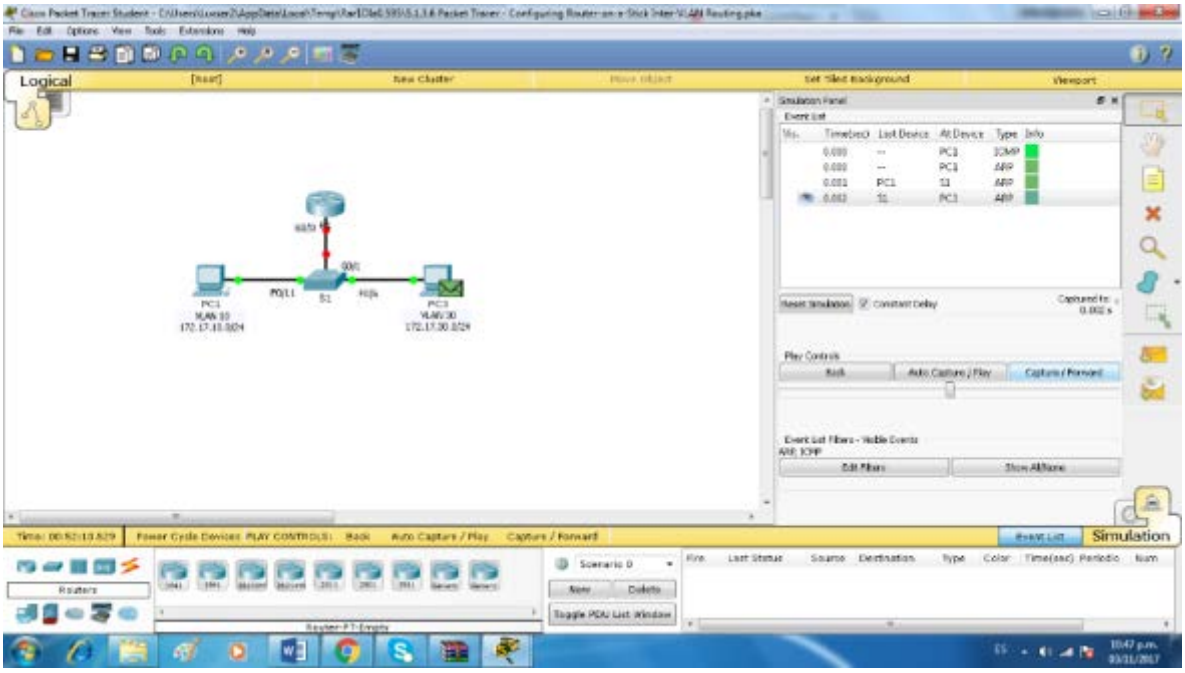
Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

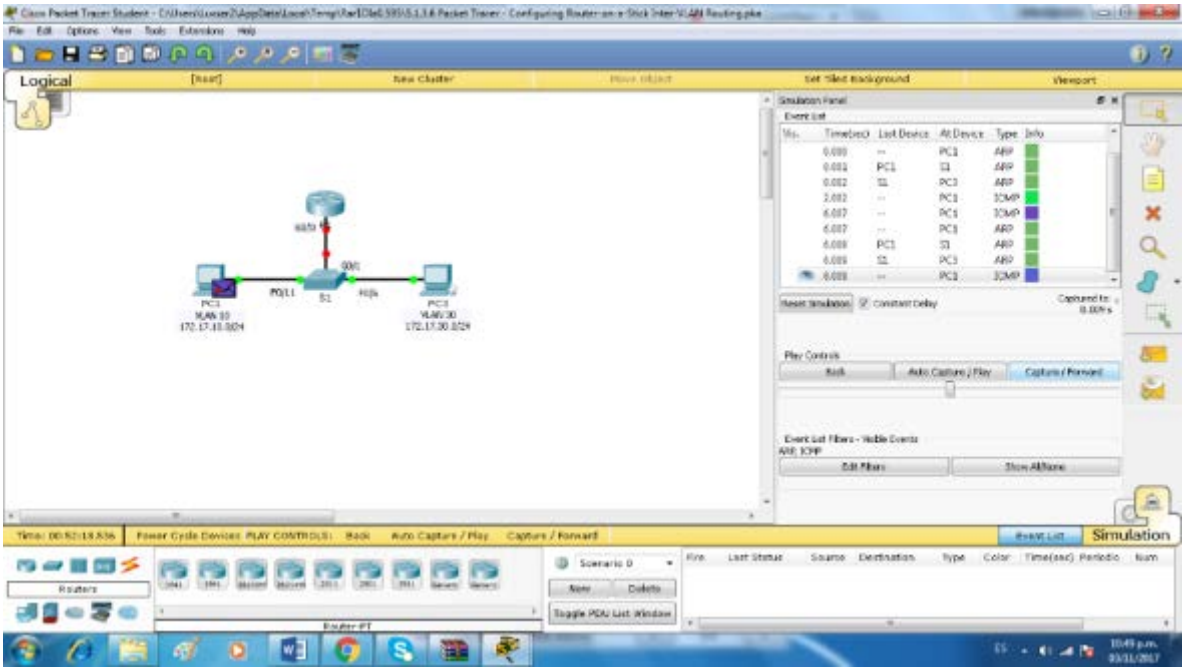
b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why?







What process failed and why?



Ha fallado porque la PC1 está en una red distinta a la PC2

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**.

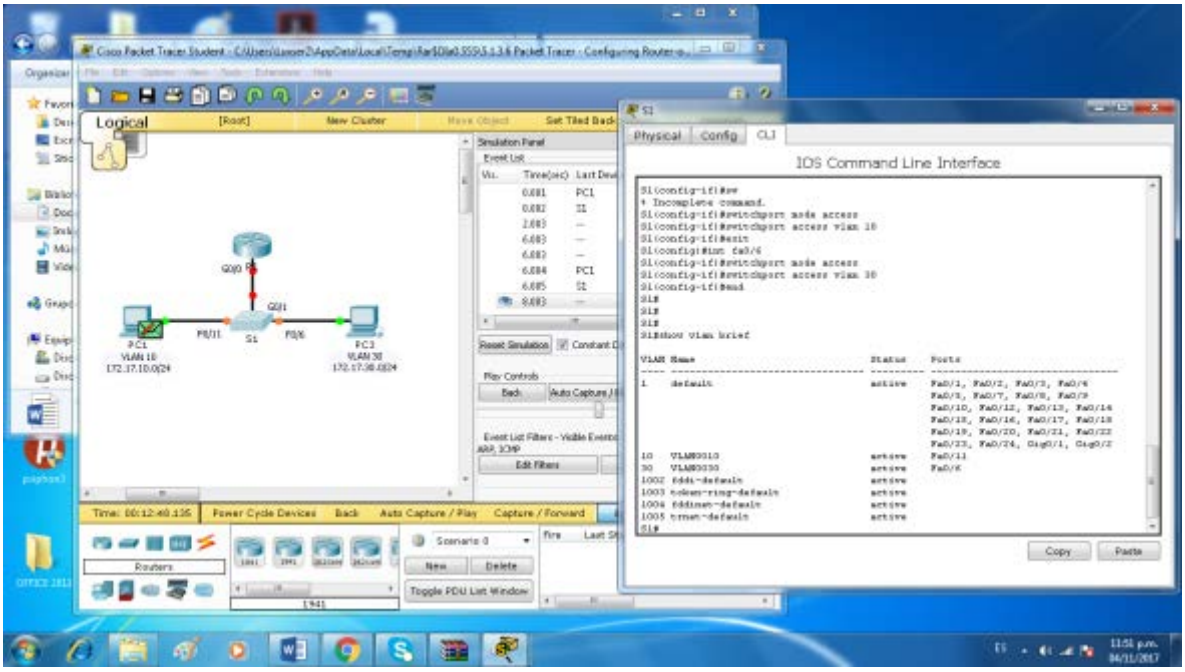
Step 2: Assign VLANs to ports.

a. Configure interface F0/6 and F0/11 as access ports and assign VLANs.

- Assign **PC1** to VLAN 10.
- Assign **PC3** to VLAN 30.

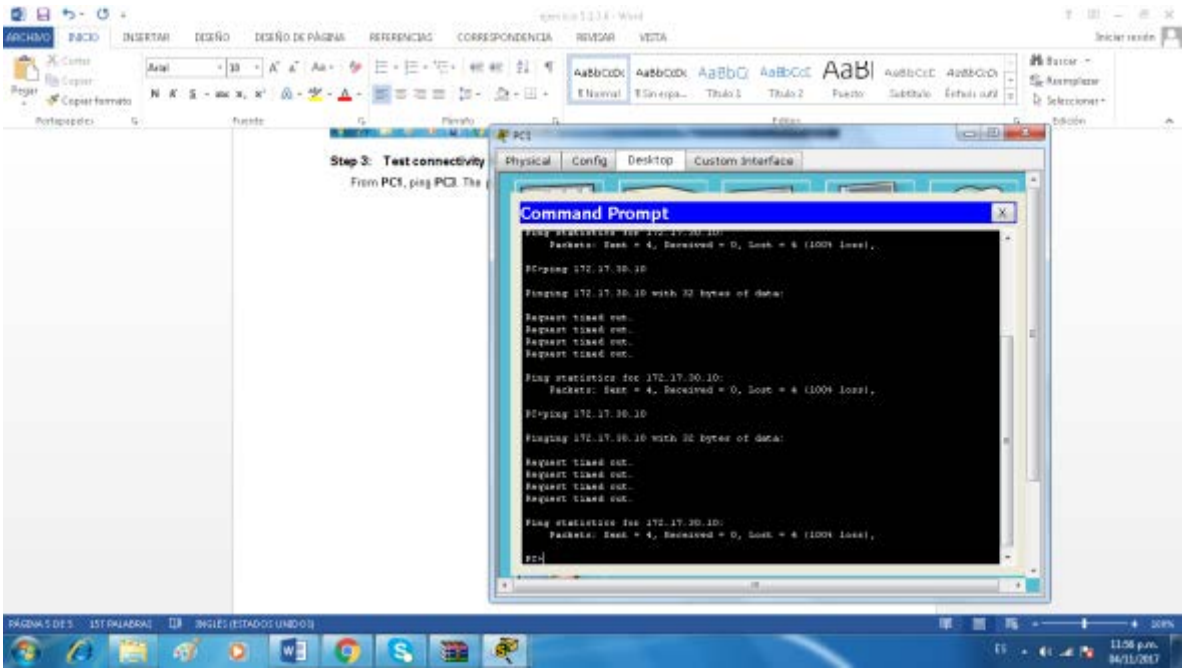
b. Issue the **show vlan brief** command to verify VLAN configuration.

S1# **show vlan brief**



Step 3: Test connectivity between PC1 and PC3.

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



Part 3: Configure Subinterfaces

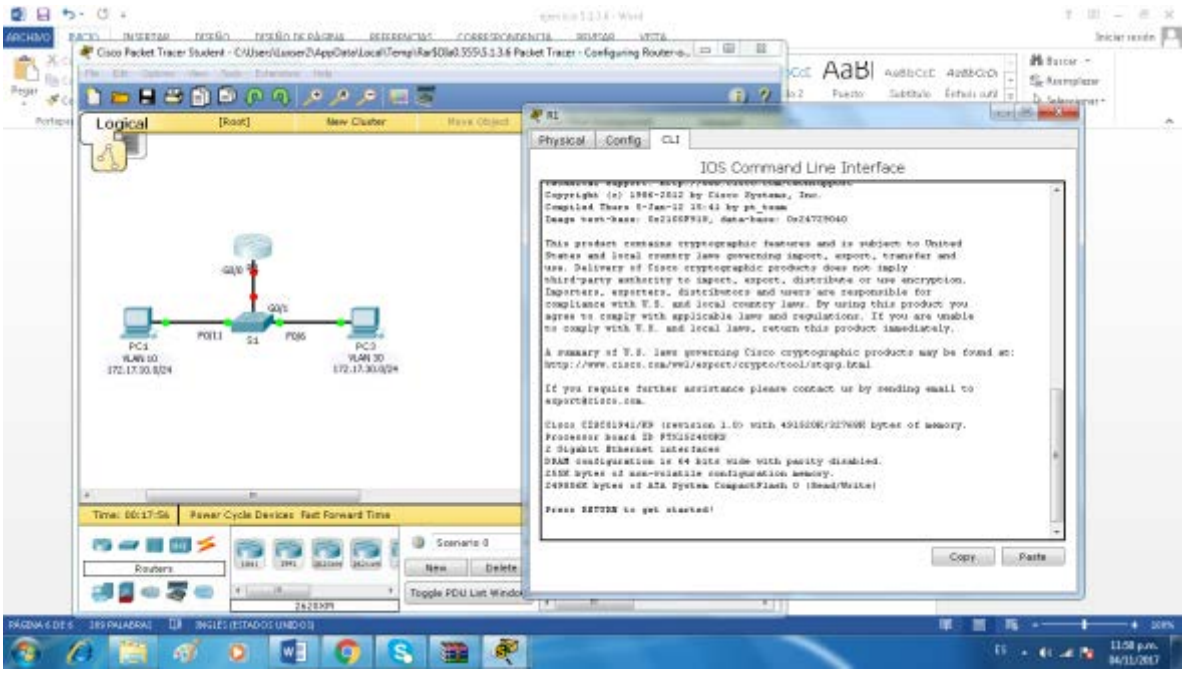
Step 1: Configure subinterfaces on R1 using the 802.1Q encapsulation.

a. Create the subinterface G0/0.10.

· Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.

· Refer to the **Address Table** and assign the correct IP address to the subinterface.

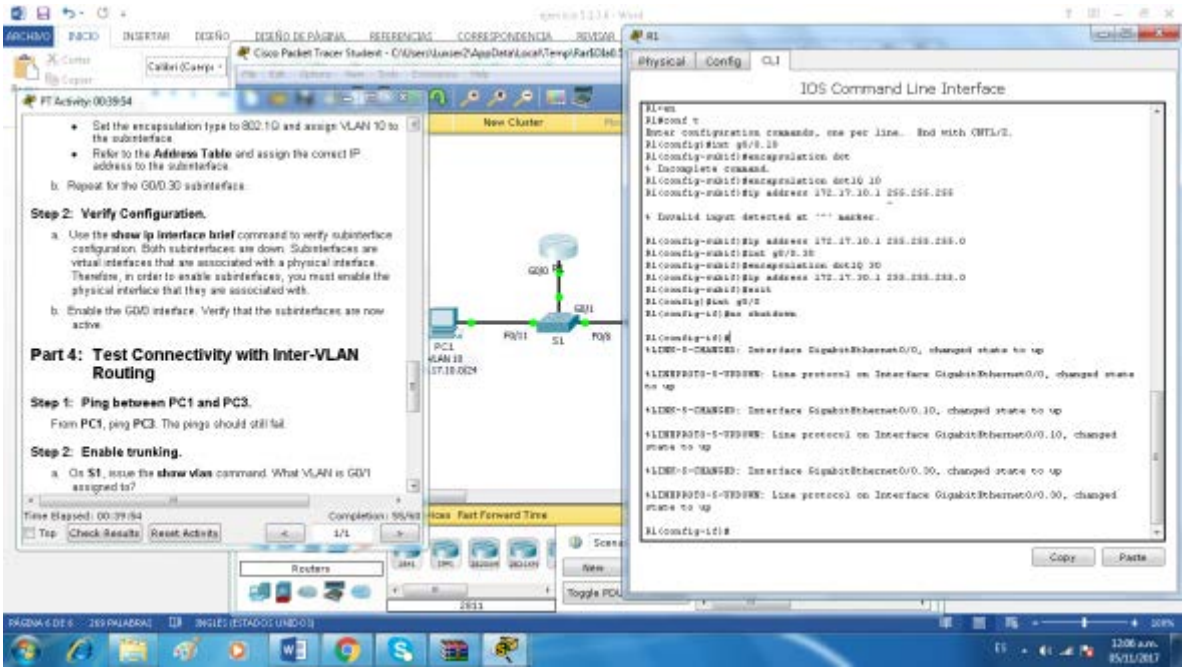
b. Repeat for the G0/0.30 subinterface.



Step 2: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

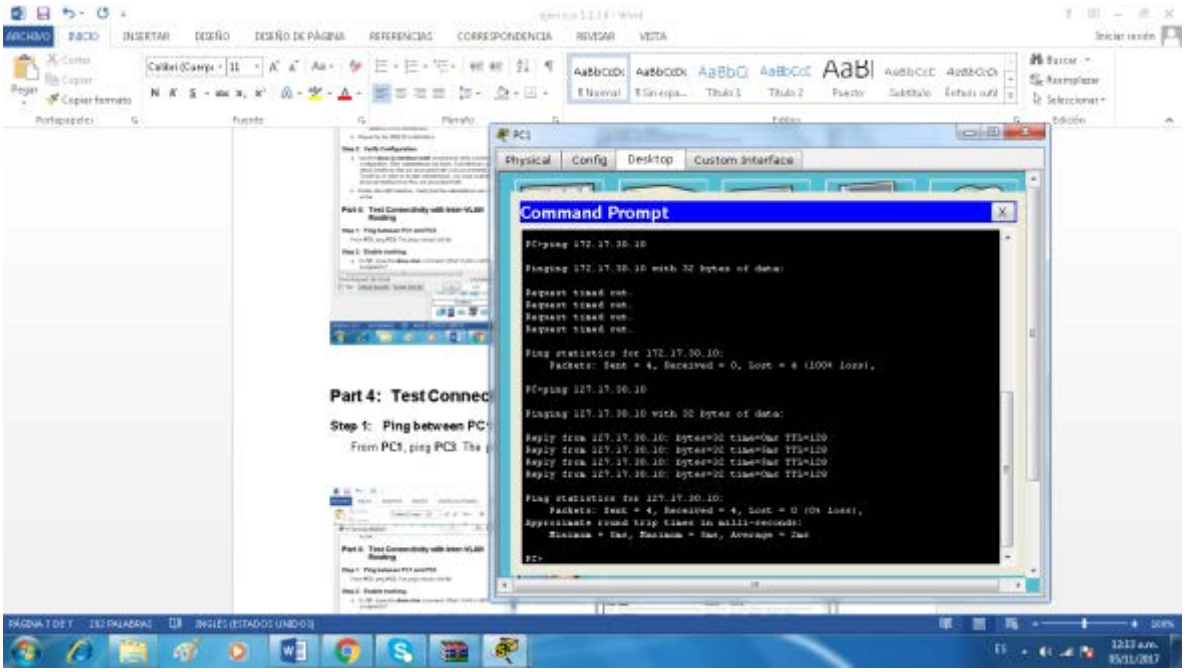
b. Enable the G0/0 interface. Verify that the subinterfaces are now active.



Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

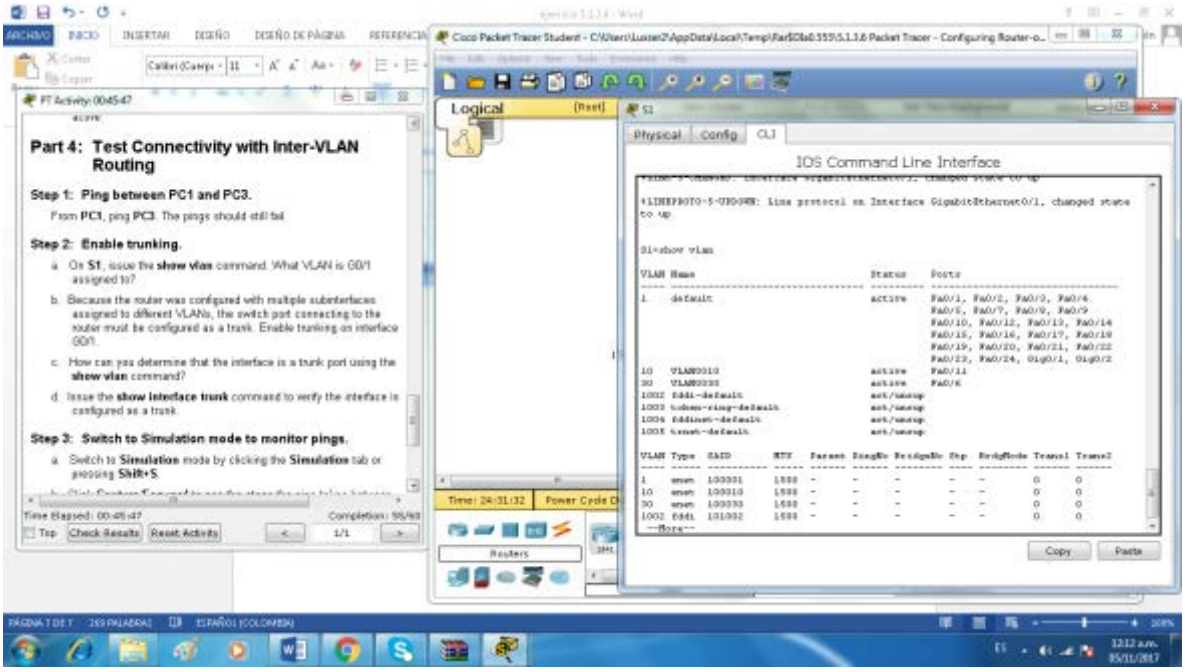
From **PC1**, ping **PC3**. The pings should still fail.

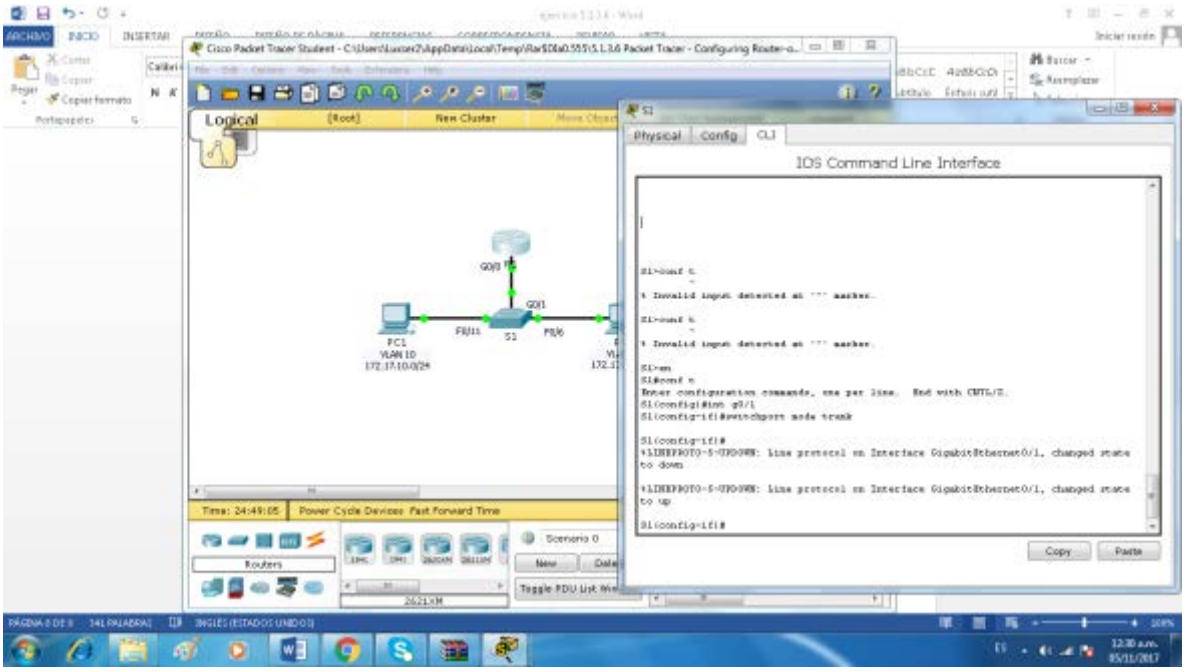


tep 2: Enable trunking.

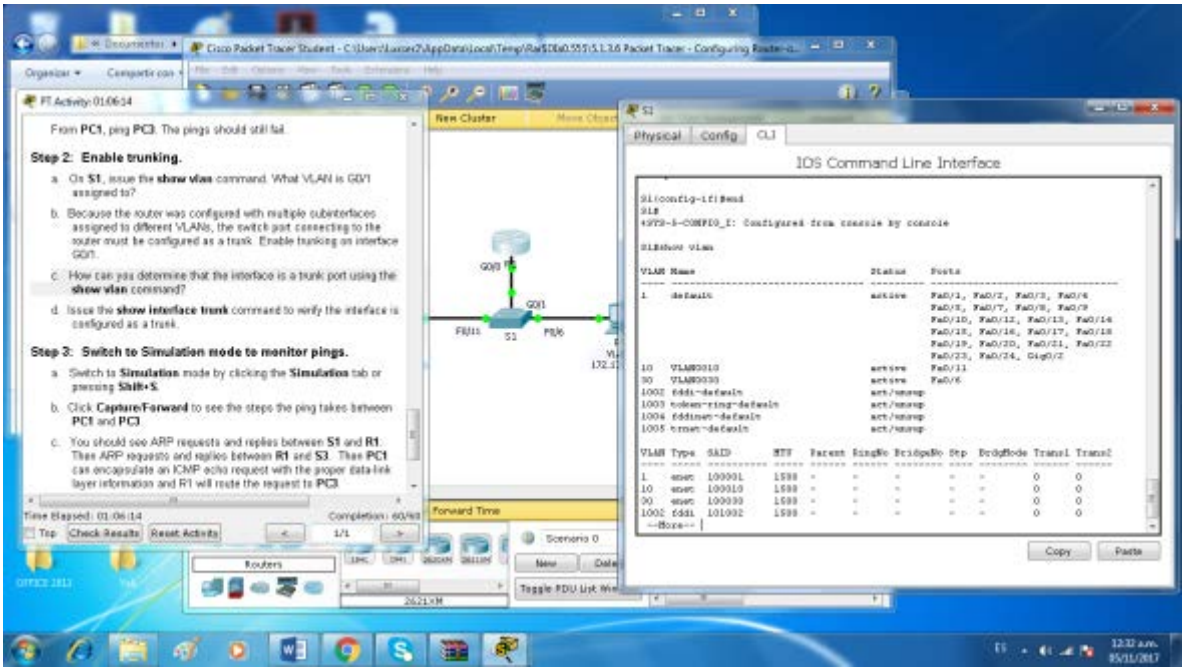
a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to?

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.

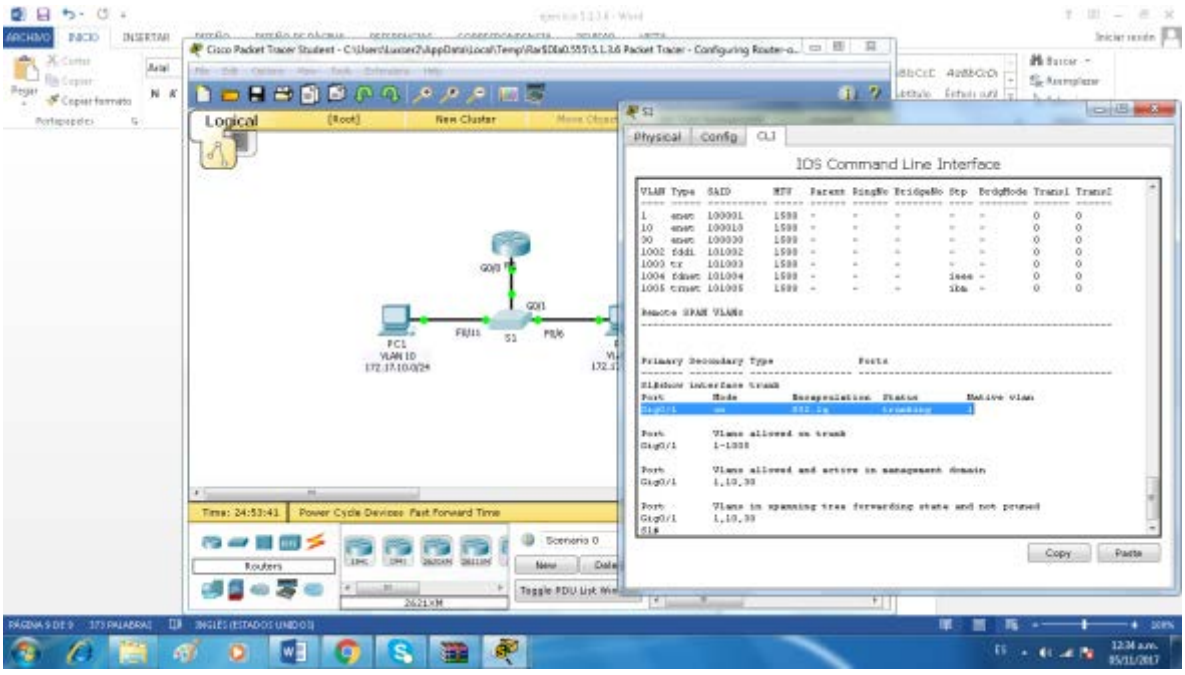


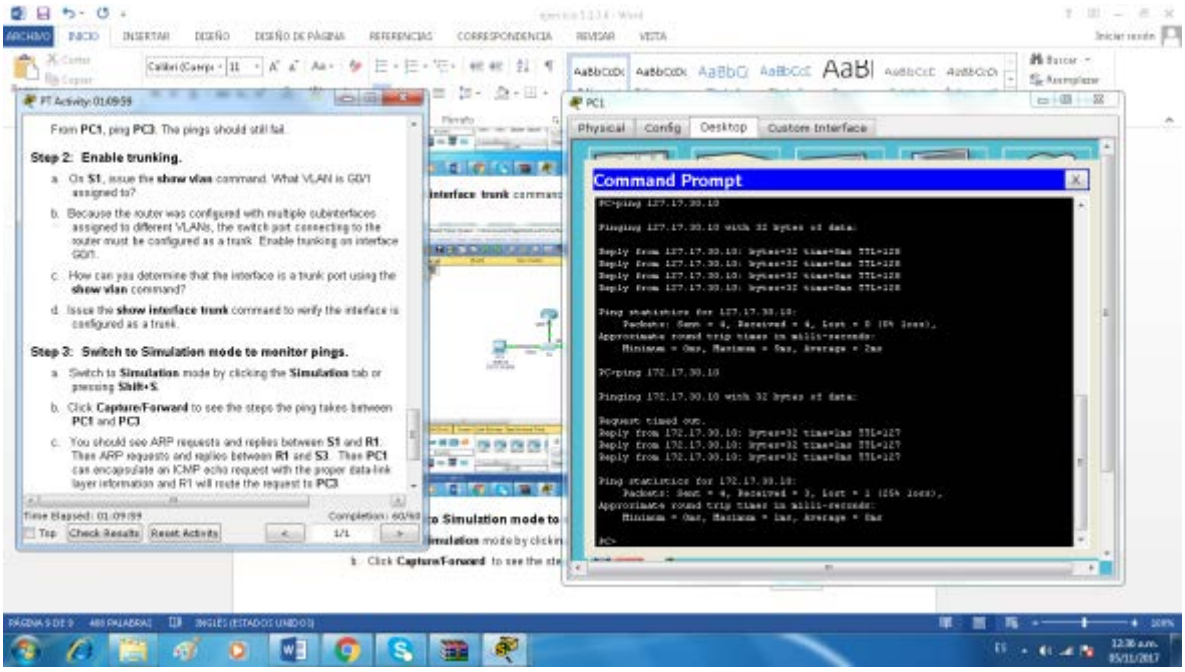


c. How can you determine that the interface is a trunk port using the**show vlan** command?



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

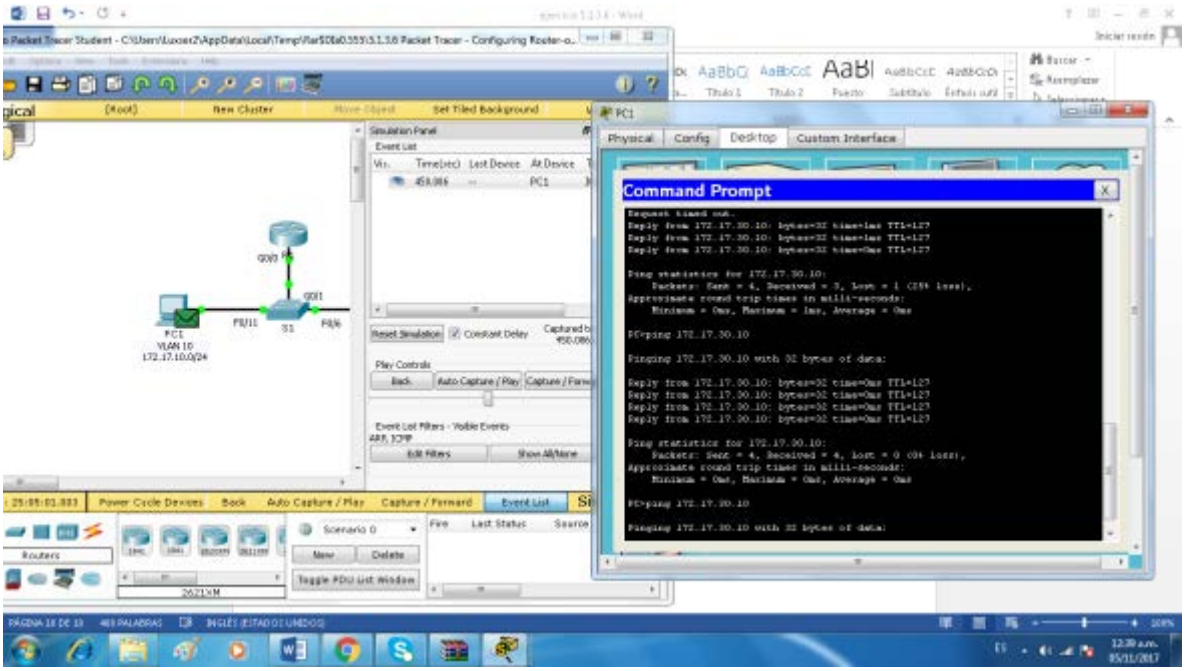


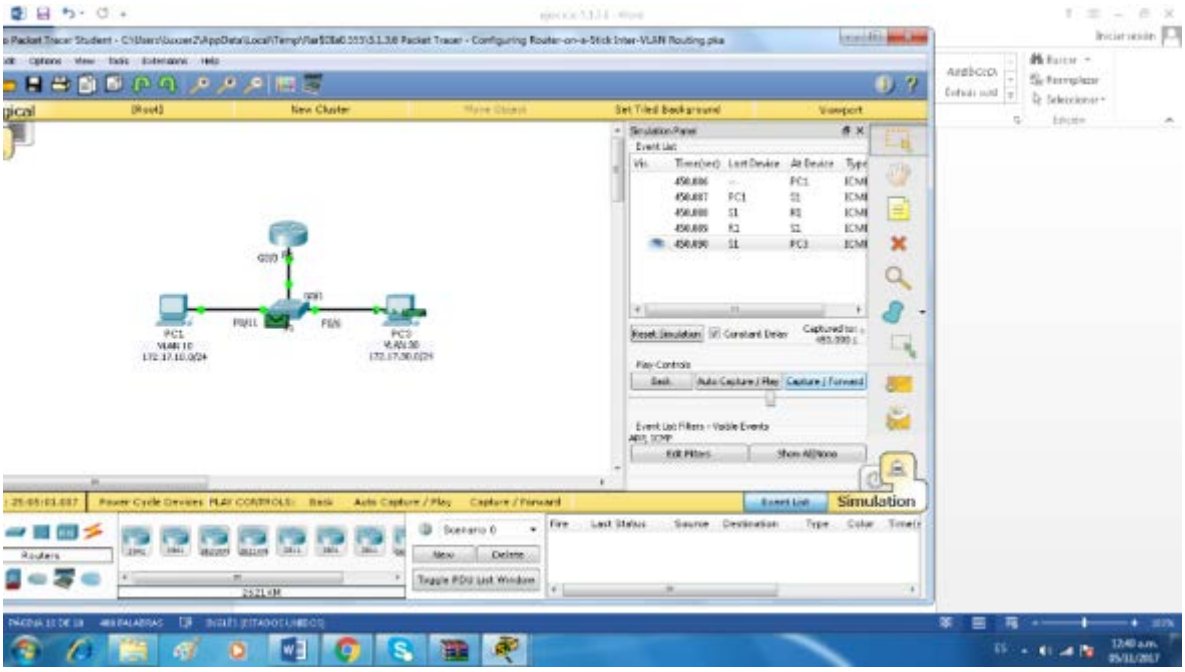


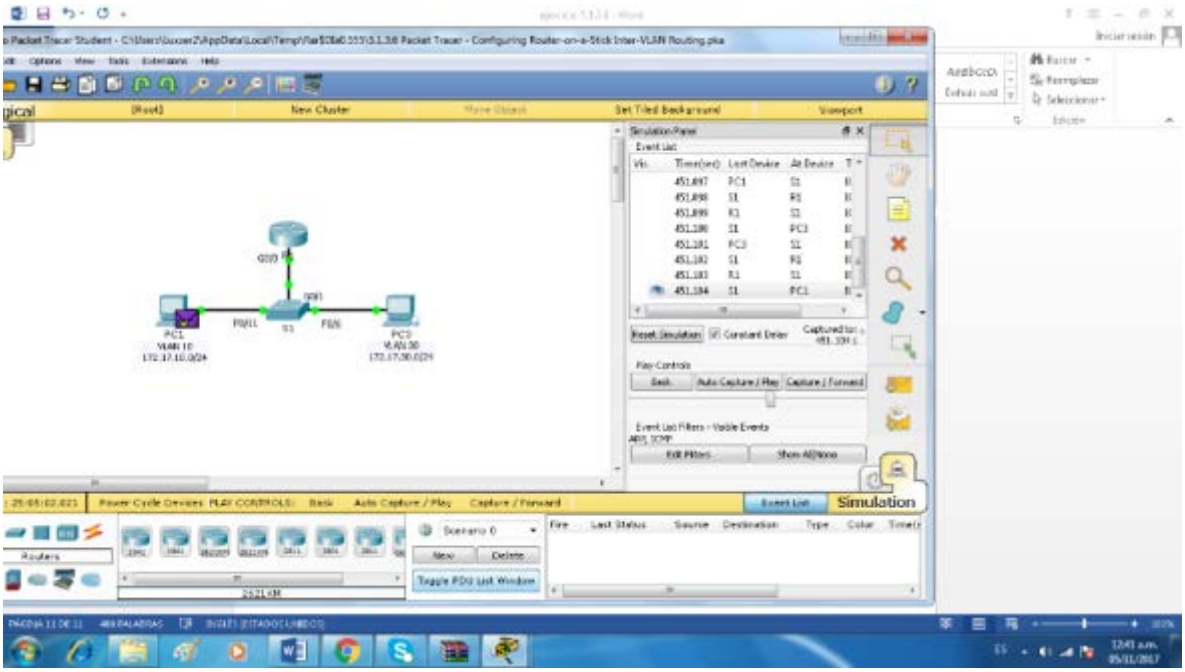
Step 3: Switch to Simulation mode to monitor pings.

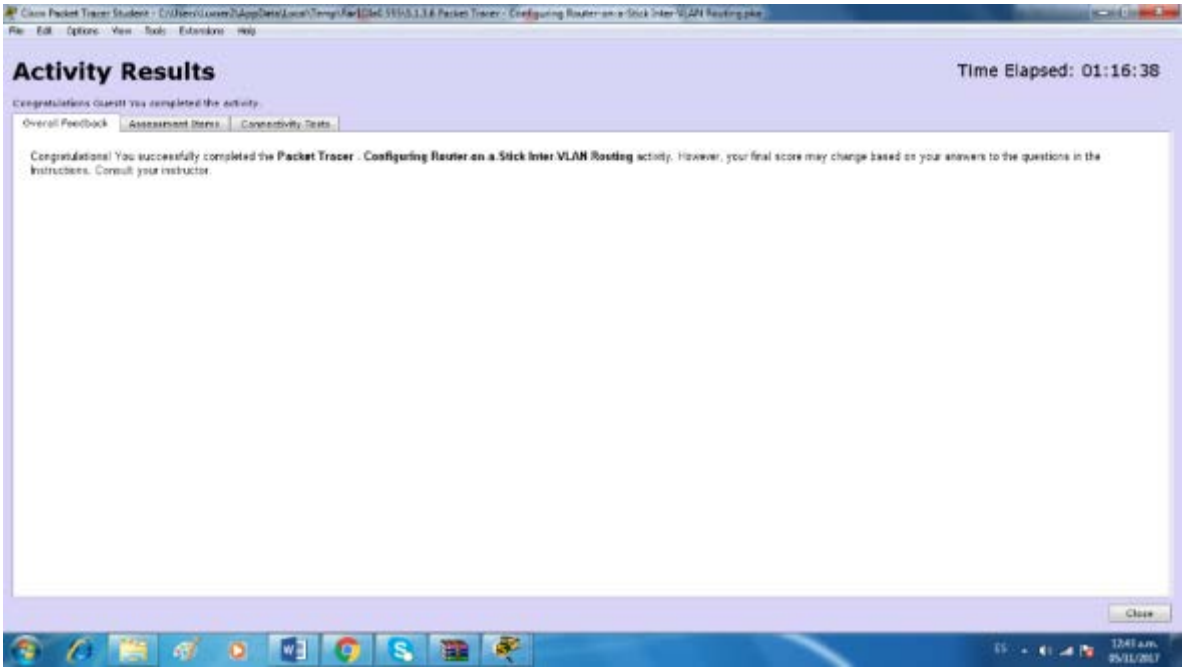
a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between**PC1** and **PC3**.








Activity Results
Time Elapsed: 01:16:38
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the Packet Tracer . Configuring Router on a Stick Inter VLAN Routing activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.
Close

5.1.3.7 Lab - Configuring 802.1Q Trunk-Based Inter-VLAN Routing

Topología

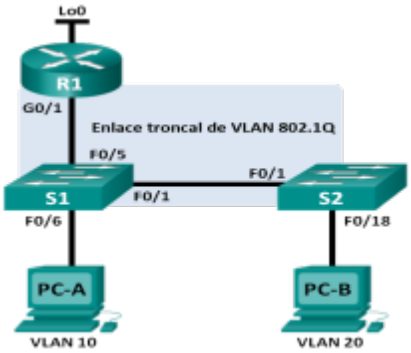


Tabla de direccionamiento

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

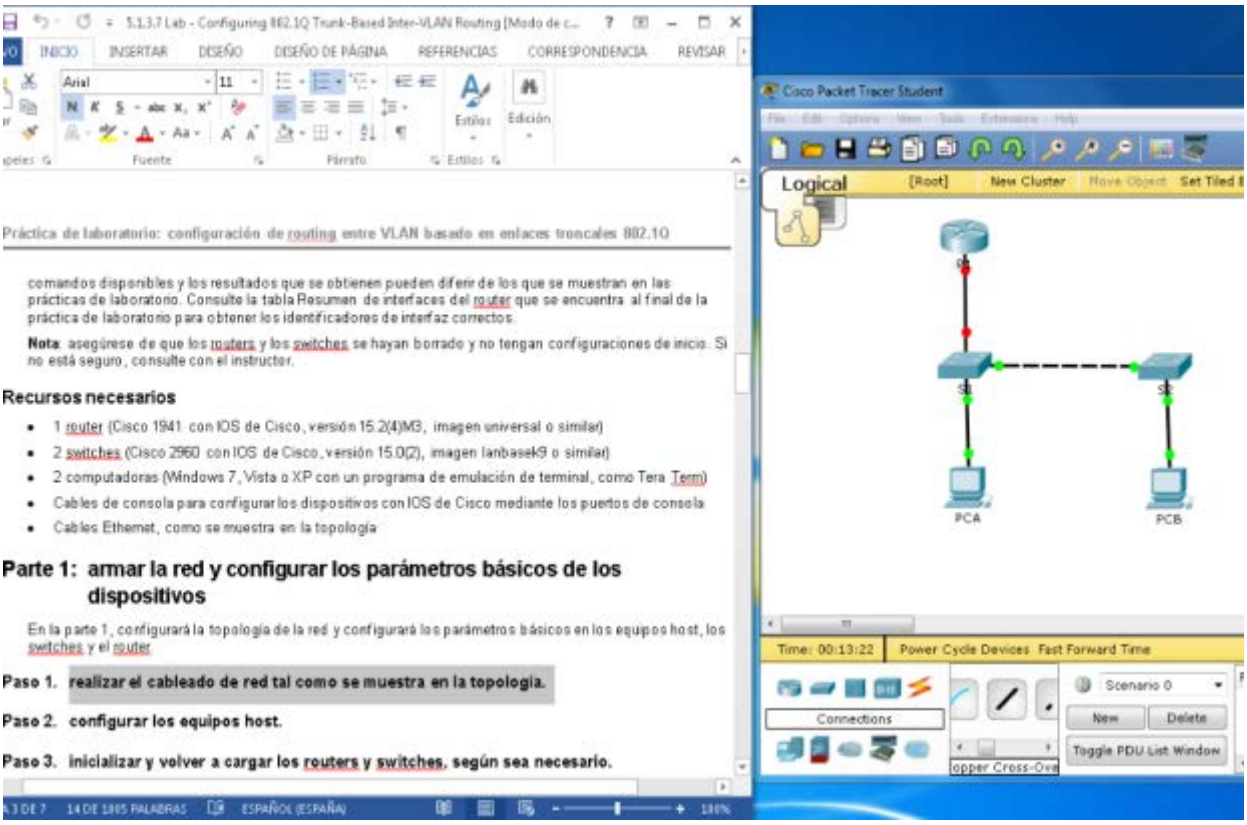
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

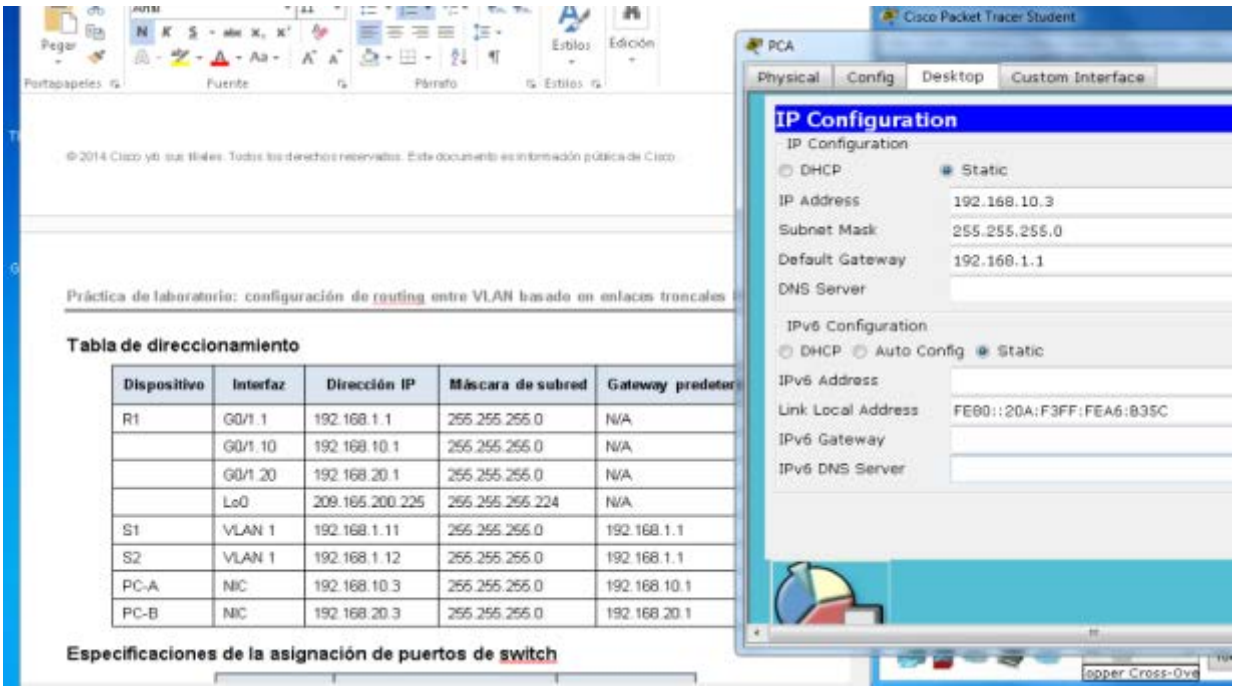
En la parte 1, configurará la topología de la red y configurará los parámetros básicos en los equipos host, los switches y el router.

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.





Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeter
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

Paso 4. configurar los parámetros básicos para cada switch.

i. Desactive la búsqueda del DNS.

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

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

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

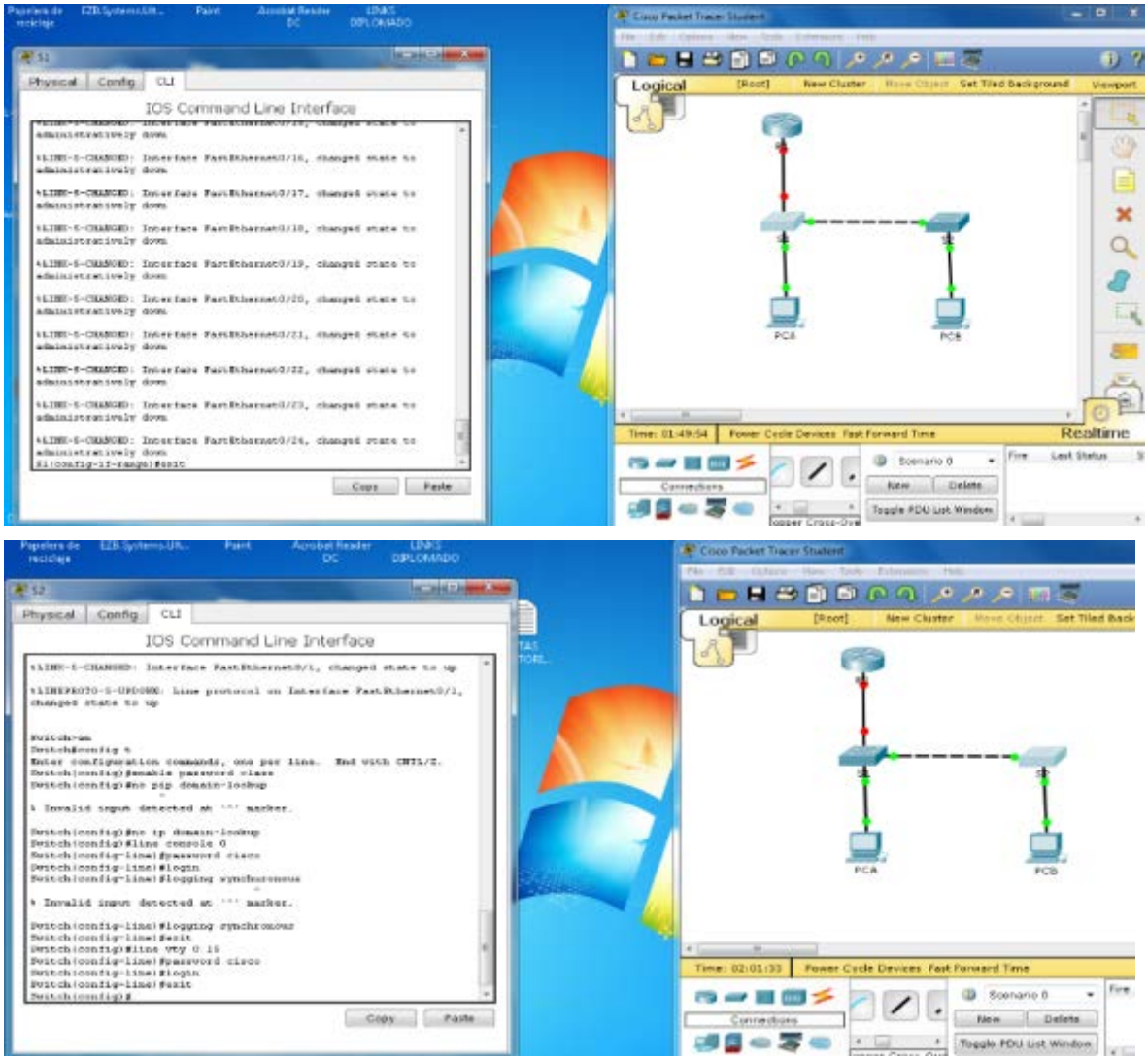
m. Configure **logging synchronous** para la línea de consola.

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

o. Configure el gateway predeterminado en los dos switches.

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

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



Paso 5. configurar los parámetros básicos para el router.

r. Desactive la búsqueda del DNS.

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

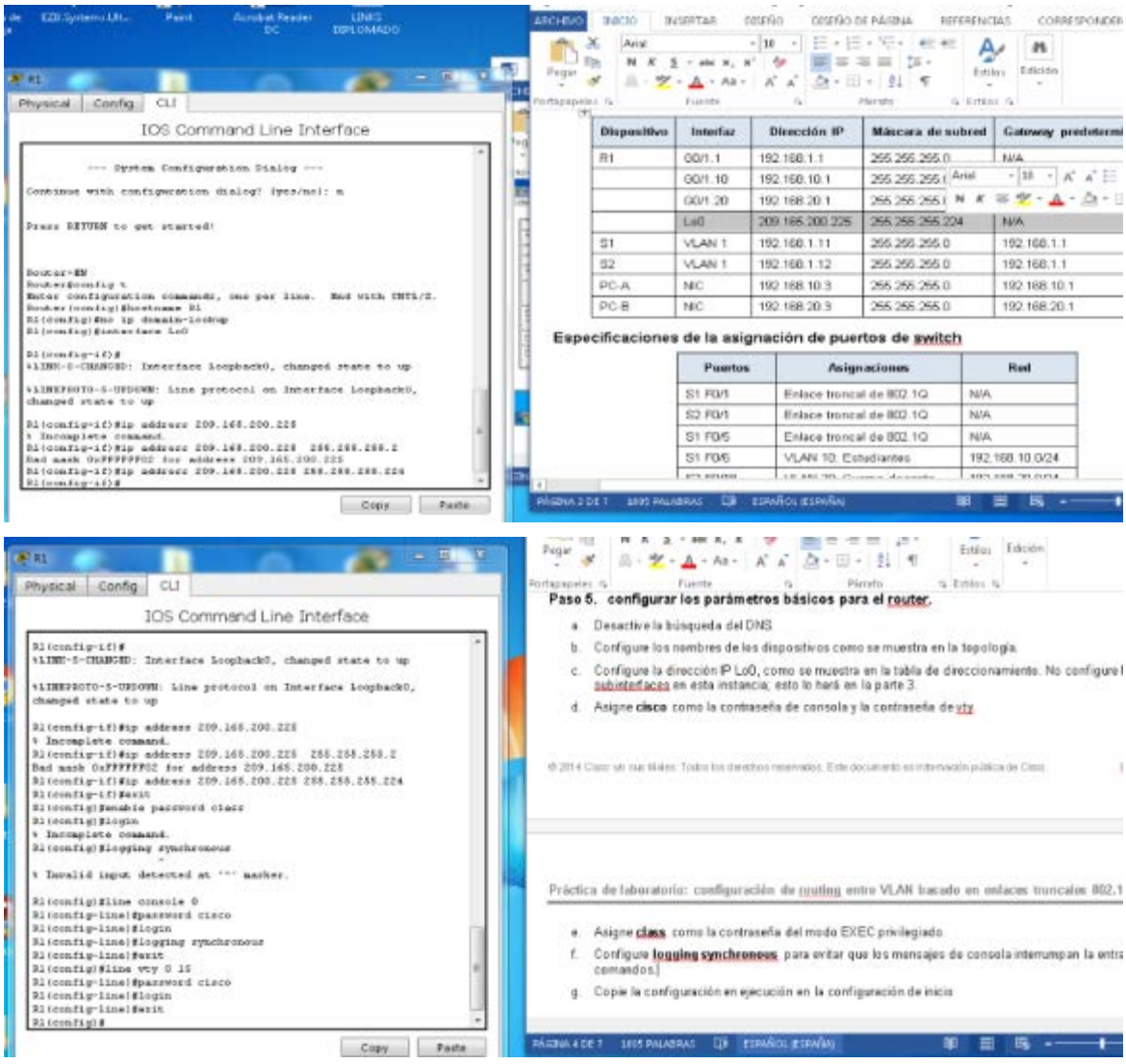
t. Configure la dirección IP Lo0, como se muestra en la tabla de direccionamiento. No configure las subinterfaces en esta instancia; esto lo hará en la parte 3.

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

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

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

x. 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.

y. 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.

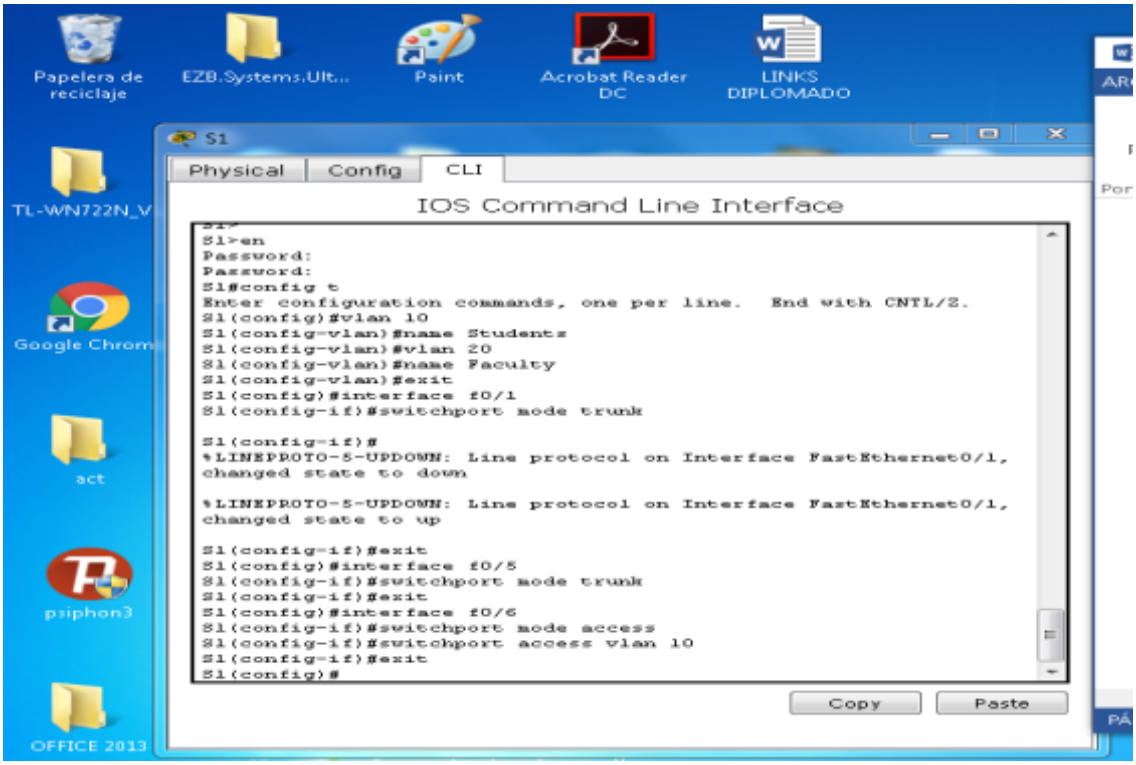
z. En el S1, configure la interfaz conectada al R1 como enlace troncal. También configure la interfaz conectada al S2 como enlace troncal. En el espacio proporcionado, escriba los comandos que utilizó.

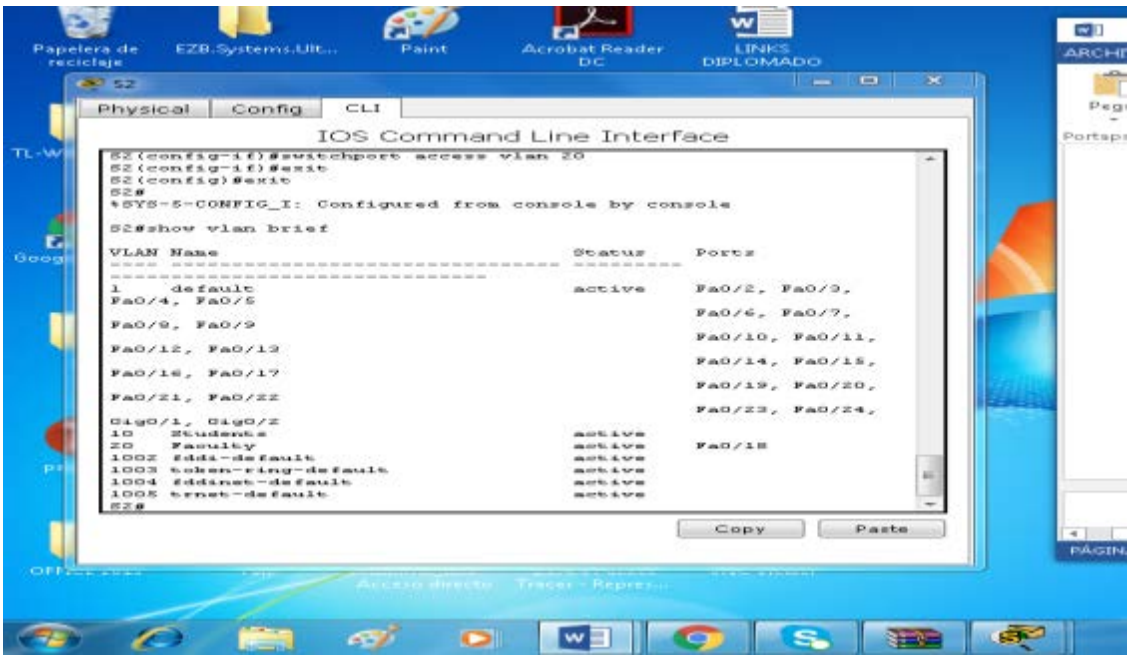
Part 16: S1(config)#vlan 10
Part 17: S1(config-vlan)#name Students
Part 18: S1(config-vlan)#vlan 20
Part 19: S1(config-vlan)#name Faculty
Part 20: S1(config-vlan)#exit
Part 21: S1(config)#interface f0/1
Part 22: S1(config-if)#switchport mode trunk

S1(config-if)#exit
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit

S1(config)#

a. 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.





Paso 2. configurar las VLAN en el switch 2.

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

c. 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.

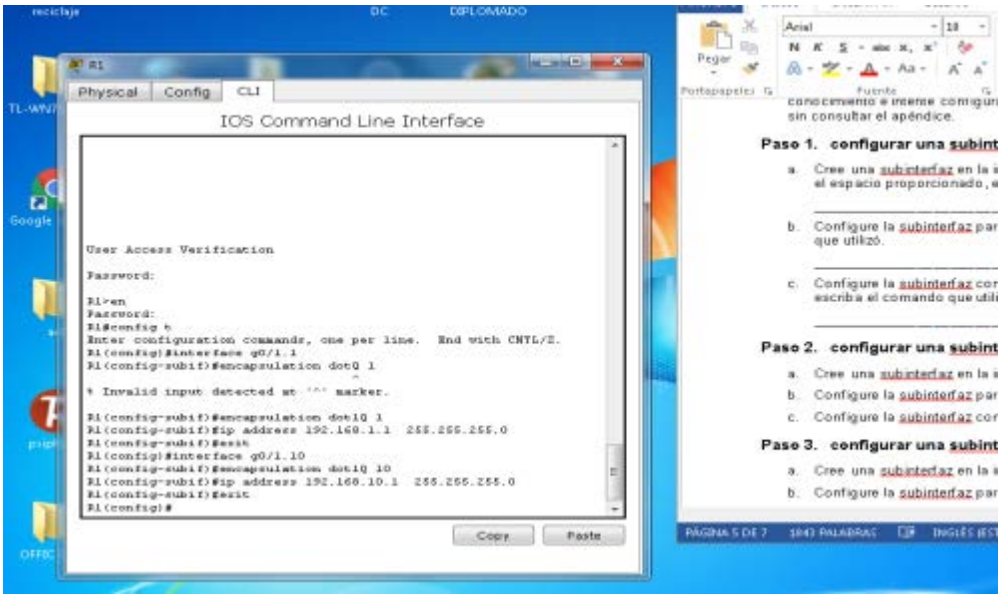
_____
_____

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

e. 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 1. configurar una subinterfaz para la VLAN 1.

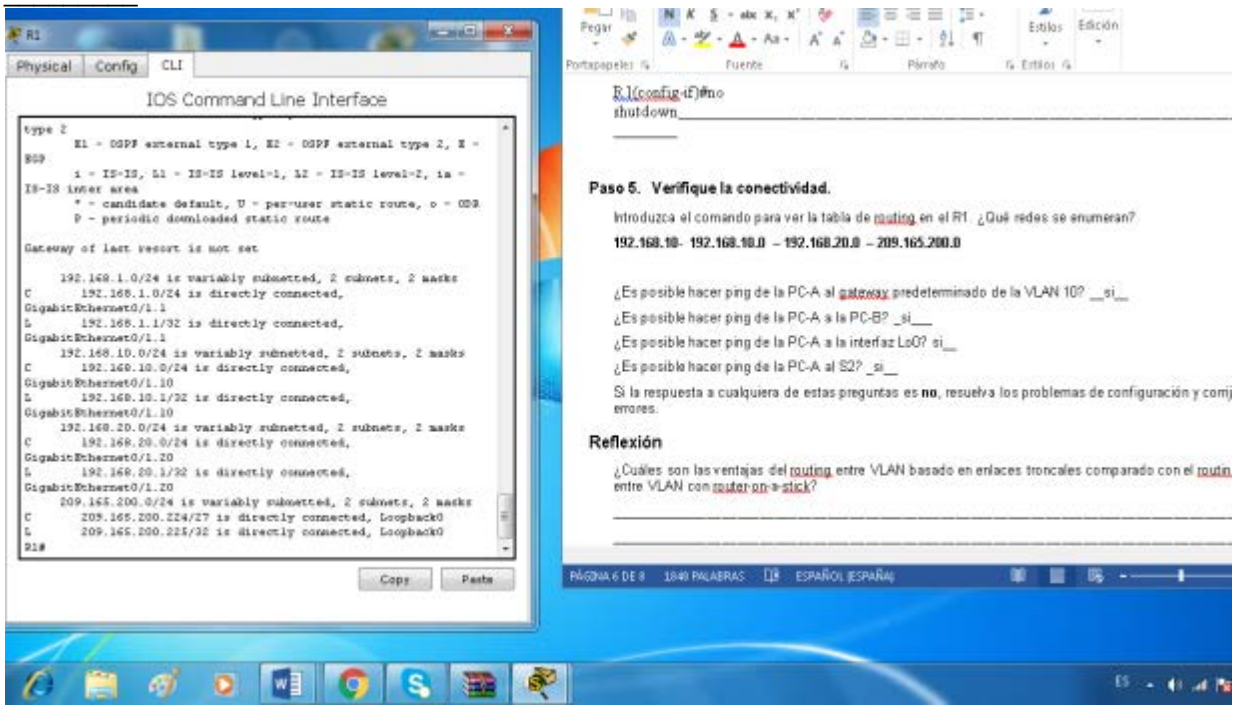
f. Cree una subinterfaz en la interfaz G0/1 del R1 para la VLAN 1 y use el 1 como ID de la subinterfaz. En el espacio proporcionado, escriba el comando que utilizó.

_____

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

_____

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



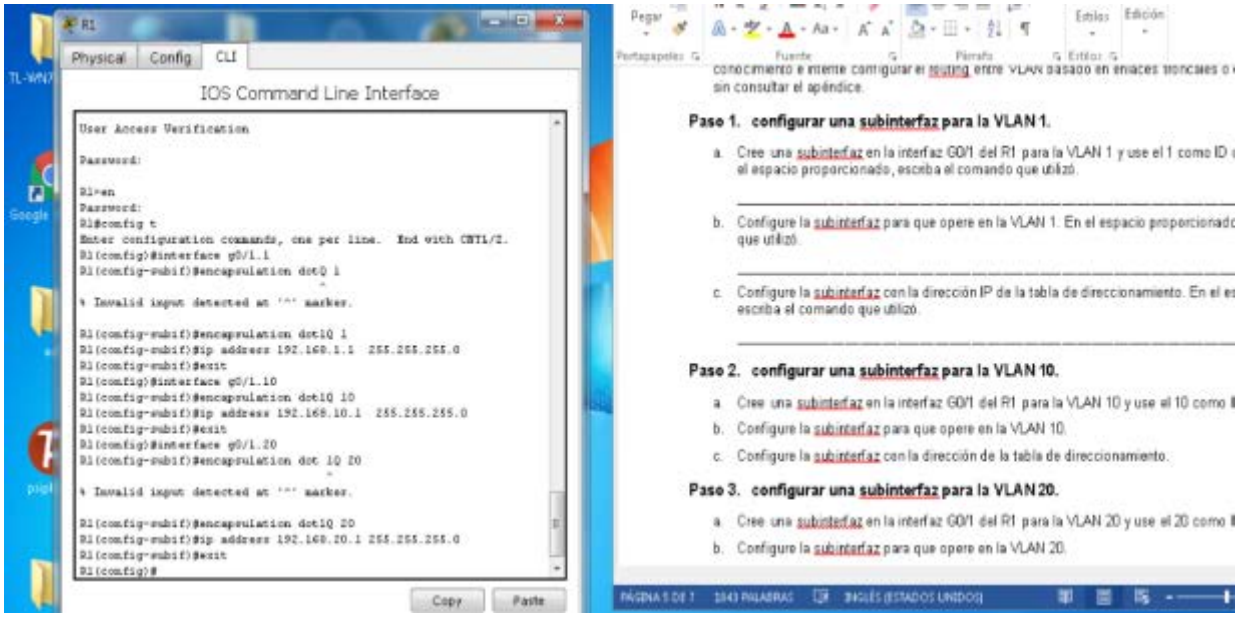
Paso 2. configurar una subinterfaz para la VLAN 10.

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

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

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

l.



Paso 3. configurar una subinterfaz para la VLAN 20.

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

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

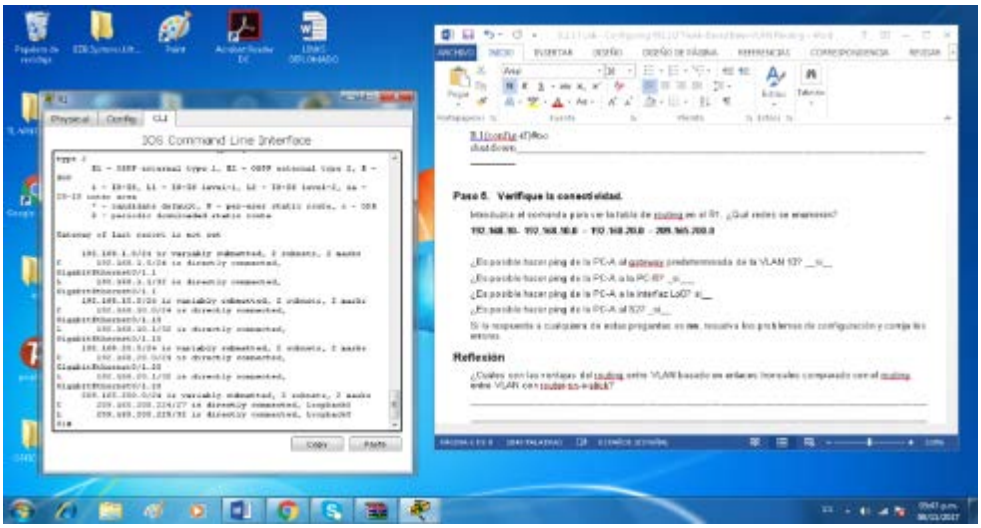
o. Configure la subinterfaz con la dirección de la tabla de direccionamiento.

Paso 4. habilitar la interfaz G0/1.

Habilite la interfaz G0/1. En el espacio proporcionado, escriba los comandos que utilizó.

R1(config)#interface g0/1

R1(config-if)#no shutdown_____



Paso 5. Verifique la conectividad.

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

192.168.10- 192.168.10.0 – 192.168.20.0 – 209.165.200.0

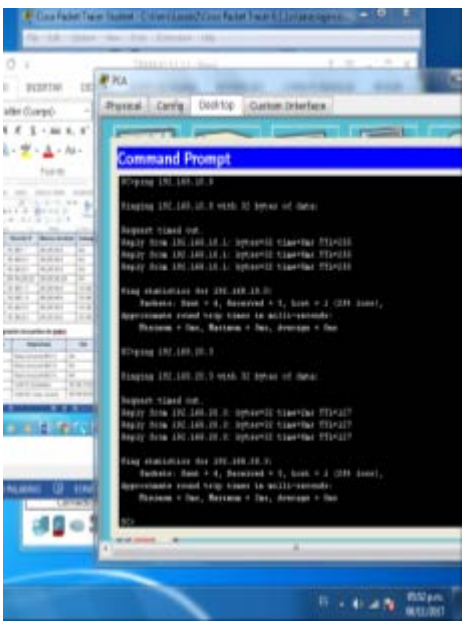
¿Es posible hacer ping de la PC-A al gateway predeterminado de la VLAN 10? __si__

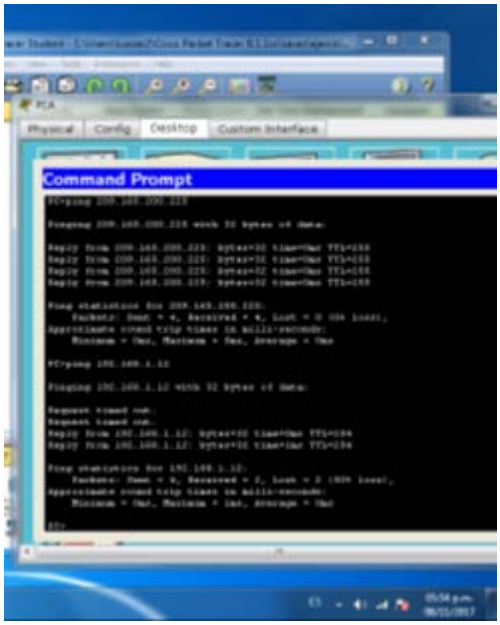
¿Es posible hacer ping de la PC-A a la PC-B? _si___

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

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

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





Reflexión

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

_El ruteo entre _permite que una sola interface pueda rutiar múltiples vlans distinto al ruteo entre el vlans con el método que requiere un puerto por vlan.

_____

Tabla de resumen de interfaces del router

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

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

Apéndice A: comandos de configuración

Switch S1

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

Switch S2

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

Router R1

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

6.2.2.5 Lab - Configuring IPv4 Static and Default Routes

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

Part 23: 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.

Part 24: configurar los parámetros básicos de los dispositivos y verificar la conectividad

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

Paso 1. Configure las interfaces de la PC.

Paso 2. configurar los parámetros básicos en los routers.

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

b. Desactive la búsqueda del DNS.

c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

Paso 3. configurar los parámetros IP en los routers.

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

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

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

Paso 4. verificar la conectividad de las LAN.

a. 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____

b. 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.

c. 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?

____porque no se está configurada la conexión entre estos dispositivos._____

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

Paso 5. reunir información.

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

¿Cuántas interfaces están activadas en el R1? ___2___

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

¿Cuántas interfaces están activadas en el R3? __4__

c. 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?**

192.168.1.1
209.165.200.225
198.133.219.1

_____

d. 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?

_____192.168.0.0_____

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

Porque los Routers solo conocen la red que se conectó directamente a ellos._____
_____

Part 25: 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.

_R1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2_____

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

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

_____
_____

¿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
```

a. 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.

_R3(config)#ip route 192.168.0.0 255.255.255.0 s0/1/0_____

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

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

_____
_____

c. ¿Es posible hacer ping del host PC-A host a al host PC-C? si

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.

a. 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.

R1(config)#ip route 198.133.219.0 255.255.255.0 10.1.1.2

R1(config)#ip route 198.133.219.0 255.255.255.0 s0/1/0

_____

b. 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.

_____ R1(config)#ip route 209.165.200.224 255.255.255.224 s0/1/0_____

R1(config)#ip route 209.165.200.224 255.255.255.224 10.1.1.2

c. 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?

_____
_____

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

Este ping debe tener éxito.

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

a. 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.

_____
_____

b. 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? _____

¿El gateway de último recurso está establecido? _____

Part 26: 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?

_____
_____

¿Cuál es el gateway de último recurso?

_____
_____

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

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

Estos pings deben tener éxito.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

Apéndice A: comandos de configuración para las partes 2, 3 y 4

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

Configuración básica de los dispositivos

Configure los parámetros IP en el router.

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

Configuraciones de rutas estáticas

Configure una ruta estática recursiva.

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

Configure una ruta estática conectada directamente.

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

Elimine las rutas estáticas.

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

o

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

o

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

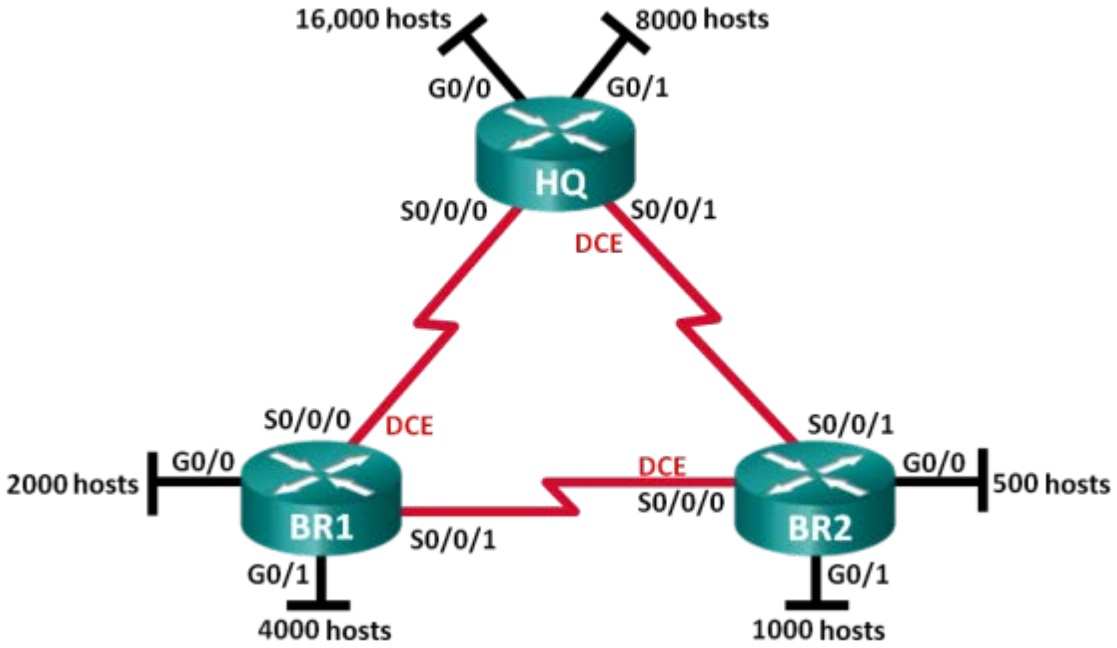
Configuración de rutas predeterminadas

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

6.3.3.7 Lab - Designing and Implementing IPv4 Addressing with VLSM

Práctica de laboratorio: diseño e implementación de direccionamiento IPv4 con VLSM

Topología



Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direcciones VLSM

Parte 3: realizar el cableado y configurar la red IPv4

Información básica/situación

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

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

diseñar el esquema de direcciones VLSM, configurará las interfaces en los routers con la información de dirección IP adecuada.

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

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

Recursos necesarios

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

Parte 1: examinar los requisitos de la red

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

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

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

¿Cuántas direcciones host se encuentran disponibles en una red /17? _32768__

¿Cuál es la cantidad total de direcciones host que se necesitan en el diagrama de la topología? _31512__

¿Cuántas subredes se necesitan en la topología de la red? _10_____

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) __172.16.254.4___

¿Cuántas direcciones IP se necesitan en la subred más grande? _16000__

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones? _16384__

¿Cuántas direcciones host admite esa subred? __16382_____

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

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

___172.16.192.0/19 Y 172.16.224.0/20_____

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred ___172.16.192.0/19____

¿Cuántas direcciones IP se necesitan para la segunda subred más grande? _8000__

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?__8192__

¿Cuántas direcciones host admite esa subred? __8190___

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

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

__172.16.224.0/20____

___172.16.240.0/21__

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred__172.16.224.0/20_____

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? _4000__

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?__4096____

¿Cuántas direcciones host admite esa subred? __4094_____

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

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

____172.16.240.0/21____

____172.16.248.0/22_____

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred _____172.16.240.0/21_____

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? _2000___

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?___2048___

¿Cuántas direcciones host admite esa subred? ___2046_____

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

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

___172.16.248.0/22_____

___172.16.252.0/23_____

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred _172.16.248.0/22____

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? _1000__

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?____1024____

¿Cuántas direcciones host admite esa subred? ____1022_____

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

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

__172.16.252.0/23_____

_____

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred ___172.16.252.0/23_____

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? _500__

¿Cuál es la subred más pequeña que admite esa cantidad de hosts?__512

_____

¿Cuántas direcciones host admite esa subred? __510_____

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

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

____172.16.254.0/30_____

____172.16.254.4/30_____

Utilice la primera dirección de red para esta subred.

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

¿Cuántas direcciones host se necesitan para cada enlace de subred serial? __2____

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones host?

_____172.16.254.8 /30_____

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

__172.16.254.0_____

__172.16.254.4_____

__172.16.254.8_____

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

__172.16.254.12_____

__172.16.254.16_____

__172.16.254.20_____

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

___172.16.254.12/30___255.255.255.252___172.16.254.13___172.16.254.14__172.16.254.15___

__172.16.254.16/30___255.255.255.252___172.16.254.17___172.16.254.18__172.16.254.19____

__172.16.254.20/30__255.255.255.252___172.16.254.21___172.16.254.22__172.16.254.23__

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	172.16.128.1	172.16.191.255
HQ G0/1	8 000	172.16.192.0	172.16.192.1	172.16.223.255
BR1 G0/1	4 000	172.16.224.0	172.16.224.1	172.16.239.255
BR1 G0/0	2 000	172.16.240.0	172.16.240.1	172.16.247.255
BR2 G0/1	1.000	172.16.248.0	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0	172.16.252.1	172.16.253.255
HQ S0/0/0-BR1 S0/0/0	2	172.16.254.0	172.16.254.1	172.16.254.3
HQ S0/0/1-BR2 S0/0/1	2	172.16.254.4	172.16.254.5	172.16.254.7
BR1 S0/0/1-BR2 S0/0/0	2	172.16.254.8	172.16.254.9	172.16.254.11

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

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

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

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

Parte 3: realizar el cableado y configurar la red IPv4

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

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

Paso 2. configurar los parámetros básicos en cada router.

a. Asigne el nombre de dispositivo al router.

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

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

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

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

f. Cifre las contraseñas de texto no cifrado.

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

Paso 3. configurar las interfaces en cada router.

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

i. Configure una descripción de interfaz para cada interfaz.

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

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

k. Active las interfaces.

Paso 4. guardar la configuración en todos los dispositivos.

Paso 5. Probar la conectividad

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

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

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

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

Nota: los pings a las interfaces GigabitEthernet en otros routers no son correctos. Las LAN definidas para las interfaces GigabitEthernet son simuladas. Debido a que no hay ningún dispositivo conectado a estas LAN, están en estado down/down. Debe haber un protocolo de routing para que otros dispositivos detecten esas subredes. Las interfaces de GigabitEthernet también deben estar en estado up/up para que un protocolo de routing pueda agregar las subredes a la tabla de routing. Estas interfaces permanecen en el estado down/down hasta que

se conecta un dispositivo al otro extremo del cable de interfaz Ethernet. Esta práctica de laboratorio se centra en VLSM y en la configuración de interfaces.

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

6.4.2.5 Lab - Calculating Summary Routes with IPv4 and IPv6

Práctica de laboratorio: cálculo de rutas resumidas IPv4 e IPv6

Topología

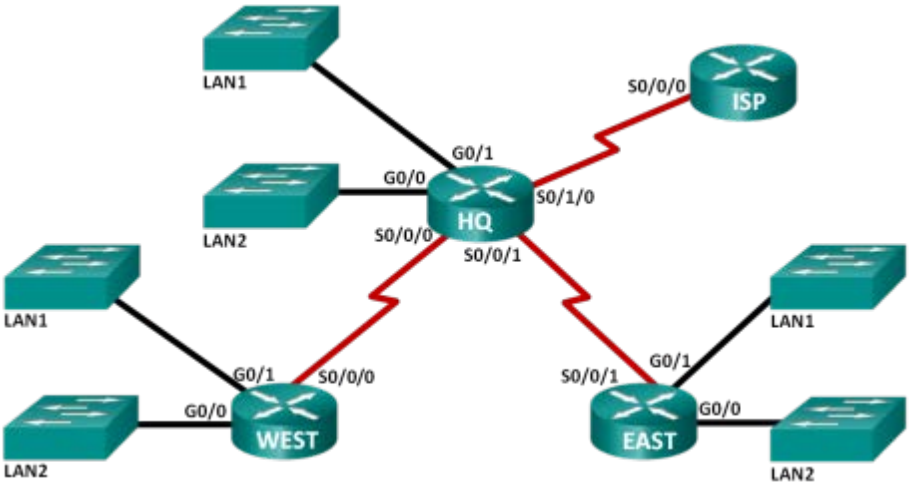


Tabla de direccionamiento

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

Objetivos

Parte 1: calcular rutas resumidas IPv4

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

Parte 2: calcular rutas resumidas IPv6

- Determinar la ruta resumida para las LAN de HQ.

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

Información básica/situación

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

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

Recursos necesarios

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

Part 27: calcular rutas resumidas IPv4

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

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

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

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

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

b. Indique la máscara de subred para la ruta resumida en formato decimal. 255.255.252.0

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

Indique los bits binarios coincidentes de las subredes de la LAN1 de HQ y la LAN2 de HQ.
11000000.10101000.010000**00**.00000000

11000000.10101000.010000**10**.00000000

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

11000000.10101000.01000000.00000000

d. Indique las direcciones de red resumidas en formato decimal. **192.168.64.0/ 22**

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de HQ	192.168.64.0	255.255.254.0	11000000.10101000.0100000**0**.00000000
LAN2 de HQ	192.168.66.0	255.255.254.0	11000000.10101000.0100001**0**.00000000
Dirección de resumen de las LAN de HQ	192.168.64.0	255.255.252.0	11000000.10101000.01000000.00000000

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

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

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

e. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes?
___23_____

f. Indique la máscara de subred para la ruta resumida en formato decimal. 255.255.254.0

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

g. Indique los bits binarios coincidentes de las subredes de la LAN1 ESTE y la LAN2 ESTE.
11000000.10101000.0100010**0**.00000000
11000000.10101000.0100010**1**.00000000

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

i. 11000000.10101000.01000100.00000000

j. Indique las direcciones de red resumidas en formato decimal. **192.168.68.0/23**

Subred	Dirección IPv4	Máscara de subred	Dirección de subred en formato binario
LAN1 de EAST	192.168.68.0	255.255.255.0	11000000.10101000.0100010**0**.00000000
LAN2 de EAST	192.168.69.0	255.255.255.0	11000000.10101000.0100010**1**.00000000
Dirección de resumen de las LAN ESTE	192.168.68.0	255.255.254.0	11000000.10101000.01000100.00000000

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

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

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

k. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? **__24_____**

l. Indique la máscara de subred para la ruta resumida en formato decimal. **255.255.255.0**

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

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

11000000.10101000.01000110.00000000

11000000.10101000.01000110.10000000

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

11000000.10101000.01000110.00000000

o. Indique las direcciones de red resumidas en formato decimal. |192.168.70.0/ 24

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de WEST	192.168.70.0	255.255.255.128	11000000.10101000.01000110.00000000
LAN2 de WEST	192.168.70.128	255.255.255.128	11000000.10101000.01000110.10000000
Dirección de resumen de las LAN OESTE	192.168.70.0	255.255.255.0	11000000.10101000.01000110.00000000

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

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

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

p. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres redes? **___21_____**

q. Indique la máscara de subred para la ruta resumida en formato decimal. 255.255.248.0

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

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

11000000.10101000.01000000.00000000

11000000.10101000.01000100.00000000

11000000.10101000.01000110.00000000

s. Agregue ceros para conformar el resto de la dirección de red en formato binario.
11000000.10101000.01000000.00000000

t. Indique las direcciones de red resumidas en formato decimal. 192.168.64.0 /21

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

Part 28: calcular rutas resumidas IPv6

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

Topología

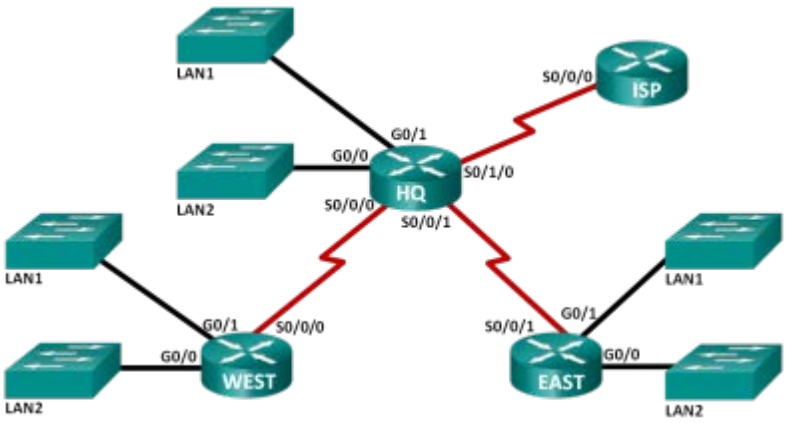


Tabla de direccionamiento

Subred	Dirección IPv6
LAN1 de HQ	2001:DB8:ACAD:E::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64
LAN1 de EAST	2001:DB8:ACAD:1::/64
LAN2 de EAST	2001:DB8:ACAD:2::/64
LAN1 de WEST	2001:DB8:ACAD:9::/64

LAN2 de WEST	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	2001:DB8:CC1E:1::/64

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

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

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

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

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

2001 : 0DB8 : ACAD : 0000 0000 0000 1110::/64

16 + 16 + 16 + 4 + 4 + 4 + 3 =/63

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

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

2001:0DB8:ACAD: 0000 0000 0000 1110::/64

2001:0DB8:ACAD: 0000 0000 0000 1111::/64

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

2001:0DB8:ACAD: 0000 0000 0000 1110::/63

Indique las direcciones de red resumidas en formato decimal.

2001:0DB8:ACAD: E::/63

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	/64	2001:0DB8:ACAD:0000:0000:0000:1110::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64	/64	2001:0DB8:ACAD:0000:0000:0000:1111::/64
Dirección de resumen de las LAN de HQ	**2001:0DB8:ACAD: E::/63**	/63	2001:0DB8:ACAD:0000:0000:0000:1110::/63

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

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

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

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

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

2001 : 0DB8 : ACAD : 0000 0000 0000 0000::/64

16 + 16 + 16 + 4 + 4 + 4 + 2 =/62

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

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

f. 2001:0DB8:ACAD:0000:0000:0000:0001::/64

2001:0DB8:ACAD:0000:0000:0000:0010::/64

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

2001:0DB8:ACAD:0000:0000:0000:0000::/62

Indique las direcciones de red resumidas en formato decimal.

2001:0DB8:ACAD: 0::/62

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	/64	**2001:0DB8:ACAD:0000:0000:0000:0001::/64**
LAN2 de EAST	2001:DB8:ACAD:2::/64	/64	**2001:0DB8:ACAD:0000:0000:0000:0010::/64**
Dirección de resumen de las LAN ESTE	**2001:0DB8:ACAD:0::/62**	/62	**2001:0DB8:ACAD:0000:0000:0000:0000::/62**

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

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

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

g. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred?
__62___

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

2001 : 0DB8 : ACAD : 0000 0000 0000 1000::/64

16 + 16 + 16 + 4 + 4 + 4 + 2 =/62

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

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

2001:0DB8:ACAD:0000:0000:0000:1001::/64

2001:0DB8:ACAD:0000:0000:0000:1010::/64

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

2001:0DB8:ACAD:0000:0000:0000:1000::/62

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

2001:0DB8:ACAD:8::/62

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	/64	**2001:0DB8:ACAD:0000:0000:0000:**1001::/64
LAN2 de WEST	2001:DB8:ACAD:A::/64	/64	**2001:0DB8:ACAD:0000:0000:0000:10****10::/64**
Dirección de resumen de las LAN OESTE	**2001:0DB8:ACAD:8::/62**	**/62**	**2001:0DB8:ACAD:0000:0000:0000:1000::/64**

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

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

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

j. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres ID de subred?
__60__

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

2001 : 0DB8 : ACAD : 0000 0000 0000 0000::/64

16 + 16 + 16 + 4 + 4 + 4 + 0 =/60

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

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

2001:0DB8:ACAD: 0000 0000 0000 1110::/63

2001:0DB8:ACAD:0000:0000:0000:0000::/62

2001:0DB8:ACAD:0000:0000:0000:1000::/62

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

2001:0DB8:ACAD:0000:0000:0000:0000::/60

Indique las direcciones de red resumidas en formato decimal.

2001:0DB8:ACAD:0::/60

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
HQ	**2001:0DB8:ACAD: E::/63**	/63	**2001:0DB8:ACAD: 0000 0000 0000 1110::/63**
EAST	**2001:0DB8:ACAD:0::/62**	/62	**2001:0DB8:ACAD:0000:0000:0000:0000::/62**
WEST	**2001:0DB8:ACAD:8::/62**	/60	**2001:0DB8:ACAD:0000:0000:0000:1000::/62**
Ruta resumida de la dirección de red	**2001:0DB8:ACAD:0::/60**	/60	**2001:0DB8:ACAD:0000:0000:0000:0000::/60**

Reflexión

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

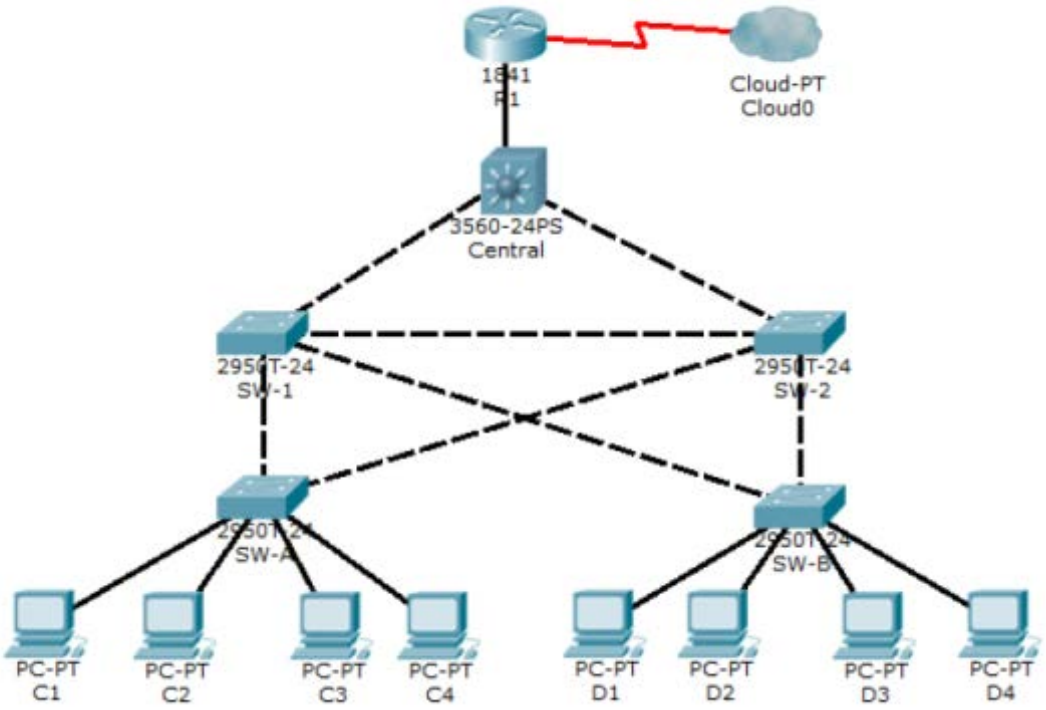
   ___LA DIFERENCIA ESTA EN QUE PARA IPV4 HAY QUE PASAR DE DECIMAL A BINARIO CON 32 BITS Y EN IPV6 HAY QUE PASAR DE EXADECIMAL A BINARIO EN 128 bits_____

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

   _ 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, ESTO NOS DA MAYOR RENDIMIENTO EN LA TRANSFERENCIA DE INFORMACIÓN POR LA RED _____

6.5.1.2 Packet Tracer - Layer 2 Security_

Topology



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:

o Enable password: **ciscoenpa55**

o Console password: **ciscoconpa55**

o VTY line password: **ciscovtypa55**

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.

Which switch is the current root bridge? Sw-1

```
SW-1#sh sp
SW-1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C61.9058
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0009.7C61.9058
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
---------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Gi0/1            Desg FWD 4         128.25   P2p

SW-1#
```

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

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)#spa
Central(config)#spanning-tree v
Central(config)#spanning-tree vlan 1 roo pr
Central(config)#spanning-tree vlan 1 roo 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(config)#
SW-1(config)#
SW-1(config)#
SW-1(config)#
SW-1(config)#
SW-1(config)#spanning-tree vlan 1 root sec
SW-1(config)#spanning-tree vlan 1 root secondary
```

Step 4: Verify the spanning-tree configuration.

Issue the **show spanning-tree** command to verify that **Central** is the root bridge.
Which switch is the current root bridge?

```
Central(config)#do sh sp
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
---------------- ---- --- --------- --------
--------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
Fa0/1            Desg FWD 19        128.1    P2p

Central(config)#
```

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.

```
SW-A(config)#inter range fast 0/1 - 4
SW-A(config-if-range)#sa
SW-A(config-if-range)#sp
SW-A(config-if-range)#span
SW-A(config-if-range)#spanning-tree po
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 has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-A(config-if-range)#
```

```
SW-B(config)#inter range f 0/1 - 4
SW-B(config-if-range)#spa
SW-B(config-if-range)#spanning-tree port
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 has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%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 has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-B(config-if-range)#
```

Step 2: Enable BPDU guard on all access ports.

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.

```
SW-A(config-if-range)#spanning-tree  bp
SW-A(config-if-range)#spanning-tree  bpduguard e
SW-A(config-if-range)#spanning-tree  bpduguard enable
SW-A(config-if-range)#
```

```
SW-B(config-if-range)#spanning-tree bp
SW-B(config-if-range)#spanning-tree bpduguard en
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 enable** command 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.

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.

On **SW-1**, enable root guard on ports Fa0/23 and Fa0/24. On **SW-2**, enable root guard on ports Fa0/23 and Fa0/24.

```
SW-1(config)#inter range fa0/23 - 24
SW-1(config-if-range)#spa
SW-1(config-if-range)#spanning-tree guard root
SW-1(config-if-range)#
SW-1(config-if-range)#
```

```
SW-2(config)#inter range fa0/23 - 24
SW-2(config-if-range)#sp
SW-2(config-if-range)#spa
SW-2(config-if-range)#spanning-tree go
SW-2(config-if-range)#spanning-tree gu
SW-2(config-if-range)#spanning-tree guard root
SW-2(config-if-range)#
SW-2(config-if-range)#
```

Part 3: Enable Storm Control

Step 1: Enable storm control for broadcasts.

a. Enable storm control for broadcasts on all ports connecting switches (trunk ports).

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.

```
SW-1(config)#inter range g0/1 , f0/1 , f0/23 - 24
SW-1(config-if-range)#storm-control broadcast level 50
SW-1(config-if-range)#
SW-1(config-if-range)#
```

```
SW-2(config)#inter range g0/1 , f0/1 , f0/23 - 24
SW-2(config-if-range)#storm-control broadcast level 50
SW-2(config-if-range)#
SW-2(config-if-range)#
```

```
Central(config)#
Central(config)#inte range g0/1 , g0/2 , f0/1
Central(config-if-range)#storm
Central(config-if-range)#storm-control bro
Central(config-if-range)#storm-control broadcast level 50
Central(config-if-range)#
```

Step 2: Verify storm control configuration.

Verify your configuration with the **show storm-control broadcast** and the **show run** commands.

```
SW-1#sh storm-control broadcast
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Fa0/1      Link Up          50.00%        50.00%        0.00%
Fa0/23     Link Up          50.00%        50.00%        0.00%
Fa0/24     Link Up          50.00%        50.00%        0.00%
Gig0/1     Link Up          50.00%        50.00%        0.00%

SW-1#
```

```
SW-2#sh storm-control broadcast
Interface  Filter State   Upper         Lower         Current
---------  -------------  ------------  ------------  ----------
Fa0/1      Link Up          50.00%        50.00%        0.00%
Fa0/23     Link Up          50.00%        50.00%        0.00%
Fa0/24     Link Up          50.00%        50.00%        0.00%
Gig0/1     Link Up          50.00%        50.00%        0.00%

SW-2#
```

```
Central#sh 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#
```

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-A** and **SW-B**. Set the maximum number of learned MAC address to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.

Note: A switch port must be configured as an access port to enable port security.

```
SW-A(config)#inter range f0/1 - 22
SW-A(config-if-range)#swit mode access
SW-A(config-if-range)#swit port-security
SW-A(config-if-range)#swit port-security maximum 2
SW-A(config-if-range)#swit port-security violation shutdown
SW-A(config-if-range)#swit port-security mac-address sticky
SW-A(config-if-range)#
SW-A(config-if-range)#
```

```
SW-B(config)#inter range f0/1 - 22
SW-B(config-if-range)#swit mode access
SW-B(config-if-range)#swit port-security
SW-B(config-if-range)#swit port-security maximum 2
SW-B(config-if-range)#swit port-security violation shutdown
SW-B(config-if-range)#swit port-security mac-address sticky
SW-B(config-if-range)#
SW-B(config-if-range)#
```

Why would you not want to enable port security on ports connected to other switches or routers?

Los puertos conectados a otros dispositivos de switch y router pueden, y deben, tener una gran cantidad de direcciones MAC aprendidas para ese único puerto. Limitar la cantidad de

direcciones MAC que se pueden aprender en estos puertos puede afectar significativamente la funcionalidad de la red.

Step 2: Verify port security.

On **SW-A**, issue the **show port-security interface fa0/1** command to verify that port security has been configured.

```
SW-A#sh port-security  inter 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#
SW-A#
```

Step 3: Disable unused ports.

Disable all ports that are currently unused.

```
SW-A(config)#
SW-A(config)#inter range f0/5 - 22
SW-A(config-if-range)#
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 FastEthernet0/7, changed state to

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
SW-A(config-if-range)#
```

```
SW-B(config)#inter 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 FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
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.

!!!Script for Central

```
!
spanning-tree mode pvst
spanning-tree vlan 1 priority 24576
!
!
!
!
!
!
interface FastEthernet0/1
 storm-control broadcast level 50
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
```

!!!Script for SW-1

```
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 28672
!
interface FastEthernet0/1
 storm-control broadcast level 50
!
interface FastEthernet0/23
 spanning-tree guard root
 storm-control broadcast level 50
!
interface FastEthernet0/24
 spanning-tree guard root
 storm-control broadcast level 50
!
interface GigabitEthernet0/1
 storm-control broadcast level 50
!
```

!!!Script for SW-2

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 storm-control broadcast level 50

!
interface FastEthernet0/23
 spanning-tree guard root
 storm-control broadcast level 50
!
interface FastEthernet0/24
 spanning-tree guard root
 storm-control broadcast level 50
!
interface GigabitEthernet0/1
 storm-control broadcast level 50
!
```

!!!Script for SW-A

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.3E81.4647
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.3EB5.12C1
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/23
!
interface FastEthernet0/24
```

!!!Script for SW-B

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.5803.C29C
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0007.EC04.EA86
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/23
!
interface FastEthernet0/24
```

6.5.1.3 Packet Tracer - Layer 2 VLAN Security

Monica Lizeth Alape

Part 1: Verify Connectivity

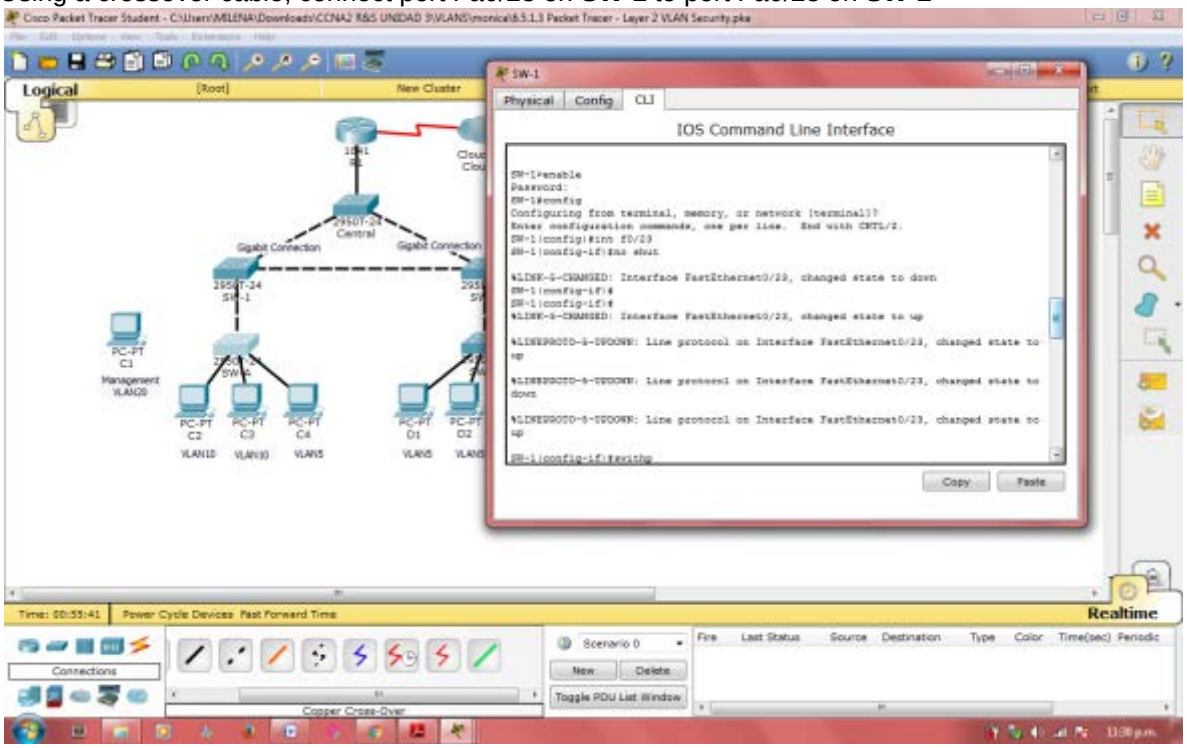
Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).
Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

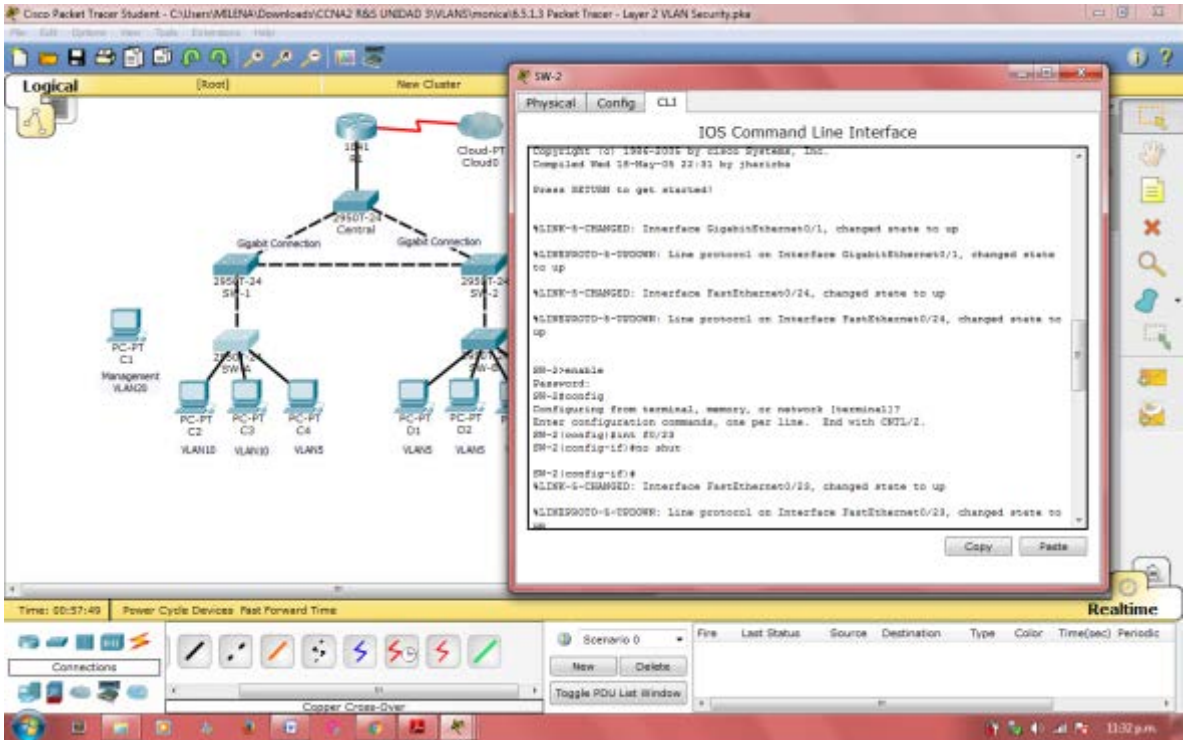
Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

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**



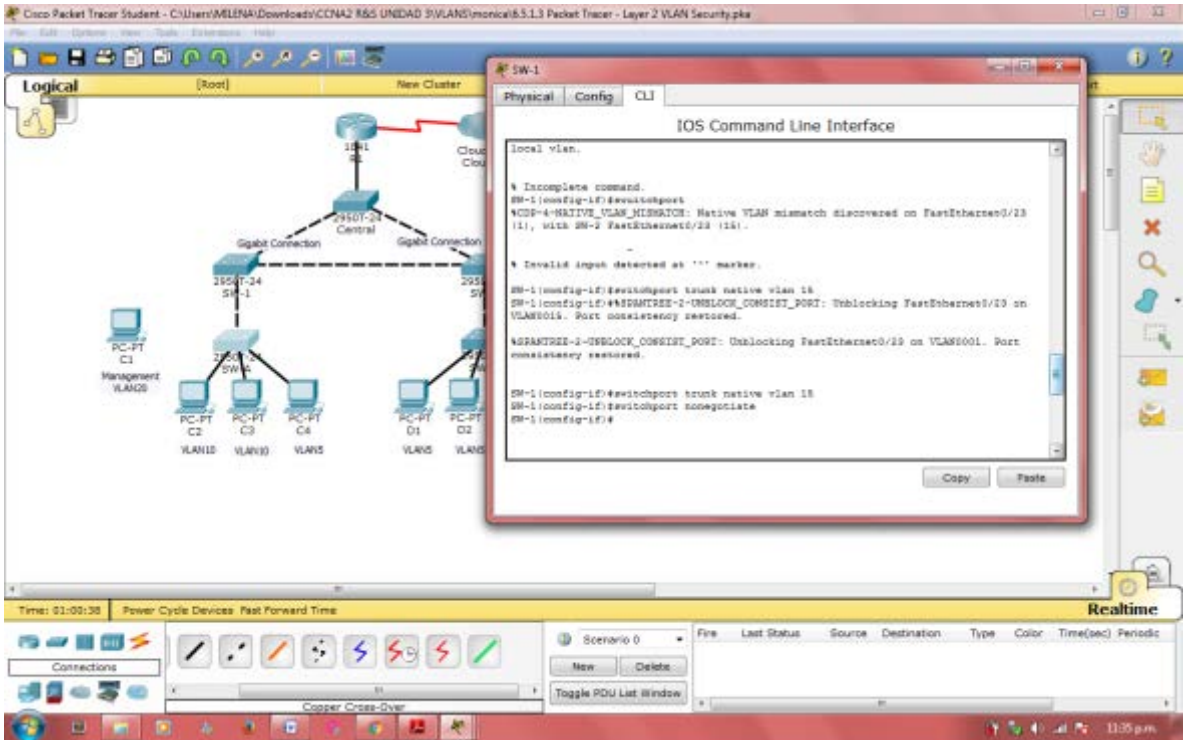


.

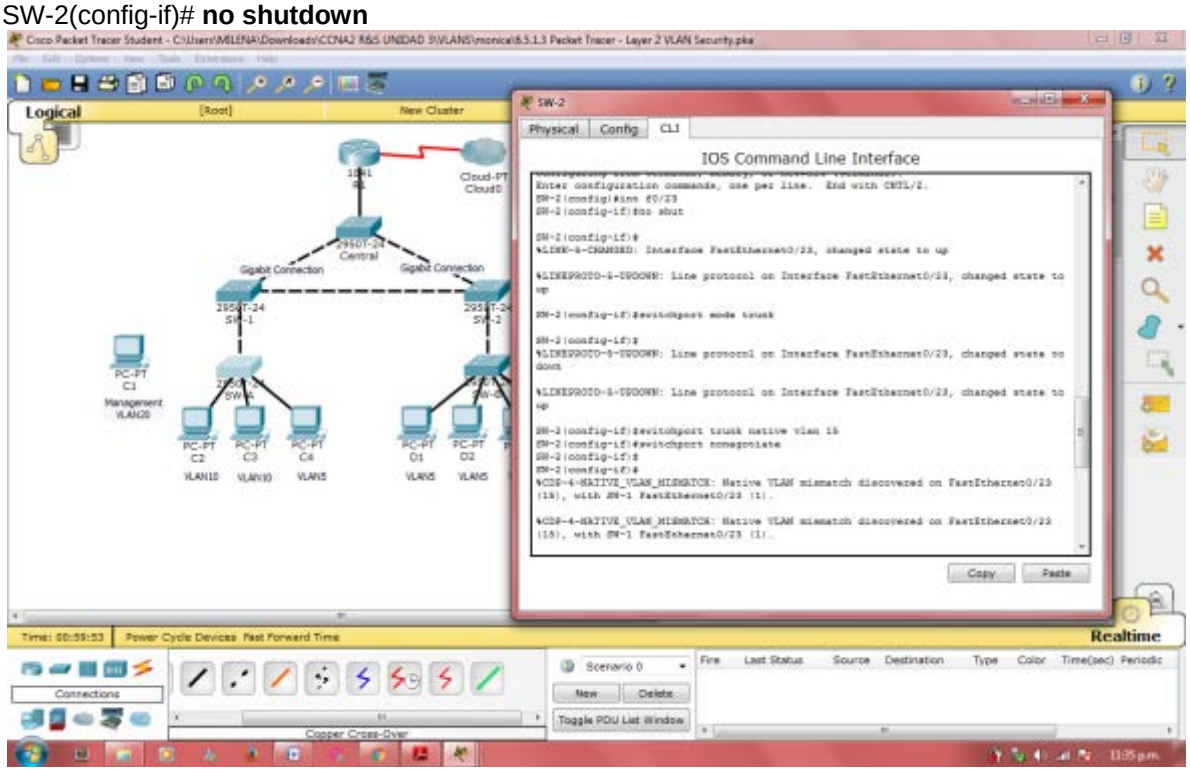
Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

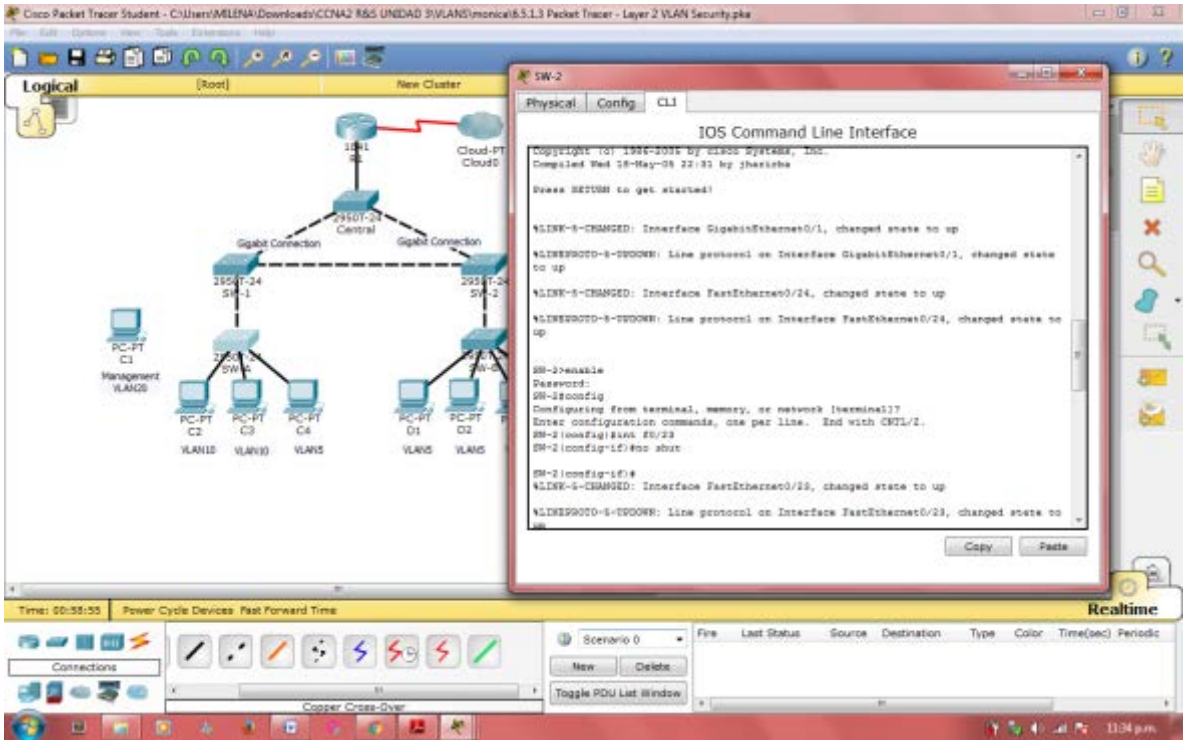
Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

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.

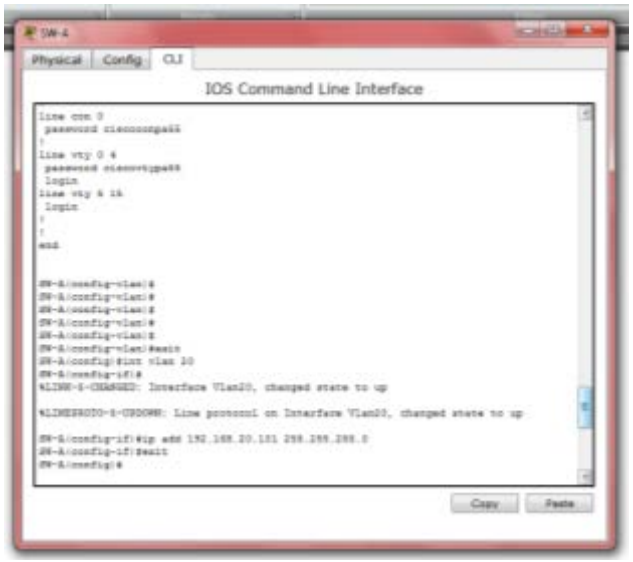
Step 1: Enable a management VLAN (VLAN 20) on SW-A.

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.

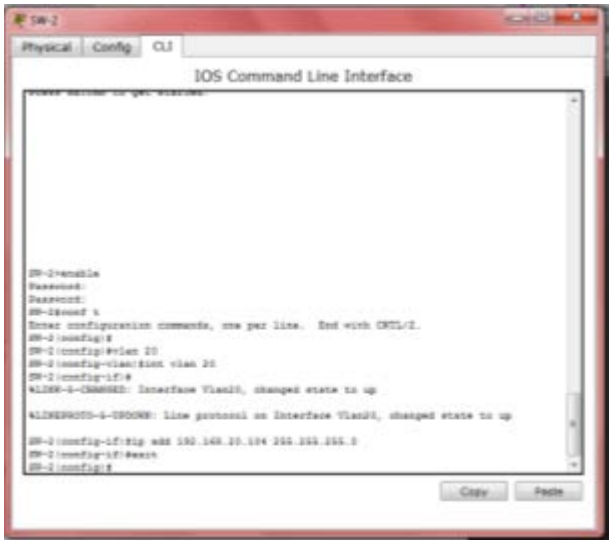
a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.

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.

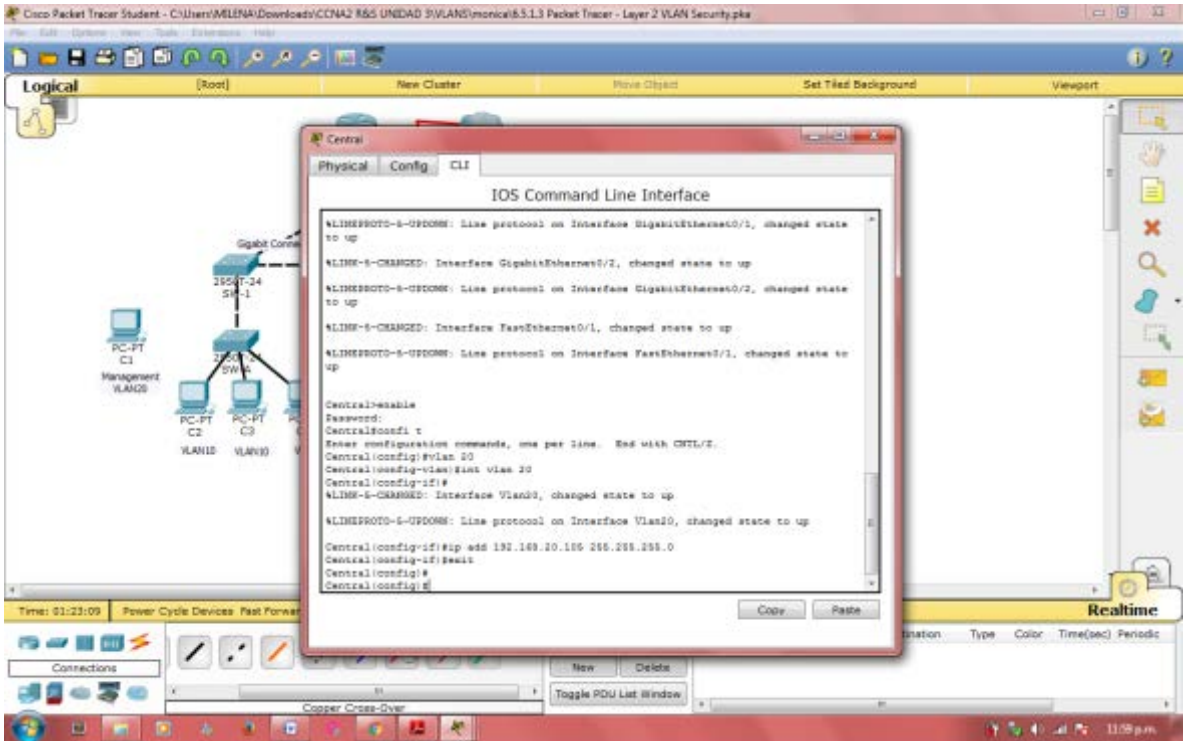
SW-B(config)# **interface vlan 20**
SW-B(config-if)# **ip address 192.168.20.2 255.255.255.0**

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**



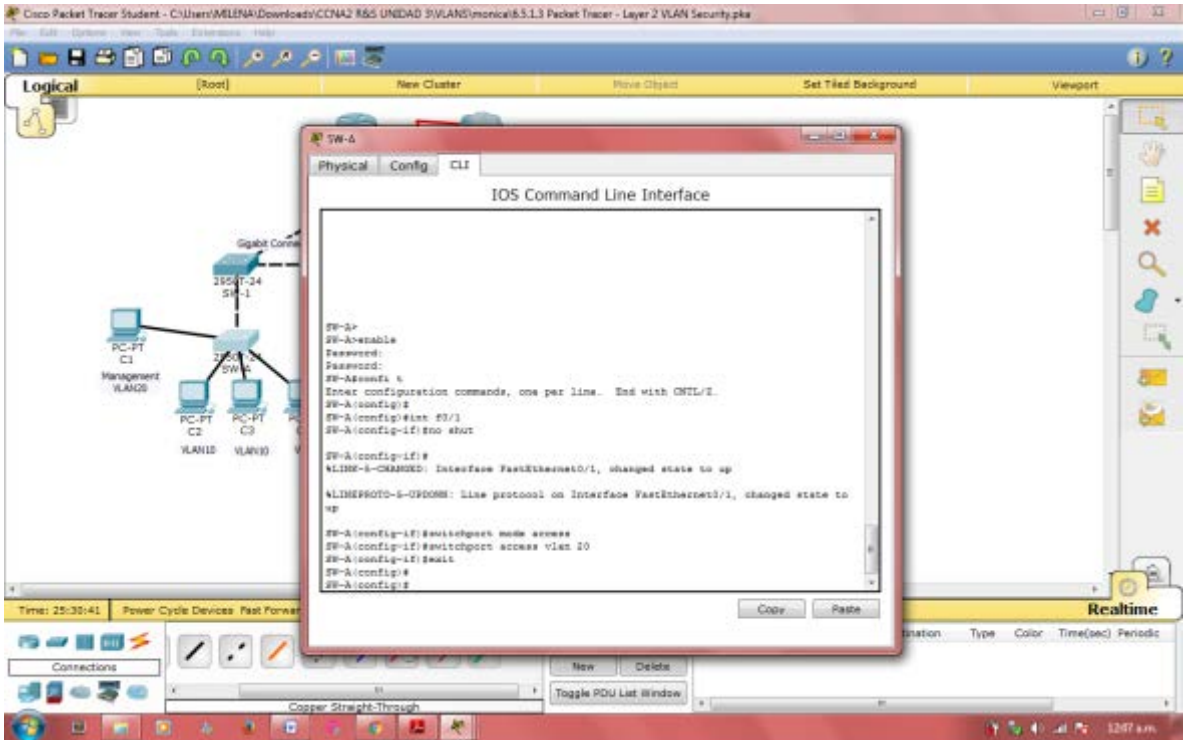
Central(config)# **interface vlan 20**
Central(config-if)# **ip address 192.168.20.5 255.255.255.0**



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**.

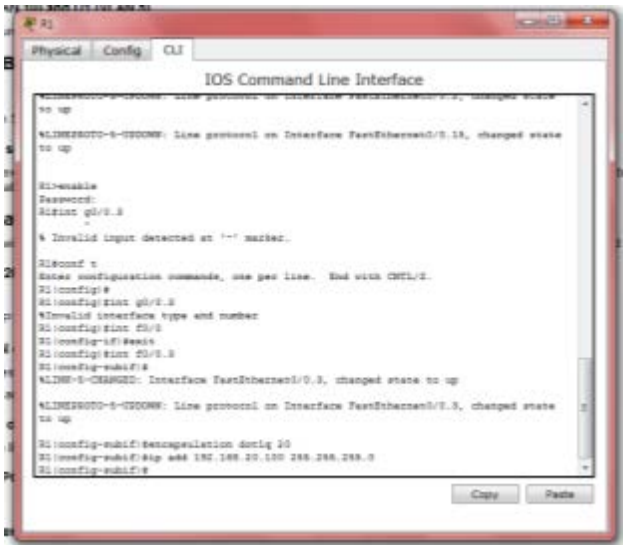
Part 4: Enable the Management PC to Access Router R1

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 Packet Tracer - Layer 2 VLAN Security**



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. **Packet Tracer - Layer 2 VLAN Security**

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

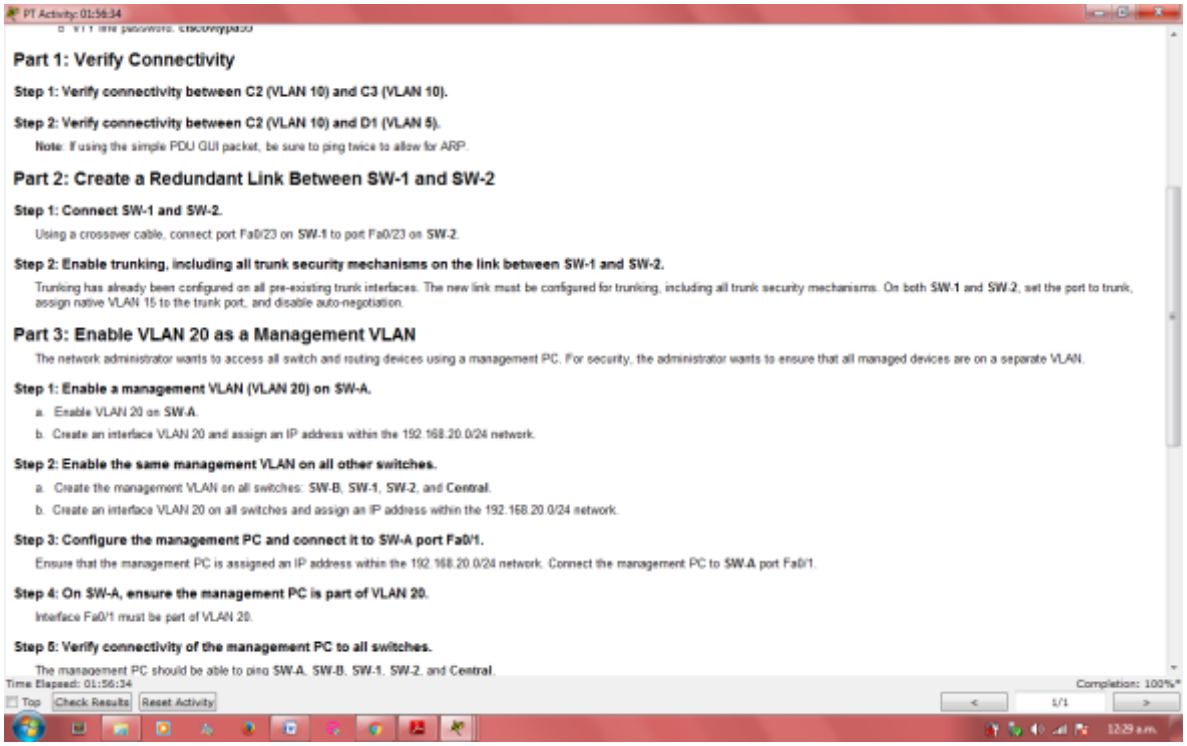
```
conf t
vlan 20
exit
interface vlan 20
ip address 192.168.20.2 255.255.255.0 Packet Tracer - Layer 2 VLAN Security
```


!!! 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
```



4. CONCLUSIONES

El anterior trabajo de manera general nos permitió interiorizar cada una de las temáticas desarrolladas, reconocer la importancia que tienen las redes a nivel global y en cada ámbito específico. Se desarrollan las competencias básicas que nos permiten llevar a cabo los procesos de configuración y administración de dispositivos tomando como base los conceptos de subredes y direccionamiento IP. De manera específica se desarrolló lo siguiente:

- ✓ Desarrollo de actividades encaminadas a la aprensión de las características y funcionalidad de la capa de transporte.
- ✓ Desarrollo de ejercicios de identificación y asignación de direcciones IP.
- ✓ Revisión de procesos de configuración de dispositivos de red.
- ✓ Identificación de los protocolos y comunicaciones de red.
- ✓ Exploración de los protocolos de la capa de aplicación y su funcionalidad.

5. BIBLIOGRAFIA

- CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1
- CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
- CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1
- CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1
- UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3